mac packet-classify

To classify Layer 3 packets as Layer 2 packets, use the **mac packet-classify** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

mac packet-classify [**bpdu**]

no mac packet-classify [**bpdu**]

Syntax Description

bpdu	(Optional) Specifies Layer 2 policy enforcement for BPDU packets.

Command Default

Layer 3 packets are not classified as Layer 2 packets.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	Added support for MAC ACLs on BPDU packets.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You can configure these interface types for multilayer MAC access control list (ACL) quality of service (QoS) filtering:

- VLAN interfaces without Layer 3 addresses
- Physical LAN ports that are configured to support Ethernet over Multiprotocol Label Switching (EoMPLS)
- Logical LAN subinterfaces that are configured to support EoMPLS

The ingress traffic that is permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering is processed by egress interfaces as MAC-layer traffic. You cannot apply egress IP ACLs to traffic that was permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering.

Microflow policing does not work on interfaces that have the **mac packet-classify** command enabled.

The **mac packet-classify** command causes the Layer 3 packets to be classified as Layer 2 packets and disables IP classification.

Traffic is classified based on 802.1Q class of service (CoS), trunk VLAN, EtherType, and MAC addresses.

Examples

This example shows how to classify incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# mac packet-classify
Router(config-if)#
```

This example shows how to disable the classification of incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# no mac packet-classify
Router(config-if)#
```

This example shows how to enforce Layer 2 policies on BPDU packets:

```
Router(config-if)# mac packet-classify bpdu
Router(config-if)#
```

This example shows how to disable Layer 2 policies on BPDU packets:

```
Router(config-if)# no mac packet-classify bpdu
Router(config-if)#
```

Related Commands

Command	Description
mac packet-classify use vlan	Enables VLAN-based QoS filtering in the MAC ACLs.

mac packet-classify use vlan

To enable VLAN-based quality of service (QoS) filtering in the MAC access control lists (ACLs), use the **mac packet-classify use vlan** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mac packet-classify use vlan

no mac packet-classify use vlan

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN-based QoS filtering in the MAC ACLs is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported in PFC3BXL or PFC3B mode only.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You must use the **no mac packet-classify use vlan** command to disable the VLAN field in the Layer 2 key if you want to apply QoS to the Layer 2 Service Advertising Protocol (SAP)-encoded packets (for example, Intermediate System-to-Intermediate System [IS-IS] and Internet Packet Exchange [IPX]).

QoS does not allow policing of non-Advanced Research Projects Agency (non-ARPA) Layer 2 packets (for example, IS-IS and IPX) if the VLAN field is enabled.

Examples

This example shows how to enable Layer 2 classification of IP packets:

```
Router(config)# mac packet-classify use vlan
Router(config)
```

This example shows how to disable Layer 2 classification of IP packets:

```
Router(config)# no mac packet-classify use vlan
Router(config)
```

Related Commands

Command	Description
mac packet-classify	Classifies Layer 3 packets as Layer 2 packets.

map ip

To classify either all the IPv4 packets, or the IPv4 packets based on either differentiated service code point (DSCP) values or precedence values into high priority or low priority for POS, channelized, and clear-channel SPAs, use the following forms of the **map ip** command in ingress-class-map configuration mode. Use the **no** forms of this command to remove the IPv4 settings.

Command to Classify all the IPv4 Packets

map ip all queue {**strict-priority** | **0**}

no map ip all queue {**strict-priority** | **0**}

Command to Classify IPv4 Packets Based on DSCP Values

map ip {**dscp-based** | **dscp** {*dscp-value* | *dscp-range*} **queue** {**strict-priority** | **0**}}

no map ip {**dscp-based** | **dscp** {*dscp-value* | *dscp-range*} **queue** {**strict-priority** | **0**}}

Command to Classify IPv4 Packets Based on Precedence Values

map ip {**precedence-based** | **precedence** {*precedence-value* | *precedence-range*} **queue strict-priority** | **0**}

no map ip {**precedence-based** | **precedence** {*precedence-value* | *precedence-range*} **queue strict-priority** | **0**}

Syntax Description

all queue	Implies the high priority or low priority configuration of all the IPv4 packets.
strict-priority	Classifies all the IPv4 packets as high priority (strict-priority).
0	Classifies all the IPv4 packets as low priority.
dscp-based	Enables classification based on DSCP value in IPv4.
dscp	Allows you to configure the DSCP value or range as high priority or low priority for IPv4 packets.
dscp-value	DSCP value for which the priority is to be configured as high or low.
dscp-range	Range of dscp-values for which the priority is to be configured as high or low.
queue	Enables the classification of an entire queue, DSCP values, or precedence values as high priority or low priority.
precedence-based	Enables the classification based on IPv4 precedence values.
precedence	Allows you to configure an IPv4 precedence value or range as high priority or low priority for IPv4 packets.
precedence-value	Precedence-value for which the priority is to be configured as high or low.
precedence-range	Range of precedence-values for which the priority is to be configured as high or low.

