

# match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** command in class-map configuration mode. To remove ACL match criteria from a class map, use the **no** form of this command.

```
match access-group { access-group | name access-group-name }
```

```
no match access-group access-group
```

## Syntax Description

<i>access-group</i>	A numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. An ACL number can be a number from 1 to 2699.
<b>name</b> <i>access-group-name</i>	A named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. The name can be a maximum of 40 alphanumeric characters

## Defaults

No match criteria are configured.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.

## Usage Guidelines

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including ACLs, protocols, input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match access-group** command specifies a numbered or named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match access-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

**Note**

The **match-access group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the optional **log** keyword of the **access-list** command are not supported when configuring match criteria. For more information about the **access-list** command, refer to the [Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services](#), Release 12.3 T.

**Examples**

The following example specifies a class map called acl144 and configures the ACL numbered 144 to be used as the match criteria for this class:

```
class-map acl144
 match access-group 144
```

**Related Commands**

Command	Description
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.
<b>match input-interface</b>	Configures a class map to use the specified input interface as a match criterion.
<b>match mpls experimental</b>	Configures a class map to use the specified EXP field value as a match criterion.
<b>match protocol</b>	Configures the match criteria for a class map on the basis of the specified protocol.

# match any

To configure the match criteria for a class map to be successful match criteria for all packets, use the **match any** command in class-map configuration mode. To remove all criteria as successful match criteria, use the **no** form of this command.

**match any**

**no match any**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No match criteria are specified.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.

## Examples

In the following configuration, all packets leaving Ethernet interface 1/1 will be policed based on the parameters specified in policy-map class configuration mode.

```
Router(config)# class-map matchany
Router(config-cmap)# match any
Router(config-cmap)# exit

Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit

Router(config)# interface ethernet1/1
Router(config-if)# service-policy output policy1
```

## Related Commands

Command	Description
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.
<b>match input-interface</b>	Configures a class map to use the specified input interface as a match criterion.
<b>match protocol</b>	Configures the match criteria for a class map on the basis of the specified protocol.

# match class-map

To use a traffic class as a classification policy, use the **match class-map** command in class-map configuration mode. To remove a specific traffic class as a match criterion, use the **no** form of this command.

**match class-map** *class-map-name*

**no match class-map** *class-map-name*

## Syntax Description

<i>class-map-name</i>	Specifies the name of the traffic class to use as a match criterion.
-----------------------	--

## Defaults

No match criteria are specified.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.0(5)XE	This 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.

## Usage Guidelines

The only method of including both match-any and match-all characteristics in a single traffic class is to use the **match class-map** command. To combine match-any and match-all characteristics into a single class, a traffic class created with the match-any instruction must use a class configured with the match-all instruction as a match criterion (through the **match class-map** command), or vice versa.

You can also use the **match class-map** command to nest traffic classes within one another, saving users the overhead of re-creating a new traffic class when most of the information exists in a previously configured traffic class.

## Examples

In the following example, the traffic class called class1 has the same characteristics as traffic class called class2, with the exception that traffic class class1 has added a destination address as a match criterion. Rather than configuring traffic class class1 line by line, a user can enter the **match class-map class2** command. This command allows all of the characteristics in the traffic class called class2 to be included in the traffic class called class1, and the user can simply add the new destination address match criterion without reconfiguring the entire traffic class.

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
```

```

Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# exit

```

The following example shows how to combine the characteristics of two traffic classes, one with match-any and one with match-all characteristics, into one traffic class with the **match class-map** command. The result of traffic class called class4 requires a packet to match one of the following three match criteria to be considered a member of traffic class called class 4: IP protocol *and* QoS group 4, destination MAC address 1.1.1, or access group 2.

In this example, only the traffic class called class4 is used with the service policy called policy1.

```

Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
Router(config-cmap)# exit

Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit

Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit

```

#### Related Commands

Command	Description
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.

# match cos

To match a packet based on a Layer 2 class of service (CoS) marking, use the **match cos** command in class-map configuration mode. To remove a specific Layer 2 CoS/Inter-Switch Link (ISL) marking, use the **no** form of this command:

```
match cos cos-value [cos-value cos-value cos-value]
```

```
no match cos cos-value [cos-value cos-value cos-value]
```

## Syntax Description

<i>cos-value</i>	(Optional) Specific IEEE 802.1Q/ISL CoS value. The <i>cos-value</i> is from 0 to 7; up to four CoS values can be specified in one <b>match cos</b> statement.
------------------	---

## Defaults

No match criteria are specified.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.1(5)T	This command was introduced.

## Examples

In the following example, the CoS-values of 1, 2, and 3 are successful match criteria for the interface containing the classification policy called cos:

```
Router(config)# class-map cos
Router(config-cmap)# match cos 1 2 3
```

In the following example, classes called voice and video-n-data are created to classify traffic based on the CoS values. QoS treatment is then given to the appropriate packets (in this case, the QoS treatment is priority 64 and bandwidth 512) in the CoS-based-treatment policy map.

```
Router(config)# class-map voice
Router(config-cmap)# match cos 7

Router(config)# class-map video-n-data
Router(config-cmap)# match cos 5

Router(config)# policy-map cos-based-treatment
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 64
Router(config-pmap-c)# exit
Router(config-pmap)# class video-n-data
Router(config-pmap-c)# bandwidth 512
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

```
Router(config)# interface fastethernet0/0.1  
Router(config-if)# service-policy output cos-based-treatment
```

The service policy configured in this section is attached to all packets leaving Fast Ethernet interface 0/0.1. The service policy can be attached to any interface that supports service policies.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.
<b>policy-map</b>	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
<b>service-policy</b>	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.
<b>set cos</b>	Sets the Layer 2 CoS value of an outgoing packet.
<b>show class-map</b>	Displays all class maps and their matching criteria.

# match destination-address mac

To use the destination MAC address as a match criterion, use the **match destination-address mac** command in class-map configuration mode. To remove a previously specified destination MAC address as a match criterion, use the **no** form of this command.

**match destination-address mac** *address*

**no match destination-address mac** *address*

<b>Syntax Description</b>	<i>address</i>	Specifies the specific destination MAC address to be used as a match criterion.
---------------------------	----------------	---

**Defaults** No destination MAC address is specified.

**Command Modes** Class-map configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(5)XE	This 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.	

**Examples** The following example specifies a class map called macaddress and specifies the destination MAC address to be used as the match criterion for this class:

```
class-map macaddress
  match destination-address mac 00:00:00:00:00:00
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.

# match discard-class

To match packets of a certain discard class, use the **match discard-class** command in class-map configuration mode.

**match discard-class** *class-number*

<b>Syntax Description</b>	<i>class-number</i>	Number of the discard class being matched. Valid values are 0 to 7.
<b>Defaults</b>	Packets will not be classified as expected.	
<b>Command Modes</b>	Class-map configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(13)T	This command was introduced.
<b>Examples</b>	The following example shows that packets in discard class 2 are matched: <pre>match discard-class 2</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>set discard-class</b>	Marks a packet with a discard-class value.

# match dscp

To identify a specific IP differentiated service code point (DSCP) value as a match criterion, use the **match dscp** command in class-map configuration mode. To remove a specific DSCP value from a class map, use the **no** form of this command.