Defaults

If there is no configuration of IPv4 DSCP value or precedence values map to high priority specified, the system treats packets with DSCP range EF as high priority and precedence range 6-7 as high priority.

Command Modes

Ingress-class-map configuration mode (config-ing-class-map)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

To classify all IPv4 packets as high or low for POS, channelized, or clear-channel SPA, use the **map ip all queue** command,

To classify IPv4 packets with specific DSCP values, enable the DSCP classification using the **map ip dscp-based** command. To classify IPV4 packets with specific DSCP values as high or low, use the **map ip dscp** {{*dscp-value* | *dscp-range*} **queue** {**strict-priority** | **0**}} command.

To classify IPv4 packets with specific precedence values, enable the precedence classification using the **map ip precedence-based** command. To classify IPv4 packets with specific precedence values as high or low, use the **map ip precedence** {{*precedence-value* | *precedence-range*} **queue** {**strict-priority** | **0**}} command.

Examples

The following example shows how to classify all the IPv4 Packets as high priority using the **map ip all queue strict-priority** command:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip all queue strict-priority
```

The following example shows how to classify IPv4 Packets with DSCP value of cs1 as high priority:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip dscp-based
Router(config-ing-class-map)# map ip dscp cs1 queue strict-priority
```

The following example shows how to classify IPv4 Packets with a precedence value 3 and 5 as high priority:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip precedence-based
Router(config-ing-class-map)# map ip precedence 3 5 queue strict-priority
```

Related Commands

Command	Description
plim qos input class-map	Attaches the classification template to an interface.

map ipv6

To classify either all the IPv6 packets, or IPv6 packets based on specific traffic class (TC) values as high priority or low priority in the context of POS, channelized, and clear-channel SPAs use the following forms of **map ipv6** commands in ingress-class-map mode. Use the **no** forms of this command listed here to remove the IPv6 settings.

Command to Classify all the IPv6 Packets

map ipv6 all queue {**strict-priority** | **0**}

no map ipv6 all queue {**strict-priority** | **0**}

Command to Classify IPv6 Traffic-Class values as High Priority or Low Priority

map ipv6 {**tc** {*tc-value* | *tc-range*} **queue** {**strict-priority** | **0**}}

no map ipv6 {**tc** {*tc-value* | *tc-range*} **queue** {**strict-priority** | **0**}}

Syntax Description

all queue	Implies the high priority or low priority configuration of all the IPv6 packets.
strict-priority	Classifies all the IPv6 packets as high priority (strict-priority).
0	Classifies all the IPv6 Packets as low priority.
tc	Allows you to configure the traffic class value or range as high priority or low priority for IPv6 packets.
tc-value	Specific traffic-class value for which the priority is to be configured as either high or low(0).
tc-range	Range of traffic-class values for which the priority is to be configured as either high or low(0).
queue	Enables classification of the entire queue, traffic-class values, or range of traffic-class values as either high priority or low priority.

Defaults

If you do not configure which IPv6 traffic class values map to high priority, the system treats packets the packets with traffic class EF as high priority.

Command Modes

Ingress-class-map configuration mode (config-ing-class-map)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

To classify all the IPv6 packets as high priority or low priority in the context of POS, channelized, or clear-channel SPAs, use the **map ipv6 all queue** command.

To classify the IPv6 packets with specific traffic class values, use the **map ipv6 tc cs2 queue strict-priority** command.

Examples

The following example shows how to classify all the IPv6 packets as high priority using the **map ipv6 all queue strict-priority** command:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ipv6 all queue strict-priority
```

The following example shows how to classify the IPv6 packets with traffic-class values cs2 as high priority:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip tc cs2 queue strict-priority
```

Related Commands

Command	Description
plim qos input class-map	Attaches the classification template to an interface.

map mpls

To classify either all the Multiprotocol Label Switching (MPLS) packets or MPLS packets with specified EXP values or range as high priority or low priority for POS, channelized, and clear-channel SPAs the following forms of the **map mpls** command are used in ingress-class-map configuration mode. Use the **no** forms of this command listed here to remove the MPLS settings.

Command to Classify all the MPLS EXP Values as High Priority or Low Priority

map mpls all queue {**strict-priority** | **0**}

no map mpls all queue

Command to Classify the MPLS EXP Values as High Priority or Low Priority

map mpls exp {{*exp-value* | *exp-range*} **queue** {**strict-priority** | **0**}}

no map mpls exp {{*exp-value* | *exp-range*} **queue** {**strict-priority** | **0**}}

Syntax Description

all queue	Implies the high priority or low priority configuration of all the MPLS Packets.
strict-priority	Classifies either all the MPLS packets or the MPLS packets with specific EXP values as high priority (strict priority).
0	Classifies MPLS packets as low priority.
exp	Allows you to configure an EXP value or a range of EXP values as high priority or low priority for MPLS packets. The valid range for EXP values is 0 to 7.
exp-value	A specific EXP value for which the priority is to be configured as high or low(0).
exp-range	A range of EXP values for which the priority is to be configured as high or low (0). The valid range for EXP values is 0 to 7.
queue	Enables the classification priority of an entire queue, EXP values, or range of EXP values as high priority or low priority.

Defaults

If you do not configure which MPLS EXP values map to high priority, the system treats packets with an EXP value of 6-7 as high priority.

Command Modes

Ingress-class-map configuration mode (config-ing-class-map)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

To classify all the MPLS packets as high priority or low priority for POS, channelized, or clear-channel SPA, use the **map mpls all queue** command.

To classify the MPLS packets with specific EXP values, use the **map mpls exp** {*exp-value* | *exp-range*} **queue** {**strict-priority** | **0**} command.

Examples

The following example shows how to classify all the MPLS packets as high priority using the **map mpls all queue strict-priority** command:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map mpls all queue strict-priority
```

The following example shows how to classify the MPLS packets with EXP value of 4 as high priority:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map mpls exp 4 queue strict-priority
```

Related Commands

Command	Description
plim qos input class-map	Attaches the classification template to an interface.

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

access-group	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.
name *access-group-name*	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.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

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.
12.0(17)SL	This command was enhanced to include matching on access lists on the Cisco 10000 series router.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.4(6)T	This command was enhanced to support Zone-Based Policy Firewall.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

Note For Zone-Based Policy Firewall, this command is not applicable to CBWFQ.

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.

Supported Platforms Other than Cisco 10000 Series Routers

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**

Note Zone-Based Policy Firewall supports only the **match access-group**, **match protocol**, and **match class-map** commands.

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 you configure match criteria. For more information about the **access-list** command, refer to the *Cisco IOS IP Application Services Command Reference*.

Cisco 10000 Series Routers

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.

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 you configure match criteria.

Examples

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

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

```
The following example pertains to Zone-Based Policy Firewall. The example defines a class
map called c1 and configures the ACL numbered 144 to be used as the match criterion for
that class.
```

```
class-map type inspect match-all c1
 match access-group 144
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
class-map	Creates a class map to be used for matching packets to a specified class.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	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.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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

match atm-clp

To enable packet matching on the basis of the ATM cell loss priority (CLP), use the **match atm-clp** command in class-map configuration mode. To disable packet matching on the basis of the ATM CLP, use the **no** form of this command.

match atm-clp

no match atm-clp

Syntax Description

This command has no arguments or keywords.

Command Default

Packets are not matched on the basis of the ATM CLP.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SRC	Support for the Cisco 7600 series router was added.
12.4(15)T2	This command was integrated into Cisco IOS Release 12.4(15)T2.
12.2(33)SB	Support for the Cisco 7300 series router was added.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

This command is supported on policy maps that are attached to ATM main interfaces, ATM subinterfaces, or ATM permanent virtual circuits (PVCs). However, policy maps (containing the **match atm-clp** command) that are attached to these types of ATM interfaces can be *input* policy maps *only.*

This command is supported on the PA-A3 adapter *only.*

Examples

The following example shows how to create a class called "class-c1" using the **class-map** command, and the **match atm-clp** command has been configured inside that class. Therefore, packets are matched on the basis of the ATM CLP and are placed into this class:

```
Router> enable
Router# configure terminal
Router(config)# class-map class-c1
Router(config-cmap)# match atm-clp
Router(config-cmap)# end
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
show atm pvc	Displays all ATM PVCs and traffic information.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

match atm oam

To enable the control traffic classification on an ATM interface, use the **match atm oam** command in class-map configuration mode. To disable the control traffic classification, use the **no** form of this command.

match atm oam

no match atm oam

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.0(30)S	This command was introduced.

Usage Guidelines

Use this command for policy maps attached to ATM interfaces or ATM permanent virtual circuits (PVCs). Policy maps containing the **match atm oam** command attached to ATM interfaces or ATM PVCs can be input policy maps only.

Examples

The following example shows the control traffic classification being configured as the match criterion in a class map. The policy map containing this class map is then applied to the ATM interface.

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# class-map class-oam
Router(config-cmap)# match atm oam
Router(config-cmap)# exit
```

Related Commands

Command	Description
show class-map	Displays all class maps and their matching criteria.
show policy-map	Displays all policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified ATM interface or on a specific PVC on the interface.

match atm-vci

To enable packet matching on the basis of the ATM virtual circuit interface (VCI), use the **match atm-vci** command in class map configuration mode. To disable packet matching on the basis of the ATM VCI, use the **no** form of this command.

match atm-vci *vc-id* [**-***vc-id*]

no match atm-vci

Syntax Description

vc-id	The VC number assigned to the virtual circuit between two provider edge routers. You can specify one VC or a range of VCs.
-*vc-id*	(Optional) The second VC number, separated from the first by a hyphen. If two VC numbers are specified, the range is 32 to 65535.