```
match [ip] dscp dscp-value [dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value]
```

```
no match [ip] dscp dscp-value [dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value]
```

## Syntax Description

<b>ip</b>	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets.
<i>dscp-value</i>	Specifies the exact value from 0 to 63 used to identify an IP DSCP value.

## Defaults

Matching on both IPv4 and IPv6 packets is the default.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the <b>match ip dscp</b> command.

## Usage Guidelines

### DSCP Values

Up to eight DSCP values can be matched in one match statement. For example, if you wanted the DSCP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified DSCP values), enter the **match dscp 0 1 2 3 4 5 6 7** command.

This command is used by the class map to identify a specific DSCP value marking on a packet. In this context, *dscp-value* arguments are used as markings only and have no mathematical significance. For instance, the *dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *dscp-value* of 2 is different from a packet marked with the *dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

### Match IPv6 Packets on DSCP Values

To match DSCP values for IPv6 packets only, the **match protocol ipv6** command must also be used. Without that command, the DSCP match defaults to match both IPv4 and IPv6 packets.

### Match IPv4 Packets on DSCP Values

To match DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword, the match occurs on both IPv4 and IPv6 packets. Alternatively, the **match protocol ip** command can be used with the **match dscp** command to classify only IPv4 packets.

**Examples****Priority50 Service Policy Matching DSCP Value**

The following example shows how to configure the service policy called “priority50” and attach service policy “priority50” to an interface. In this example, the class map called “ipdscp15” will evaluate all packets entering interface Fast Ethernet 1/0/0 for an IP DSCP value of 15. If the incoming packet has been marked with the IP DSCP value of 15, the packet will be treated as priority traffic and will be allocated with bandwidth of 50 kbps.

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match ip dscp 15
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipdscp15
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet1/0/0
Router(config-if)# service-policy output priority50
```

**Related Commands**

Command	Description
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.
<b>policy-map</b>	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
<b>service-policy</b>	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.
<b>set dscp</b>	Marks the DSCP value for packets within a traffic class.
<b>show class-map</b>	Displays all class maps and their matching criteria.

# match fr-dlci

To specify the Frame Relay data-link connection identifier (DLCI) number as a match criterion in a class map, use the **match fr-dlci** command in class-map configuration mode. To remove a previously specified DLCI number as a match criterion, use the **no** form of this command.

**match fr-dlci** *dlci-number*

**no match fr-dlci** *dlci-number*

## Syntax Description

<i>dlci-number</i>	Number of the DLCI associated with the packet.
--------------------	--

## Defaults

No DLCI number is specified.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.2(13)T	This command was introduced.

## Usage Guidelines

This match criterion can be used in main interfaces and point-to-multipoint subinterfaces in Frame Relay networks, and it can also be used in hierarchical policy maps.

## Examples

In the following example a class map called “class1” has been created and the Frame Relay DLCI number of 500 has been specified as a match criterion. Packets matching this criterion are placed in class1.

```
Router(config)# class-map class1
Router(config-cmap)# match fr-dlci 500
Router(config-cmap)# end
```

## Related Commands

Command	Description
<b>show class-map</b>	Displays all class maps and their matching criteria.
<b>show policy-map interface</b>	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.

# match input-interface

To configure a class map to use the specified input interface as a match criterion, use the **match input-interface** command in class-map configuration mode. To remove the input interface match criterion from a class map, use the **no** form of this command.

**match input-interface** *interface-name*

**no match input-interface** *interface-name*

## Syntax Description

<i>interface-name</i>	Name of the input interface to be used as match criteria.
-----------------------	---

## Defaults

No match criteria are specified.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.

## Usage Guidelines

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including input interfaces, access control lists (ACLs), protocols, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match input-interface** command specifies the name of an input interface to be used as the match criterion against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match input-interface** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

---

**Examples**

The following example specifies a class map called eth1 and configures the input interface named ethernet1 to be used as the match criterion for this class:

```
class-map ethernet1
 match input-interface ethernet1
```

---

**Related Commands**

Command	Description
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.
<b>match access-group</b>	Configures the match criteria for a class map based on the specified ACL.
<b>match mpls experimental</b>	Configures a class map to use the specified EXP field value as a match criterion.
<b>match protocol</b>	Configures the match criteria for a class map on the basis of the specified protocol.

# match ip dscp

The **match ip dscp** command is replaced by the **match dscp** command. See the **match dscp** command for more information.

# match ip precedence

The **match ip precedence** command is replaced by the **match precedence** command. See the **match precedence** command for more information.

# match ip rtp

To configure a class map to use the Real-Time Protocol (RTP) protocol port as the match criterion, use the **match ip rtp** command in class-map configuration mode. To remove the RTP protocol port match criterion, use the **no** form of this command.

**match ip rtp** *starting-port-number port-range*

**no match ip rtp**

## Syntax Description

<i>starting-port-number</i>	The starting RTP port number. Values range from 2000 to 65535.
<i>port-range</i>	The RTP port number range. Values range from 0 to 16383.

## Defaults

No match criteria are specified.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.1(2)T	This command was introduced.

## Usage Guidelines

This command is used to match IP RTP packets that fall within the specified port range. It matches packets destined to all even User Datagram Port (UDP) port numbers in the range <starting port range> <starting port range + port range>.

Use of an RTP port range as the match criterion is particularly effective for applications that use RTP, such as voice or video.

## Examples

The following example specifies a class map called eth1 and configures the RTP port number 2024 and range 1000 to be used as the match criteria for this class:

```
class-map ethernet1
 match ip rtp 2024 1000
```

## Related Commands

Command	Description
<b>ip rtp priority</b>	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
<b>match access-group</b>	Configures the match criteria for a class map based on the specified ACL number.

# match mpls experimental

To configure a class map to use the specified value of the experimental (EXP) field as a match criterion, use the **match mpls experimental** command in class-map configuration mode. To remove the EXP field match criterion from a class map, use the **no** form of this command.

**match mpls experimental** *number*

**no match mpls experimental** *number*

## Syntax Description

<i>number</i>	EXP field value (any number from 0 through 7) to be used as a match criterion. Numbers can be space delimited (for example, 3 4 7).
---------------	---

## Defaults

No match criteria are specified.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.0(7)XE1	This 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(4)T	This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card.
12.2(4)T2	This command was implemented on the Cisco 7500 series.

## Usage Guidelines

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including input interfaces, access control lists (ACLs), protocols, quality of service (QoS) labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match mpls experimental** command specifies the name of an EXP field value to be used as the match criterion against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match mpls experimental** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

**Examples**

The following example specifies a class map called eth1 and configures the Multiprotocol Label Switching (MPLS) experimental values of 1 and 2 to be used as the match criterion for this class:

```
Router(config)# class-map ethernet1
Router(config-cmap)# match mpls experimental 1 2
```

**Related Commands**

Command	Description
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.
<b>match access-group</b>	Configures the match criteria for a class map based on the specified ACL.
<b>match input-interface</b>	Configures a class map to use the specified input interface as a match criterion.
<b>match protocol</b>	Matches traffic by a particular protocol.
<b>match qos-group</b>	Configures the match criteria for a class map based on the specified protocol.

# match mpls experimental topmost

To match the experimental (EXP) value in the topmost label, use the **match mpls experimental topmost** command in class-map configuration mode.

**match mpls experimental topmost** *value*

## Syntax Description

<i>value</i>	Value of the Multiprotocol Label Switching (MPLS) EXP field in the topmost label header. Valid values are 0 to 7.
--------------	---

## Defaults

Packets will not be classified as expected.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.2(13)T	This command was introduced.

## Usage Guidelines

You can enter this command on the input and the output interfaces. It will match only on MPLS packets.

## Examples

The following example shows that the EXP value 3 in the topmost label is matched:

```
match mpls experimental topmost 3
```

## Related Commands

Command	Description
<b>set mpls experimental topmost</b>	Sets the MPLS EXP field value in the topmost MPLS label header at the input and/or output interfaces.

# match not

To specify the single match criterion value to use as an unsuccessful match criterion, use the **match not** command in class-map configuration mode. To remove a previously specified source value to not use as a match criterion, use the **no** form of this command.

**match not** *match-criteria*

**no match not** *match-criteria*

## Syntax Description

<i>match-criteria</i>	Specifies the match criterion value that is an unsuccessful match criterion. All other values of the specified match criterion will be considered successful match criteria.
-----------------------	--

## Defaults

No default behavior or values

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.

## Usage Guidelines

The **match not** command is used to specify a QoS policy value that is not used as a match criterion. When the **match not** command is used, all other values of that QoS policy become successful match criteria.

For instance, if the **match not qos-group 4** command is issued in class-map configuration mode, the specified class will accept all QoS group values except 4 as successful match criteria.

## Examples

In the following traffic class, all protocols except IP are considered successful match criteria:

```
Router(config)# class-map noip
Router(config-cmap)# match not protocol ip
Router(config-cmap)# exit
```

## Related Commands

Command	Description
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.

## match packet length (class-map)

To specify the Layer 3 packet length in the IP header as a match criterion in a class map, use the **match packet length** command in class-map configuration mode. To remove a previously specified Layer 3 packet length as a match criterion, use the **no** form of this command.

```
match packet length {max maximum-length-value [min minimum-length-value] | min
minimum-length-value [max maximum-length-value]}
```

```
no match packet length {max maximum-length-value [min minimum-length-value] | min
minimum-length-value [max maximum-length-value]}
```

### Syntax Description

<b>max</b>	Maximum. Indicates that a maximum value for the Layer 3 packet length is to be specified.
<i>maximum-length-value</i>	Specifies the maximum length value of the Layer 3 packet length, in bytes. The range is from 1 to 2000.
<b>min</b>	Minimum. Indicates that a minimum value for the Layer 3 packet length is to be specified.
<i>minimum-length-value</i>	Specifies the minimum length value of the Layer 3 packet length, in bytes. The range is from 1 to 2000.

### Defaults

If only the minimum value is specified, a packet with a Layer 3 length greater than the minimum is viewed as matching the criterion.

If only the maximum value is specified, a packet with a Layer 3 length less than the maximum is viewed as matching the criterion.

### Command Modes

Class-map configuration

### Command History

Release	Modification
12.2(13)T	This command was introduced.

### Usage Guidelines

This command considers only the Layer 3 packet length in the IP header. It does not consider the Layer 2 packet length in the IP header.

When using this command, you must at least specify the maximum or minimum value. However, you do have the option of entering both values.

### Examples

In the following example a class map called “class 1” has been created, and the Layer 3 packet length has been specified as a match criterion. In this example, packets with a minimum Layer 3 packet length of 100 and a maximum Layer 3 packet length of 300 are viewed as meeting the match criteria.

```
Router(config)# class map match-all class1
Router(config-cmap)# match packet length min 100 max 300
```

Related Commands	Command	Description
	<b>show class-map</b>	Displays all class maps and their matching criteria.
	<b>show policy-map interface</b>	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.

# match precedence

To identify IP precedence values as match criteria, use the **match precedence** command in class-map configuration mode. To remove IP precedence values from a class map, use the **no** form of this command.

**match [ip] precedence** *precedence-value* [*precedence-value precedence-value precedence-value*]

**no match [ip] precedence** *precedence value* [*precedence-value precedence-value precedence-value*]

## Syntax Description

<b>ip</b>	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both the IPv4 and IPv6 packets.
<i>precedence-value</i>	Specifies the exact value from 0 to 7 used to identify a precedence value.

## Defaults

Matching on both IPv4 and IPv6 packets is the default.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.2(13)T	This command was introduced.

## Usage Guidelines

### Precedence Value Arguments

Up to four precedence values can be matched in one match statement. For example, if you wanted the precedence values of 0, 1, 2, or 3 (note that only one of the precedence values must be a successful match criterion, not all of the specified precedence values), enter the **match ip precedence 0 1 2 3** command.

The *precedence-value* arguments are used as markings only. In this context, the IP precedence values have no mathematical significance. For instance, the *precedence-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *precedence-value* of 2 is different from a packet marked with the *precedence-value* of 1. The treatment of these different packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

### Match on Precedence for IPv6 Only

To match on precedence values for IPv6 packets only, the **match protocol ipv6** command must also be used. Without that command, the precedence match defaults to match both IPv4 and IPv6 packets.

### Match on Precedence for IPv4 Packets Only

To match on precedence values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword, the match occurs on both IPv4 and IPv6 packets.

**Examples****IPv4-Specific Traffic Match**

The following example shows how to configure the service policy called “priority50” and attach service policy “priority50” to an interface, matching for IPv4 traffic only. In a network where both IPv4 and IPv6 are running, you might find it necessary to distinguish between the protocols for matching and traffic segregation. In this example, the class map called “ipprec5” will evaluate all IPv4 packets entering Fast Ethernet interface 1/0/0 for a precedence value of 5. If the incoming IPv4 packet has been marked with the precedence value of 5, the packet will be treated as priority traffic and will be allocated with bandwidth of 50 kbps.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match ip precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet1/0/0
Router(config-if)# service-policy input priority50
```

**IPv6-Specific Traffic Match**

The following example shows the same service policy matching on precedence for IPv6 traffic only. Notice that the **match protocol** command with the **ipv6** keyword precedes the **match precedence** command. The **match protocol** command is required to perform matches on IPv6 traffic alone.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match protocol ipv6
Router(config-cmap)# match precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet1/0/0
Router(config-if)# service-policy input priority50
```

**Related Commands**

Command	Description
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.
<b>policy-map</b>	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
<b>service-policy</b>	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.
<b>set ip precedence</b>	Sets the precedence value in the IP header.
<b>show class-map</b>	Displays all class maps and their matching criteria, or a specified class map and its matching criteria.

# match protocol

To configure the match criteria for a class map on the basis of the specified protocol, use the **match protocol** command in class-map configuration mode. To remove protocol-based match criteria from a class map, use the **no** form of this command.