Command Default

No match criteria are configured.

Command Modes

Class map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Release 2.3	This command was introduced.
12.2(33)SRE	This command was modified. This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

When you configure the **match atm-vci** command in class map configuration mode, you can add this class map to a policy map that can be attached only to an ATM permanent virtual path (PVP).

Note On the Cisco 7600 series router, the **match atm-vci** command is supported only in the ingress direction on an ATM VP.

You can use the **match not** command to match any VC except those you specify in the command.

Examples

The following example shows how to enable matching on VC ID 50:

```
Router(config)# class-map map1
Router(config-cmap)# match atm-vci 50
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match not	Specifies a single match criterion value to use as an unsuccessful match criterion.

match class-map

To use a traffic class as a classification policy, use the **match class-map** command in class-map or policy inline 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

class-map-name	Name of the traffic class to use as a match criterion.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)

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.
12.4(6)T	This command was enhanced to support Zone-Based Policy Firewall.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

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, do one of the following:

- Create a traffic class with the match-any instruction and use a class configured with the match-all instruction as a match criterion (using the **match class-map** command).
- Create a traffic class with the match-all instruction and use a class configured with the match-any instruction as a match criterion (using the **match class-map** command).

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.

When packets are matched to a class map, a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the 'inspect' action.

Examples

Non-Zone-Based Policy Firewall 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, you 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 you 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. Match criteria IP protocol *and* QoS group 4 are required in the definition of the traffic class named class3 and included as a possible match in the definition of the traffic class named class4 with the **match class-map class3** command.

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
class-map	Creates a class map to be used for matching packets to a specified class.

match cos

To match a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking, use the **match cos** command in class-map configuration mode. To remove a specific Layer 2 CoS/ISL marking as a match criterion, 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

Supported Platforms Other Than the Cisco 10000 Series Routers	
cos-value	Specific IEEE 802.1Q/ISL CoS value. The *cos-value* is from 0 to 7; up to four CoS values, separated by a space, can be specified in one **match cos** statement.
Cisco 10000 Series Routers	
cos-value	Specific packet CoS bit value. Specifies that the packet CoS bit value must match the specified CoS value. The *cos-value* is from 0 to 7; up to four CoS values, separated by a space, can be specified in one **match cos** statement.

Command Default

Packets are not matched on the basis of a Layer 2 CoS/ISL marking.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.0(25)S	This command was integrated into Cisco IOS Release 12.0(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was implemented on the Cisco 10000 series router.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	Support for the Cisco 7600 series router was added.
12.4(15)T2	This command was integrated into Cisco IOS Release 12.4(15)T2.
12.2(33)SB	Support for the Cisco 7300 series router was added.

Examples

In the following example, the CoS values of 1, 2, and 3 are successful match criteria for the interface that contains 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 the CoS-based-treatment policy map (in this case, the QoS treatment is priority 64 and bandwidth 512). The service policy configured in this example 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:

```
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
```

Related Commands

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

match cos inner

To match the inner cos of QinQ packets on a Layer 2 class of service (CoS) marking, use the **match cos inner** command in class-map configuration mode. To remove a specific Layer 2 CoS inner tag marking, use the **no** form of this command.

match cos *cos-value*

no match cos *cos-value*

Syntax Description

cos-value	Specific IEEE 802.1Q/ISL CoS value. The *cos-value* is from 0 to 7; up to four CoS values can be specified in one **match cos** statement.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

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

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

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
show class-map	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*

Syntax Description

address	Destination MAC address to be used as a match criterion.

Command Default

No destination MAC address is specified.

Command Modes

Class-map configuration (config-cmap)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.

match discard-class

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

match discard-class *class-number*

no match discard-class *class-number*

Syntax Description

class-number	Number of the discard class being matched. Valid values are 0 to 7.

Command Default

Packets will not be classified as expected.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A discard-class value has no mathematical significance. For example, the discard-class value 2 is not greater than 1. The value simply indicates that a packet marked with discard-class 2 should be treated differently than a packet marked with discard-class 1.

Packets that match the specified discard-class value are treated differently from packets marked with other discard-class values. The discard-class is a matching criterion only, used in defining per hop behavior (PHB) for dropping traffic.

Examples

The following example shows that packets in discard class 2 are matched:

```
Router(config-cmap)# match discard-class 2
```

Related Commands

Command	Description
set discard-class	Marks a packet with a discard-class value.

match dscp

To identify one or more differentiated service code point (DSCP), Assured Forwarding (AF), and Certificate Server (CS) values 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*

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets. **Note** For the Cisco 10000 series router, the **ip** keyword is required.
dscp-value	The DSCP value used to identify a DSCP value. For valid values, see the "Usage Guidelines."

Command Default

No match criteria is configured.

If you do not enter the **ip** keyword, matching occurs on both IPv4 and IPv6 packets.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **match ip dscp** command.
12.0(28)S	Support for this command in IPv6 was added in Cisco IOS Release S12.0(28)S on the
12.0(17)SL	This command was implemented on the Cisco 10000 series router.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Usage Guidelines

DSCP Values

You must enter one or more differentiated service code point (DSCP) values. The command may include any combination of the following:

- numbers (0 to 63) representing differentiated services code point values
- af numbers (for example, af11) identifying specific AF DSCPs
- cs numbers (for example, cs1) identifying specific CS DSCPs
- **default**—Matches packets with the default DSCP.
- **ef**—Matches packets with EF DSCP.

For example, if you wanted the DCSP 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 than a packet marked with the *dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of Quality of Service (QoS) policies in policy-map class configuration mode.

Match 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.

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 may be used with **match dscp** to classify only IPv4 packets.

After the DSCP bit is set, other QoS features can then operate on the bit settings.

The network can give priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data is then queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) can ensure that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Cisco 10000 Series Router

The Cisco 10000 series router supports DSCP matching of IPv4 packets only. You must include the **ip** keyword when specifying the DSCP values to use as match criterion.

You cannot use the **set ip dscp** command with the **set ip precedence** command to mark the same packet. DSCP and precedence values are mutually exclusive. A packet can have one value or the other, but not both.

Examples

The following example shows how to set multiple match criteria. In this case, two IP DSCP value and one AF value.

```
Router(config)# class-map map1
Router(config-cmap)# match dscp 1 2 af11
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match protocol ip	Matches DSCP values for packets.
match protocol ipv6	Matches DSCP values for IPv6 packets.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set dscp	Marks the DSCP value for packets within a traffic class.
show class-map	Displays all class maps and their matching criteria.

match field

To configure the match criteria for a class map on the basis of the fields defined in the protocol header description files (PHDFs), use the **match field** command in class-map configuration mode. To remove the specified match criteria, use the **no** form of this command.

match field *protocol protocol-field* {**eq** [*mask*] | **neq** [*mask*] | **gt** | **lt** | **range** *range* | **regex** *string*} *value* [**next** *next-protocol*]

no match field *protocol protocol-field* {**eq** [*mask*] | **neq** [*mask*] | **gt** | **lt** | **range** *range* | **regex** *string*} *value* [**next** *next-protocol*]

Syntax Description

protocol	Name of protocol whose PHDF has been loaded onto a router.
protocol-field	Match criteria is based upon the specified field within the loaded protocol.
eq	Match criteria is met if the packet is equal to the specified value or mask.
neq	Match criteria is met if the packet is not equal to the specified value or mask.
mask	(Optional) Can be used when the **eq** or the **neq** keywords are issued.
gt	Match criteria is met if the packet does not exceed the specified value.
lt	Match criteria is met if the packet is less than the specified value.
range *range*	Match criteria is based upon a lower and upper boundary protocol field range.
regex *string*	Match criteria is based upon a string that is to be matched.
value	Value for which the packet must be in accordance with.
next *next-protocol*	Specify the next protocol within the stack of protocols that is to be used as the match criteria.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

Before issuing the **match-field** command, you must load a PHDF onto the router via the **load protocol** command. Thereafter, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Match criteria are defined via a start point, offset, size, value to match, and mask. A match can be defined on a pattern with any protocol field.

Examples

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf

class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp

class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp

class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030

class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030

class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030

policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop

policy-map type access-control fpm-udp-policy
 class blaster3
 drop

policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy

interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
load protocol	Loads a PHDF onto a router.
match start	Configures the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3).

match flow pdp

To specify a Packet Data Protocol (PDP) flow as a match criterion in a class map, use the **match flow pdp** command in class-map configuration mode. To remove a PDP flow as a match criterion, use the **no** form of this command.

match flow pdp

no match flow pdp

Syntax Description

This command has no arguments or keywords.

Command Default

A PDP flow is not specified as a match criterion.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.3(8)XU	This command was introduced.
12.3(11)YJ	This command was integrated into Cisco IOS Release 12.3(11)YJ.
12.3(14)YQ	This command was integrated into Cisco IOS Release 12.3(14)YQ.
12.3(14)YU	This command was integrated into Cisco IOS Release 12.3(14)YU.
12.4(2)XB	This command was integrated into Cisco IOS Release 12.4(2)XB.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

The **match flow pdp** command allows you to match and classify traffic on the basis of a PDP flow.