**match protocol** *protocol-name*

**no match protocol** *protocol-name*

## Syntax Description

<i>protocol-name</i>	<p>Name of the protocol used as a matching criterion. Supported protocols include the following:</p> <ul style="list-style-type: none"> <li>• <b>aarp</b>—AppleTalk Address Resolution Protocol</li> <li>• <b>arp</b>—IP Address Resolution Protocol (ARP)</li> <li>• <b>bridge</b>—bridging</li> <li>• <b>bstun</b>—Block Serial Tunneling</li> <li>• <b>cdp</b>—Cisco Discovery Protocol</li> <li>• <b>clns</b>—ISO Connectionless Network Service</li> <li>• <b>clns_es</b>—ISO CLNS End System</li> <li>• <b>clns_is</b>—ISO CLNS Intermediate System</li> <li>• <b>cmns</b>—ISO Connection-Mode Network Service</li> <li>• <b>compressedtcp</b>—compressed TCP</li> <li>• <b>decnet</b>—DECnet</li> <li>• <b>decnet_node</b>—DECnet Node</li> <li>• <b>decnet_router-I1</b>—DECnet Router L1</li> <li>• <b>decnet_router-I2</b>—DECnet Router L2</li> <li>• <b>dlsw</b>—data-link switching</li> <li>• <b>ip</b>—IP</li> <li>• <b>ipv6</b>—IPv6</li> <li>• <b>ipx</b>—Novell IPX</li> <li>• <b>llc2</b>—llc2</li> <li>• <b>pad</b>—packet assembler/disassembler links</li> <li>• <b>qllc</b>—Qualified Logical Link Control protocol</li> <li>• <b>rsrb</b>—remote source-route bridging</li> <li>• <b>snapshot</b>—snapshot routing support</li> <li>• <b>stun</b>—serial tunnel</li> </ul>
----------------------	--

## Defaults

No default behavior or values

**Command Modes** Class-map configuration

### Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(13)E	This command was implemented on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	This command was modified to remove apollo, vines, and xns from the list of protocols used as matching criteria. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in Release 12.2(13)T.  In addition, the <b>ipv6</b> keyword was added to support protocol matching on IPv6 packets.

### Usage Guidelines

For class-based weighted fair queuing (CBWFQ), you define traffic classes based on match criteria including protocols, access control lists (ACLs), input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match protocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match protocol** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

To match protocols known to network-based application recognition (NBAR), use the **match protocol (NBAR)** command.

### Examples

The following example specifies a class map called ipx and configures the Internetwork Packet Exchange (IPX) protocol as a match criterion for it:

```
class-map ipx
  match protocol ipx
```

Related Commands	Command	Description
	<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.
	<b>match access-group</b>	Configures the match criteria for a class map based on the specified ACL.
	<b>match input-interface</b>	Configures a class map to use the specified input interface as a match criterion.
	<b>match precedence</b>	Identifies IP precedence values as match criteria.
	<b>match protocol (NBAR)</b>	Configures NBAR to match traffic by a protocol type known to NBAR.
	<b>match qos-group</b>	Configures a class map to use the specified EXP field value as a match criterion.

# match protocol (NBAR)

To configure network-based application recognition (NBAR) to match traffic by a protocol type known to NBAR, use the **match protocol** command in class-map configuration mode. To disable NBAR from matching traffic by a known protocol type, use the **no** form of this command.

```
match protocol protocol-name [variable-field-name value]
```

```
no match protocol protocol-name [variable-field-name value]
```

## Syntax Description

<i>protocol-name</i>	Identifies a particular protocol type known to NBAR. These known protocol types can be used to match traffic. For a list of protocol types known to NBAR, see <a href="#">Table 7</a> , <a href="#">Table 8</a> , and <a href="#">Table 9</a> in “Usage Guidelines.”
<i>variable-field-name</i>	(Optional and only usable with custom protocols) Used for specifying a pre-defined variable that was created when you created a custom protocol. The <i>variable-field-name</i> will match the <i>field-name</i> variable entered when you created the custom protocol.
<i>value</i>	(Optional and only usable with custom protocols) A specific value in the custom payload to match. A value can only be entered along with a <i>variable-field-name</i> . The value can be expressed in decimal or hexadecimal format.

## Defaults

No default behavior or values.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12(1)E. The <i>variable-field-name value</i> option was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)T. This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

## Usage Guidelines

Use the **match protocol** (NBAR) command to match protocol types that are known to NBAR. NBAR is capable of classifying the following types of protocols:

- Non-User Datagram Protocol (UDP) and non-Transmission Control Protocol (TCP) IP protocols
- TCP and UDP protocols that use statically assigned port numbers

- TCP and UDP protocols that dynamically assign port numbers and, therefore, require stateful inspection.

Table 7 lists the non-UDP and non-TCP IP protocols NBAR can classify.

**Table 7 Non-UDP and Non-TCP Protocols**

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release <sup>1</sup>
EGP	IP	8	Exterior Gateway Protocol	egp	12.0(5)XE2 12.1(1)E 12.1(5)T
EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp	12.0(5)XE2 12.1(1)E 12.1(5)T
GRE	IP	47	Generic Routing Encapsulation	gre	12.0(5)XE2 12.1(1)E 12.1(5)T
ICMP	IP	1	Internet Control Message Protocol	icmp	12.0(5)XE2 12.1(1)E 12.1(5)T
IPINIP	IP	4	IP in IP	ipinip	12.0(5)XE2 12.1(1)E 12.1(5)T
IPSec	IP	50, 51	IP Encapsulating Security Payload/Authentication Header	ipsec	12.0(5)XE2 12.1(1)E 12.1(5)T

1. Indicates the Cisco IOS maintenance release that first supported the protocol. This table is updated when a protocol is added to a new Cisco IOS release train.

Table 8 lists the TCP and UDP static port protocols NBAR can classify.

**Table 8 TCP and UDP Static Port Protocols**

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release <sup>1</sup>
BGP	TCP/UDP	179	Border Gateway Protocol	bgp	12.0(5)XE2 12.1(1)E 12.1(5)T
CU-SeeMe	TCP/UDP	7648, 7649	Desktop videoconferencing	cuseeme	12.0(5)XE2 12.1(1)E 12.1(5)T
CU-SeeMe	UDP	24032	Desktop video conferencing	cuseeme	12.0(5)XE2 12.1(1)E 12.1(5)T

**Table 8 TCP and UDP Static Port Protocols (continued)**

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release <sup>1</sup>
DHCP/ BOOTP	UDP	67, 68	Dynamic Host Configuration Protocol/ Bootstrap Protocol	dhcp	12.0(5)XE2 12.1(1)E 12.1(5)T
DNS	TCP/UDP	53	Domain Name System	dns	12.0(5)XE2 12.1(1)E 12.1(5)T
Finger	TCP	79	Finger user information protocol	finger	12.0(5)XE2 12.1(1)E 12.1(5)T
Gopher	TCP/UDP	70	Internet Gopher Protocol	gopher	12.0(5)XE2 12.1(1)E 12.1(5)T
HTTP	TCP	80 <sup>2</sup>	Hypertext Transfer Protocol	http	12.0(5)XE2 12.1(1)E 12.1(5)T
HTTPS	TCP	443	Secured HTTP	secure-http	12.0(5)XE2 12.1(1)E 12.1(5)T
IMAP	TCP/UDP	143, 220	Internet Message Access Protocol	imap	12.0(5)XE2 12.1(1)E 12.1(5)T
IRC	TCP/UDP	194	Internet Relay Chat	irc	12.0(5)XE2 12.1(1)E 12.1(5)T
Kerberos	TCP/UDP	88, 749	Kerberos Network Authentication Service	kerberos	12.0(5)XE2 12.1(1)E 12.1(5)T
L2TP	UDP	1701	L2F/L2TP tunnel	l2tp	12.0(5)XE2 12.1(1)E 12.1(5)T
LDAP	TCP/UDP	389	Lightweight Directory Access Protocol	ldap	12.0(5)XE2 12.1(1)E 12.1(5)T
MS-PPTP	TCP	1723	Microsoft Point-to-Point Tunneling Protocol for VPN	pptp	12.0(5)XE2 12.1(1)E 12.1(5)T
MS-SQLServer	TCP	1433	Microsoft SQL Server Desktop Videoconferencing	sqlserver	12.0(5)XE2 12.1(1)E 12.1(5)T

**Table 8 TCP and UDP Static Port Protocols (continued)**

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release <sup>1</sup>
NetBIOS	TCP	137, 139	NetBIOS over IP (MS Windows)	netbios	12.0(5)XE2 12.1(1)E 12.1(5)T
NetBIOS	UDP	137, 138	NetBIOS over IP (MS Windows)	netbios	12.0(5)XE2 12.1(1)E 12.1(5)T
NFS	TCP/UDP	2049	Network File System	nfs	12.0(5)XE2 12.1(1)E 12.1(5)T
NNTP	TCP/UDP	119	Network News Transfer Protocol	nntp	12.0(5)XE2 12.1(1)E 12.1(5)T
Notes	TCP/UDP	1352	Lotus Notes	notes	12.0(5)XE2 12.1(1)E 12.1(5)T
Novadigm	TCP/UDP	3460-3465	Novadigm Enterprise Desktop Manager (EDM)	novadigm	12.1(2)E 12.1(5)T
NTP	TCP/UDP	123	Network Time Protocol	ntp	12.0(5)XE2 12.1(1)E 12.1(5)T
PCAnywhere	TCP	5631, 65301	Symantec PCAnywhere	pcanywhere	12.0(5)XE2 12.1(1)E 12.1(5)T
PCAnywhere	UDP	22, 5632	Symantec PCAnywhere	pcanywhere	12.0(5)XE2 12.1(1)E 12.1(5)T
POP3	TCP/UDP	110	Post Office Protocol	pop3	12.0(5)XE2 12.1(1)E 12.1(5)T
Printer	TCP/UDP	515	Printer	printer	12.1(2)E 12.1(5)T
RIP	UDP	520	Routing Information Protocol	rip	12.0(5)XE2 12.1(1)E 12.1(5)T
RSVP	UDP	1698, 1699	Resource Reservation Protocol	rsvp	12.0(5)XE2 12.1(1)E 12.1(5)T
SFTP	TCP	990	Secure FTP	secure-ftp	12.0(5)XE2 12.1(1)E 12.1(5)T

**Table 8** TCP and UDP Static Port Protocols (continued)

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release <sup>1</sup>
SHTTP	TCP	443	Secure HTTP	secure-http	12.0(5)XE2 12.1(1)E 12.1(5)T
SIMAP	TCP/UDP	585, 993	Secure IMAP	secure-imap	12.0(5)XE2 12.1(1)E 12.1(5)T
SIRC	TCP/UDP	994	Secure IRC	secure-irc	12.0(5)XE2 12.1(1)E 12.1(5)T
SLDAP	TCP/UDP	636	Secure LDAP	secure-ldap	12.0(5)XE2 12.1(1)E 12.1(5)T
SMTP	TCP	25	Simple Mail Transfer Protocol	smtp	12.0(5)XE2 12.1(1)E 12.1(5)T
SNMP	TCP/UDP	161, 162	Simple Network Management Protocol	snmp	12.0(5)XE2 12.1(1)E 12.1(5)T
SNNTTP	TCP/UDP	563	Secure NNTP	secure-nntp	12.0(5)XE2 12.1(1)E 12.1(5)T
SOCKS	TCP	1080	Firewall security protocol	socks	12.0(5)XE2 12.1(1)E 12.1(5)T
SPOP3	TCP/UDP	995	Secure POP3	secure-pop3	12.0(5)XE2 12.1(1)E 12.1(5)T
SSH	TCP	22	Secured Shell	ssh	12.0(5)XE2 12.1(1)E 12.1(5)T
STELNET	TCP	992	Secure Telnet	secure-telnet	12.0(5)XE2 12.1(1)E 12.1(5)T
Syslog	UDP	514	System Logging Utility	syslog	12.0(5)XE2 12.1(1)E 12.1(5)T

**Table 8 TCP and UDP Static Port Protocols (continued)**

Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release <sup>1</sup>
Telnet	TCP	23	Telnet Protocol	telnet	12.0(5)XE2 12.1(1)E 12.1(5)T
X Windows	TCP	6000-6003	X11, X Windows	xwindows	12.0(5)XE2 12.1(1)E 12.1(5)T

1. Indicates the Cisco IOS maintenance release that first supported the protocol. This table is updated when a protocol is added to a new Cisco IOS release train.
2. In Release 12.3(4)T, the NBAR Extended Inspection for Hypertext Transfer Protocol (HTTP) Traffic feature was introduced. This feature allows NBAR to scan TCP ports that are not well-known and identify HTTP traffic traversing these ports.

**Table 9** lists the TCP and UDP stateful protocols NBAR can classify. This table includes packets that require sub-port classification and classification based on deep packet inspection

**Table 9 TCP and UDP Stateful Protocols**

Protocol	Type	Description	Syntax	Cisco IOS Release <sup>1</sup>
Citrix ICA	TCP/ UDP	Citrix ICA traffic by application name	citrix citrix app	12.1(2)E 12.1(5)T
FTP	TCP	File Transfer Protocol	ftp	12.0(5)XE2 12.1(1)E 12.1(5)T
Exchange	TCP	MS-RPC for Exchange	exchange	12.0(5)XE2 12.1(1)E 12.1(5)T
FastTrack		FastTrack  For a list of common FastTrack applications, see the NBAR chapter of the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> , Release 12.3.	fasttrack	12.1(12c)E
Gnutella	TCP	Gnutella  For a list of common Gnutella applications, see the NBAR chapter of the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> , Release 12.3.	gnutella	12.1(12c)E

**Table 9** TCP and UDP Stateful Protocols (continued)

Protocol	Type	Description	Syntax	Cisco IOS Release <sup>1</sup>
HTTP	TCP	HTTP with URL, MIME, or host classification	http	12.0(5)XE2 12.1(1)E 12.1(5)T (HTTP host classification is not available on the 12.0 XE release train)
Napster	TCP	Napster traffic	napster	12.1(5)T
Netshow	TCP/ UDP	Microsoft Netshow	netshow	12.0(5)XE2 12.1(1)E 12.1(5)T
r-commands	TCP	rsh, rlogin, rexec	rcmd	12.0(5)XE2 12.1(1)E 12.1(5)T
RealAudio	TCP/ UDP	RealAudio Streaming Protocol	realaudio	12.0(5)XE2 12.1(1)E 12.1(5)T
RTP	TCP/ UDP	Real-Time Transport Protocol Payload Classification	rtp	12.2(8)T
SQL*NET	TCP/ UDP	SQL*NET for Oracle	sqlnet	12.0(5)XE2 12.1(1)E 12.1(5)T
StreamWorks	UDP	Xing Technology Stream Works audio and video	streamwork	12.0(5)XE2 12.1(1)E 12.1(5)T
SunRPC	TCP/ UDP	Sun Remote Procedure Call	sunrpc	12.0(5)XE2 12.1(1)E 12.1(5)T
TFTP	UDP	Trivial File Transfer Protocol	tftp	12.0(5)XE2 12.1(1)E 12.1(5)T
VDOLive	TCP/ UDP	VDOLive Streaming Video	vdolive	12.0(5)XE2 12.1(1)E 12.1(5)T

1. Indicates the Cisco IOS maintenance release that first supported the protocol. This table is updated when a protocol is added to a new Cisco IOS release train.

### Custom Protocols Created with the ip nbar custom Command

The *variable-field-name* value is used in conjunction with the **variable field-name field-length** options that are entered when you create a custom protocol using the **ip nbar custom** command. The variable option allows NBAR to match based on a specific value of a custom protocol. For instance, if **ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005** is entered to create a custom protocol, and then a class map using the **match protocol ftdd scid 804** is created, the created class map will match all traffic entering or leaving TCP ports 5001-5005 that have value “804” at byte 125.

Up to 24 variable values per custom protocol can be expressed in class maps. For instance, in the following configuration, 4 variables are used and 20 more “scid” values could be used.

```
ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005
```

```
class-map active-craft
match protocol ftdd scid 0x15
match protocol ftdd scid 0x21
```

```
class-map passive-craft
match protocol ftdd scid 0x11
match protocol ftdd scid 0x22
```

### Examples

The following example configures NBAR to match File Transfer Protocol (FTP) traffic:

```
match protocol ftp
```

In the following example, custom protocol ftdd is created using a variable. A class map matching this custom protocol based on the variable is also created. In this example, class map matchscidinftdd will match all traffic entering or leaving TCP ports 5001-5005 that has the value “804” at byte 125. The variable scid is 2 bytes in length.

```
ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005
```

```
class-map matchscidinftdd
match protocol ftdd scid 804
```

The same example above can also be done using hexadecimal values in the class map as follows:

```
ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005
```

```
class-map matchscidinftdd
match protocol ftdd scid 0x324
```

In the following example, the **variable** keyword is used while creating a custom protocol, and class maps are configured to classify different values within the variable field into different traffic classes.

Specifically, in the example below, variable scid values 0x15, 0x21, and 0x27 will be classified into class map active-craft while scid values 0x11, 0x22, and 0x25 will be classified into class map passive-craft.

```
ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005
```

```
class-map active-craft
match protocol ftdd scid 0x15
match protocol ftdd scid 0x21
match protocol ftdd scid 0x27
```

```
class-map passive-craft
match protocol ftdd scid 0x11
match protocol ftdd scid 0x22
match protocol ftdd scid 0x25
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.
<b>ip nbar custom</b>	Extends the capability of NBAR Protocol Discovery to classify and monitor additional static port applications, or allows NBAR to classify non-supported static port traffic.

# match protocol citrix

To configure network-based application recognition (NBAR) to match Citrix traffic, use the **match protocol citrix** command in class-map configuration mode. To disable NBAR from matching Citrix traffic, use the **no** form of this command.

```
match protocol citrix [app application-name-string]
```

```
no match protocol citrix [app application-name-string]
```

## Syntax Description

<b>app</b>	(Optional) Specifies matching of an application name string.
<i>application-name-string</i>	(Optional) Specifies string to be used as the subprotocol parameter.

## Defaults

No match criteria are specified.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.1(2)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was implemented on Catalyst 6000 family switches without FlexWAN modules.

## Usage Guidelines

Entering the **match protocol citrix** command without the **app** keyword establishes all Citrix traffic as successful match criteria.

## Examples

The following example configures NBAR to match all Citrix traffic:

```
match protocol citrix
```

The following example configures NBAR to match Citrix traffic with the application name of packet1:

```
match protocol citrix app packet1
```

# match protocol fasttrack

To configure network-based application recognition (NBAR) to match FastTrack peer-to-peer traffic, use the **match protocol fasttrack** command in class-map configuration mode. To disable NBAR from matching FastTrack traffic, use the **no** form of this command.

**match protocol fasttrack file-transfer** *“regular-expression”*

**no match protocol fasttrack file-transfer** *“regular-expression”*

Syntax Description	file-transfer	Indicates that a regular expression will be used to identify specific FastTrack traffic.
	<i>“regular-expression”</i>	The regular expression used to identify specific FastTrack traffic. For instance, entering “cisco” as the regular expression would classify the FastTrack traffic containing the string “cisco” as matches for the traffic policy.  To specify that all FastTrack traffic be identified by the traffic class, use “*” as the regular expression.

**Defaults** No default behavior or values.

**Command Modes** Class-map configuration

Command History	Release	Modification
	12.1(12c)E	This command was introduced.
	12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

**Usage Guidelines** To specify that all FastTrack traffic be identified by the traffic class, use “\*” as the regular expression. Some applications that use FastTrack include KaZaA, Grokster, and Morpheus (although newer versions of Morpheus use Gnutella).

---

**Examples**

The following example configures NBAR to match all FastTrack traffic:

```
match protocol fasttrack file-transfer ""
```

In the following example, all FastTrack files that have the “.mpeg” extension will be classified into class map nbar:

```
class-map match-all nbar  
match protocol fasttrack file-transfer "*.mpeg"
```

The following example configures NBAR to match FastTrack traffic that contains the string “cisco”:

```
match protocol fasttrack file-transfer "**cisco**"
```

# match protocol gnutella

To configure network-based application recognition (NBAR) to match Gnutella peer-to-peer traffic, use the **match protocol gnutella** command in class-map configuration mode. To disable NBAR from matching Gnutella traffic, use the **no** form of this command.

```
match protocol gnutella file-transfer "regular-expression"
```

```
no match protocol gnutella file-transfer "regular-expression"
```

Syntax Description	file-transfer	Indicates that a regular expression will be used to identify specific Gnutella traffic.
	"regular-expression"	The regular expression used to identify specific Gnutella traffic. For instance, entering "cisco" as the regular expression would classify the Gnutella traffic containing the string "cisco" as matches for the traffic policy.  To specify that all Gnutella traffic be identified by the traffic class, use "*" as the regular expression.

**Defaults** No default behavior or values.

**Command Modes** Class-map configuration

Command History	Release	Modification
	12.1(12c)E	This command was introduced.
	12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

**Usage Guidelines** To specify that all Gnutella traffic be identified by the traffic class, use "\*" as the regular expression. Applications that use Gnutella include the following:

- BearShare
- Gnewtellium
- Gnucleus
- Gtk-Gnutella
- JTella
- LimeWire
- Morpheus
- Mutella

- Phex
- Qtella
- Swapper
- XoloX
- XCache

---

**Examples**

The following example configures NBAR to match all Gnutella traffic:

```
match protocol gnutella file-transfer ""
```

In the following example, all Gnutella files that have the “.mpeg” extension will be classified into class map nbar:

```
class-map match-all nbar  
match protocol gnutella file-transfer "*.mpeg"
```

In the following example, only Gnutella traffic that contains the characters “cisco” is classified:

```
class-map match-all nbar  
match protocol gnutella file-transfer "*cisco*"
```

# match protocol http

To configure network-based application recognition (NBAR) to match Hypertext Transfer Protocol (HTTP) traffic by URL, HOST, or Multipurpose Internet Mail Extension (MIME)-type, use the **match protocol http** command in class-map configuration mode. To disable NBAR from matching HTTP traffic by URL, HOST, or MIME-type, use the **no** form of this command.

```
match protocol http [url url-string | host hostname-string | mime MIME-type]
```

```
no match protocol http [url url-string | host hostname-string | mime MIME-type]
```

Syntax Description	
<b>url</b>	(Optional) Specifies matching by a URL.
<i>url-string</i>	(Optional) User-specified URL of HTTP traffic to be matched.
<b>host</b>	(Optional) Specifies matching by a host name.
<i>hostname-string</i>	(Optional) User-specified host name to be matched.
<b>mime</b>	(Optional) Specifies matching by MIME text string.
<i>MIME-type</i>	(Optional) User-specified MIME text string to be matched.

**Defaults** No match criteria are specified.

**Command Modes** Class-map configuration

Command History	Release	Modification
	12.0(5)XE2	This command was introduced.
	12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
	12.1(2)E	The <i>hostname-string</i> argument was added.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
	12.1(13)E	This command was implemented on Catalyst 6000 family switches without FlexWAN modules.
	12.3(4)T	The NBAR Extended Inspection for HTTP Traffic feature was introduced. This feature allows NBAR to scan Transmission Control Protocol (TCP) ports that are not well-known and identify HTTP traffic traversing these ports.

**Usage Guidelines** In Cisco IOS Release 12.3(4)T, the NBAR Extended Inspection for HTTP Traffic feature was introduced. This feature allows NBAR to scan TCP ports that are not well-known and identify HTTP traffic traversing these ports. This feature is enabled automatically when a service policy containing the **match protocol http** command is attached to an interface.

When matching by MIME-type, the MIME-type can contain any user-specified text string. Refer to the the Internet Assigned Numbers Authority (IANA) web page ([www.iana.com](http://www.iana.com)) for a list of the IANA-registered MIME types.

When matching by MIME-type is performed, NBAR matches a packet containing the MIME-type and all subsequent packets until the next HTTP transaction.

When matching by HOST is performed, NBAR performs a regular expression match on the host field contents inside an HTTP packet and classifies all packets from that host.

HTTP URL matching supports GET, PUT, HEAD, POST, DELETE, and TRACE. When matching by URL, NBAR recognizes the HTTP packets containing the URL, and then matches all packets that are part of the HTTP request. When specifying a URL for classification, include only the portion of the URL following the www.hostname.domain in the match statement. For example, in the URL www.anydomain.com/latest/whatsnew.html include only /latest/whatsnew.html.

To match the www.anydomain.com portion, use the host name matching feature. The URL or host specification strings can take the form of a regular expression with options shown in [Table 10](#).

**Table 10** URL or HOST Specification String Options

Options	Description
*	Match any zero or more characters in this position.
?	Match any one character in this position.
	Match one of a choice of characters.
( )	Match one of a choice of characters in a range. For example, xyz.(gif   jpg) matches either xyz.gif or xyz.jpg.
[ ]	Match any character in the range specified, or one of the special characters. For example, [0-9] is all of the digits; [*] is the “*” character, and [[] is the “[” character.

## Examples

The following example classifies, within the class map called “class1,” HTTP packets based on any URL containing the string “whatsnew/latest” followed by zero or more characters:

```
class-map class1
match protocol http url whatsnew/latest*
```

The following example classifies, within the class map called “class2,” packets based on any host name containing the string “cisco” followed by zero or more characters:

```
class-map class2
match protocol http host cisco*
```

The following example classifies, within the class map called “class3,” packets based on the Joint Photographic Experts Group (JPEG) MIME type:

```
class-map class3
match protocol http mime “*jpeg”
```

# match protocol rtp

To configure network-based application recognition (NBAR) to match Real-Time Transfer Protocol (RTP) traffic, use the **match protocol rtp** command in class-map configuration mode. To disable NBAR from matching RTP traffic, use the **no** form of this command.

**match protocol rtp** [**audio** | **video** | **payload-type** *payload-string*]

**no match protocol rtp** [**audio** | **video** | **payload-type** *payload-string*]

## Syntax Description

<b>audio</b>	(Optional) Specifies matching by audio payload-type values in the range of 0 to 23. These payload-type values are reserved for audio traffic.
<b>video</b>	(Optional) Specifies matching by video payload-type values in the range of 24 to 33. These payload-type values are reserved for video traffic.
<b>payload-type</b>	(Optional) Specifies matching by a specific payload-type value, providing more granularity than is available with the <b>audio</b> or <b>video</b> keywords.
<i>payload-string</i>	(Optional) User-specified string that contains the specific payload-type values.  A <i>payload-string</i> argument can contain commas to separate payload-type values and hyphens to indicate a range of payload-type values. A <i>payload-string</i> argument can be specified in hexadecimal (prepend 0x to the value) and binary (prepend b to the value) notation in addition to standard number values.

## Defaults

No match criteria are specified.

## Command Modes

Class-map configuration

## Command History

Release	Modification
12.2(8)T	This command was introduced.
12.1(11b)E	This command was incorporated into the Cisco IOS Release 12.1(11b)E.
12.1(13)E	This command was implemented on Catalyst 6000 family switches without FlexWAN modules.

## Usage Guidelines

Entering the **match protocol rtp** command without any other keywords establishes all RTP traffic as successful match criteria.

RTP is a packet format for multimedia data streams. It can be used for media-on-demand as well as interactive services such as Internet telephony. RTP consists of a data and a control part. The control part is called Real-Time Transport Control Protocol (RTCP). It is important to note that the NBAR RTP Payload Classification feature does not identify RTCP packets and that RTCP packets run on odd-numbered ports while RTP packets run on even-numbered ports.

The payload type field of an RTP packet identifies the format of the RTP payload and is represented by a number. NBAR matches RTP traffic on the basis of this field in the RTP packet. A working knowledge of RTP and RTP payload types is helpful if you want to configure NBAR to match RTP traffic. For more information about RTP and RTP payload types, refer to RFC 1889, *RTP: A Transport Protocol for Real-Time Applications*.

---

**Examples**

The following example configures NBAR to match all RTP traffic:

```
class-map class1
  match protocol rtp
```

The following example configures NBAR to match RTP traffic with the payload-types 0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, and 64:

```
class-map class2
  match protocol rtp payload-type "0, 1, 4-0x10, 10001b-10010b, 64"
```

# match qos-group

To identify a specific quality of service (QoS) group value as a match criterion, use the **match qos-group** command in class-map configuration mode. To remove a specific QoS group value from a class map, use the **no** form of this command.

**match qos-group** *qos-group-value*

**no match qos-group** *qos-group-value*

<b>Syntax Description</b>	<i>qos-group-value</i>	Specifies the exact value from 0 to 99 used to identify a QoS group value.
---------------------------	------------------------	--

<b>Defaults</b>	No match criteria are specified.
-----------------	----------------------------------

<b>Command Modes</b>	Class-map configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.1 CC	This command was introduced.
	12.05(XE)	This command was incorporated into Cisco IOS Release 12.0(5)XE.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. This command can be used with the <b>random-detect discard-class-based</b> command.

<b>Usage Guidelines</b>	<p>The <b>match qos-group</b> command is used by the class map to identify a specific QoS group value marking on a packet. This command can also be used to convey the received Multiprotocol Label Switching (MPLS) experimental (EXP) field value to the output interface.</p>
-------------------------	--

The *qos-group-value* arguments are used as markings only. The QoS group values have no mathematical significance. For instance, the *qos-group-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *qos-group-value* of 2 is different than a packet marked with the *qos-group-value* of 1. The treatment of these packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

The QoS group value is local to the router, meaning that the QoS group value that is marked on a packet does not leave the router when the packet leaves the router. If you need a marking that resides in the packet, use IP precedence setting, IP differentiated services code point (DSCP) setting, or another method of packet marking.

<b>Examples</b>	<p>The following example shows how to configure the service policy called “priority50” and attach service policy “priority50” to an interface. In this example, the class map called “qosgroup5” will evaluate all packets entering Fast Ethernet interface 1/0/0 for a QoS group value of 5. If the incoming packet has been marked with the QoS group value of 5, the packet will be treated with a priority level of 50.</p>
-----------------	---

```
Router(config)# class-map qosgroup5
Router(config-cmap)# match qos-group 5
```

```

Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class qosgroup5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet1/0/0
Router(config-if)# service-policy output priority50

```

The following example shows that the packet named “qos-group 1” belongs to a particular class:

```
match qos-group 1
```

#### Related Commands

Command	Description
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.
<b>policy-map</b>	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
<b>service-policy</b>	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.
<b>set precedence</b>	Specifies an IP precedence value for packets within a traffic class.
<b>set qos-group</b>	Sets a group ID that can be used later to classify packets.

# match source-address mac

To use the source MAC address as a match criterion, use the **match source-address mac** command in class-map configuration mode. To remove a previously specified source MAC address as a match criterion in class-map configuration mode, use the **no** form of this command.

**match source-address mac** *address-destination*

**no match source-address mac** *address-destination*

<b>Syntax Description</b>	<i>address-destination</i>	Specifies the source destination MAC address to be used as a match criterion.
---------------------------	----------------------------	---

<b>Defaults</b>	No default behavior or values
-----------------	-------------------------------

<b>Command Modes</b>	Class-map configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(5)XE	This 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.	

<b>Usage Guidelines</b>	<p>This command can be used only on an input interface with a MAC address. These interfaces include Fast Ethernet and Ethernet interfaces.</p> <p>This command cannot be used on output interfaces with no MAC address, such as serial and ATM interfaces.</p>
-------------------------	--

<b>Examples</b>	The following example uses the MAC address mac 0.0.0 as a match criterion:
-----------------	--

```
class-map matchsrcmac
  match source-address mac 0.0.0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.

# max-reserved-bandwidth

To change the percent of interface bandwidth allocated for Resource Reservation Protocol (RSVP), class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PVC Interface Priority Queueing (PIPQ), use the **max-reserved-bandwidth** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**max-reserved-bandwidth** *percent*

**no max-reserved-bandwidth**

Syntax Description	<i>percent</i>	Percent of interface bandwidth allocated for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PIPQ.
--------------------	----------------	--

Defaults	75 percent
----------	------------

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

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

**Usage Guidelines**

The sum of all bandwidth allocation on an interface should not exceed 75 percent of the available bandwidth on an interface. The remaining 25 percent of bandwidth is used for overhead, including Layer 2 overhead, control traffic, and best-effort traffic.

If you need to allocate more than 75 percent for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PIPQ, you can use the **max-reserved-bandwidth** command. The *percent* argument specifies the maximum percentage of the total interface bandwidth that can be used.

**Examples**

In the following example, the policy map called `policy1` is configured for three classes with a total of 8 Mbps configured bandwidth, as shown in the output from the **show policy-map** command:

```
Router# show policy-map policy1

Policy Map policy1
  Weighted Fair Queueing
    Class class1
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
    Class class2
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
    Class class3
      Bandwidth 3000 (kbps) Max Threshold 64 (packets)
```

When you enter the **service-policy** command in an attempt to attach the policy map on a 10-Mbps Ethernet interface, an error message such as the following is produced:

```
I/f Ethernet1/1 class class3 requested bandwidth 3000 (kbps) Available only 2500 (kbps)
```

The error message is produced because the default maximum configurable bandwidth is 75 percent of the available interface bandwidth, which in this example is 7.5 Mbps. To change the maximum configurable bandwidth to 80 percent, use the **max-reserved-bandwidth** command in interface configuration mode, as follows:

```
max-reserved-bandwidth 80
service output policy1
end
```

To verify that the policy map was attached, enter the **show policy-map interface** command:

```
Router# show policy-map interface e1/1

Ethernet1/1 output :policy1
  Weighted Fair Queueing
    Class class1
      Output Queue:Conversation 265
      Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
      (discards/tail drops) 0/0
    Class class2
      Output Queue:Conversation 266
      Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
      (discards/tail drops) 0/0
    Class class3
      Output Queue:Conversation 267
      Bandwidth 3000 (kbps) Packets Matched 0 Max Threshold 64 (packets)
      (discards/tail drops) 0/0
```

### Virtual Template Configuration Example

The following example configures a strict priority queue in a virtual template configuration with CBWFQ. The **max-reserved-bandwidth** command changes the maximum bandwidth allocated between CBWFQ and IP RTP Priority from the default (75 percent) to 80 percent.

```
multilink virtual-template 1
interface virtual-template 1
  ip address 172.16.1.1 255.255.255.0
  no ip directed-broadcast
  ip rtp priority 16384 16383 25
  service-policy output policy1
  ppp multilink
  ppp multilink fragment-delay 20
  ppp multilink interleave
  max-reserved-bandwidth 80
end

interface Serial0/1
  bandwidth 64
  ip address 10.1.1.2 255.255.255.0
  no ip directed-broadcast
  encapsulation ppp
  ppp multilink
end
```



#### Note

To make the virtual access interface function properly, do not configure the **bandwidth** command on the virtual template. Configure it on the actual interface, as shown in the example.

Related Commands	Command	Description
	<b>bandwidth (policy-map class)</b>	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
	<b>ip rtp priority</b>	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
	<b>service-policy</b>	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.
	<b>show policy-map</b>	Displays the configuration of all classes comprising the specified service policy map or all classes for all existing policy maps.
	<b>show policy-map interface</b>	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.

# mpls experimental

To configure Multiprotocol Label Switching (MPLS) experimental (EXP) 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 **mpls experimental** command in `vc-class` configuration mode. To remove the MPLS EXP levels from the VC class, use the **no** form of this command.

To configure the MPLS EXP levels for a VC member of a bundle, use the **mpls experimental** command in `bundle-vc` configuration mode. To remove the MPLS EXP levels from the VC, use the **no** form of this command.

**mpls experimental** [*other* | *range*]

**no mpls experimental**

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

## Defaults

Defaults to **other**, that is, any MPLS EXP levels that are not explicitly configured.

## Command Modes

VC-class configuration (for a VC class)

Bundle-vc configuration (for ATM VC bundle members)

## Command History

Release	Modification
12.2(8)T	This command was introduced.

## Usage Guidelines

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

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

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

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

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

**Note**

If you are using an ATM interface, you must configure all MPLS EXP levels (ranging from 0 to 7) for the bundle. To do this, Cisco recommends configuring one member of the bundle with the **mpls experimental other** command. The **other** keyword defaults to any MPLS EXP levels in the range from 0 to 7 that are not explicitly configured.

**Examples**

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

```
vc-class atm control-class
  mpls experimental 7
```

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

```
pvc-bundle control-class 401
  mpls experimental 4-2
```

**Related Commands**

Command	Description
<b>bump</b>	Configures the bumping rules for a VC class that can be assigned to a VC bundle.
<b>bundle</b>	Creates a bundle or modifies an existing bundle to enter bundle configuration mode.
<b>class-vc</b>	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
<b>protect</b>	Configures a VC or PVC class with protected group or protected VC/PVC status for application to a VC/PVC bundle member.
<b>pvc-bundle</b>	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.
<b>ubr</b>	Configures UBR QoS and specifies the output PCR for an ATM PVC, PVC range, SVC, VC class, or VC bundle member.
<b>vbr-nrt</b>	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.
<b>vc-class atm</b>	Configures a VC class for an ATM VC or interface.