The **match flow pdp** command is included with the Flow-Based QoS for GGSN feature available with Cisco IOS Release 12.4(9)T. The Flow-Based QoS for GGSN feature is designed specifically for the Gateway General Packet Radio Service (GPRS) Support Node (GGSN).

Per-PDP Policing

The Flow-Based QoS for GGSN feature includes per-PDP policing (session-based policing).

The **match flow pdp** command (when used in conjunction with the **class-map** command, the **policy-map** command, the **police rate pdp** command, and the **service-policy** command) allows you to configure per-PDP policing (session-based policing) for downlink traffic on a GGSN.

Note the following points related to per-PDP policing:

- When using the **class-map** command to define a class map for PDP flow classification, do not use the **match-any** keyword.
- Per-PDP policing functionality requires that you configure Universal Mobile Telecommunications System (UMTS) quality of service (QoS). For information on configuring UMTS QoS, see the “Configuring QoS on the GGSN” section of the *Cisco GGSN Release 6.0 Configuration Guide*, Cisco IOS Release 12.4(2)XB.

- The policy map created to configure per-PDP policing cannot contain multiple classes within which only the **match flow pdp** command has been specified. In other words, if there are multiple classes in the policy map, the **match flow pdp** command must be used in conjunction with another match statement (for example, **match precedence**) in at least one class.

For More Information

For more information about the GGSN, along with the instructions for configuring the Flow-Based QoS for GGSN feature, see the *Cisco GGSN Release 6.0 Configuration Guide*, Cisco IOS Release 12.4(2)XB.

Note To configure the Flow-Based QoS for GGSN feature, follow the instructions in the section called "Configuring Per-PDP Policing."

For more information about the GGSN-specific commands, see the *Cisco GGSN Release 6.0 Command Reference*, Cisco IOS Release 12.4(2)XB.

Examples

The following example shows how to specify PDP flows as the match criterion in a class map named class-pdp:

```
class-map class-pdp
 match flow pdp
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match precedence	Identifies IP precedence values as match criteria.
police rate pdp	Configures PDP traffic policing using the police rate.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an interface.

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

dlci-number	Number of the DLCI associated with the packet.

Command Default

No DLCI number is specified.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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
show class-map	Displays all class maps and their matching criteria.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

match input vlan

To configure a class map to match incoming packets that have a specific virtual local area network (VLAN) ID, use the **match input vlan** command in class map configuration mode. To remove the matching of VLAN IDs, use the **no** form of this command.

match input vlan *input-vlan-list*

no match input vlan *input-vlan-list*

Syntax Description

input-vlan-list	One or more VLAN IDs to be matched. The valid range for VLAN IDs is from 1 to 4094, and the list of VLAN IDs can include one or all of the following: • Single VLAN IDs, separated by spaces. For example: 100 200 300 • One or more ranges of VLAN IDs, separated by spaces. For example: 1-1024 2000-2499

Command Default

By default, no matching is done on VLAN IDs.

Command Modes

Class map configuration

Command History

Release	Modification
12.2(18)SXE	This command was introduced for Cisco Catalyst 6500 series switches and Cisco 7600 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **match input vlan** command allows you to create a class map that matches packets with one or more specific VLAN IDs, as they were received on the input (ingress) interface. This enables hierarchical Quality of Service (HQoS) for Ethernet over MPLS (EoMPLS) Virtual Circuits (VC), allowing parent and child relationships between QoS class maps and policy maps. This in turn enables service providers to easily classify and shape traffic for a particular EoMPLS network.

In EoMPLS applications, the parent class map typically specifies the maximum bandwidth for all of the VCs in a specific EoMPLS network. Then the child class maps perform other QoS operations, such as traffic shaping, on a subset of this traffic.

Do not confuse the **match input vlan** command with the **match vlan** command, which is also a class-map configuration command.

- The **match vlan** command matches the VLAN ID on packets for the particular interface at which the policy map is applied. Policy maps using the **match vlan** command can be applied to either ingress or egress interfaces on the router, using the **service-policy** {**input** | **output**} command.
- The **match input vlan** command matches the VLAN ID that was on packets when they were received on the ingress interface on the router. Typically, policy maps using the **match input vlan** command are applied to egress interfaces on the router, using the **service-policy output** command.

The **match input vlan** command can also be confused with the **match input-interface vlan** command, which matches packets being received on a logical VLAN interface that is used for inter-VLAN routing.

Tip Because class maps also support the **match input-interface** command, you cannot abbreviate the **input** keyword when giving the **match input vlan** command.

Note The **match input vlan** command cannot be used only on Layer 2 LAN ports on FlexWAN, Enhanced FlexWAN, and Optical Service Modules (OSM) line cards.

Restrictions

The following restrictions apply when using the **match input vlan** command:

- You cannot attach a policy with **match input vlan t**o an interface if you have already attached a service policy to a VLAN interface (a logical interface that has been created with the **interface vlan** command).
- Class maps that use the **match input vlan** command support only the **match-any** option. You cannot use the **match-all** option in class maps that use the **match input vlan** command.
- If the parent class contains a class map with a **match input vlan** command, you cannot use a **match exp** command in a child class map.

Examples

The following example shows how to create a class map and policy map that matches packets with a VLAN ID of 1000. The policy map shapes this traffic to a committed information rate (CIR) value of 10 Mbps (10,000,000 bps). The final lines then apply this policy map to a specific gigabit Ethernet WAN interface:

```
Router# configure terminal
Router(config)# class-map match-any vlan1000
Router(config-cmap)# match input vlan 1000
Router(config-cmap)# exit
Router(config)# policy-map policy1000
Router(config-pmap)# class vlan1000
Router(config-pmap-c)# exit
Router(config-pmap)# shape average 10000000
Router(config-pmap)# interface GE-WAN 3/0
Router(config-if)# service-policy output policy1000
Router(config-if)#
```

The following example shows how to configure a class map to match VLAN IDs 100, 200, and 300:

```
Router# configure terminal
Router(config)# class-map match-any hundreds
Router(config-cmap)# match input vlan 100 200 300
Router(config-cmap)#
```

The following example shows how to configure a class map to match all VLAN IDs from 2000 to 2999 inclusive:

```
Router# configure terminal
Router(config)# class-map match-any vlan2000s
Router(config-cmap)# match input vlan 2000-2999
Router(config-cmap)#
```

The following example shows how to configure a class map to match both a range of VLAN IDs, as well as specific VLAN IDs:

```
Router# configure terminal
Router(config)# class-map match-any misc
Router(config-cmap)# match input vlan 1 5 10-99 2000-2499
Router(config-cmap)#
```

Related Commands

Command	Description
clear cef linecard	Clears Cisco Express Forwarding (CEF) information on one or more line cards, but does not clear the CEF information on the main route processor (RP). This forces the line cards to synchronize their CEF information with the information that is on the RP.
match qos-group	Identifies a specified QoS group value as a match criterion.
mls qos trust	Sets the trusted state of an interface, to determine which incoming QoS field on a packet, if any, should be preserved.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
show platform qos policy-map	Displays the type and number of policy maps that are configured on the router.

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

interface-name	Name of the input interface to be used as match criteria.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)

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.
12.0(17)SL	This command was enhanced to include matching on the input interface.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Supported Platforms Other Than Cisco 10000 Series Routers

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 experimental (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.

Cisco 10000 Series Routers

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

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.

Examples

The following example specifies a class map called ethernet1 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
class-map	Creates a class map to be used for matching packets to a specified class.
match access-group	Configures the match criteria for a class map based on the specified ACL.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	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) port as the match criterion, use the **match ip rtp** command in class-map configuration mode. To remove the RTP port match criterion, use the **no** form of this command.

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

no match ip rtp

Syntax Description

starting-port-number	The starting RTP port number. Values range from 2000 to 65535.
port-range	The RTP port number range. Values range from 0 to 16383.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 from the *starting-port-number* argument to the *starting-port-number* plus the *port-range* argument.

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 ethernet1 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
ip rtp priority	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
match access-group	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 or values of the experimental (EXP) field as a match criteria, use the **match mpls experimental** command in class-map configuration mode. To remove the EXP field match criteria from a class map, use the **no** form of this command.

match mpls experimental *number*

no match mpls experimental *number*

Syntax Description

number	EXP field value (any number from 0 through 7) to be used as a match criterion. You can specify multiple values, separated by a space (for example, 3 4 7).

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Supported Platforms Other Than the Cisco 10000 Series

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria such as input interfaces, access control lists (ACLs), protocols, quality of service (QoS) labels, and experimental (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 compared 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.

Cisco 10000 Series

This command is available only on the ESR-PRE1 module.

For CBWFQ, you define traffic classes based on match criteria such as input interfaces, ACLs, protocols, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

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.

Examples

The following example specifies a class map called ethernet1 and configures the Multiprotocol Label Switching (MPLS) experimental values of 1 and 2 to be used as the match criteria for this class:

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

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match access-group	Configures the match criteria for a class map based on the specified ACL.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental topmost	Matches the EXP value in the topmost label.
match protocol	Matches traffic by a particular protocol.
match qos-group	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 header, use the **match mpls experimental topmost** command in class-map configuration mode. To remove the EXP match criterion, use the **no** form of this command.

match mpls experimental topmost *number*

no match mpls experimental topmost *number*

Syntax Description

number	Multiprotocol Label Switching (MPLS) EXP field in the topmost label header. Valid values are 0 to 7.

Command Default

No EXP match criterion is configured for the topmost label header.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

You can enter this command on the input interfaces 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 header is matched:

```
Router(config-cmap)# match mpls experimental topmost 3
```

Related Commands

Command	Description
set mpls experimental topmost	Sets the MPLS EXP field value in the topmost MPLS label header at the input 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 QoS 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-criterion*

no match not *match-criterion*

Syntax Description

match-criterion	The match criterion value that is an unsuccessful match criterion. All other values of the specified match criterion will be considered successful match criteria.

Command Default

No default behavior or values

Command Modes

QoS class-map configuration (config-cmap)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **match not** command is used to specify a quality of service (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 QoS class-map configuration mode, the specified class will accept all QoS group values except 4 as successful match criteria.

Examples

The following example shows a traffic class in which 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
class-map	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

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

Command Default

The Layer 3 packet length in the IP header is not used as a match criterion.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was implemented on Cisco ASR 1000 series routers.

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.

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.

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 bytes and a maximum Layer 3 packet length of 300 bytes are viewed as meeting the match criteria.

```
Router> enable
Router# configure terminal
Router(config)# class-map match-all class1
Router(config-cmap)# match packet length min 100 max 300
Router(config-cmap)# end
```

Related Commands

Command	Description
show class-map	Displays all class maps and their matching criteria.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

match port-type

To match the access policy on the basis of the port for a class map, use the **match port-type** command in class-map configuration mode. To delete the port type, use the **no** form of this command.

match port-type {**routed** | **switched**}

no match port-type {**routed** | **switched**}

Syntax Description

routed	Matches the routed interface. Use this keyword if the class map has to be associated with only a routed interface.
switched	Matches the switched interface. Use this keyword if the class map has to be associated with only a switched interface.

Command Default

Access policy is not matched.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used because, on the basis of the port on which a user is connecting, the access policies that are applied to it can be different.

Examples

The following example shows that an access policy has been matched on the basis of the port for a class map:

```
Router(config-cmap)# match port-type routed
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match tag (class-map)	Specifies the tag to be matched for a tag type of class map.

match precedence

To identify IP precedence values to use as the match criterion, 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-criteria1* | *precedence-criteria2* | *precedence-criteria3* | *precedence-criteria4*}

no match [**ip**] **precedence** {*precedence-criteria1* | *precedence-criteria2* | *precedence-criteria3* | *precedence-criteria4*}

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IP and IPv6 packets. **Note** For the Cisco 10000 series router, the **ip** keyword is required.
precedence-criteria1 *precedence-criteria2* *precedence-criteria3* *precedence-criteria4*	Identifies the precedence value. You can enter up to four different values, separated by a space. See the "Usage Guidelines" for valid values.

Command Default

No match criterion is configured.

If you do not enter the **ip** keyword, matching occurs on both IPv4 and IPv6 packets.

Command Modes

Class-map configuration mode (config-cmap)

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **match ip precedence** command.
12.0(17)SL	This command was implemented on the Cisco 10000 series router.
12.0(28)S	Support for this command in IPv6 was added on the Cisco 12000 series Internet router.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Usage Guidelines

You can enter up to four matching criteria, as number abbreviation (0 to 7) or criteria names (critical, flash, and so on), in a single 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-criteria* numbers are not mathematically significant; that is, the *precedence-criteria* of 2 is not greater than 1. The way that these different packets are treated depends upon quality of service (QoS) policies, set in the policy-map configuration mode.

You can configure a QoS policy to include IP precedence marking for packets entering the network. Devices within your network can then use the newly marked IP precedence values to determine how to treat the packets. For example, class-based weighted random early detection (WRED) uses IP precedence values to determine the probability that a packet is dropped. You can also mark voice packets with a particular precedence. You can then configure low-latency queueing (LLQ) to place all packets of that precedence into the priority queue.

Matching Precedence for IPv6 and IPv4 Packets on the Cisco 10000 and 7600 Series Routers

On the Cisco 7600 Series and 10000 Series Routers, you set matching criteria based on precedence values for only IPv6 packets using the **match protocol** command with the **ipv6** keyword. Without that keyword, the precedence match defaults to match both IPv4 and IPv6 packets. You set matching criteria based on precedence values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets.

Precedence Values and Names

The following table lists all criteria conditions by value, name, binary value, and recommended use. You may enter up to four criteria, each separated by a space. Only one of the precedence values must be a successful match criterion. Table 9 lists the IP precedence values.

Table 9 IP Precedence Values

Precedence Value	Precedence Name	Binary Value	Recommended Use
0	routine	000	Default marking value
1	priority	001	Data applications
2	immediate	010	Data applications
3	flash	011	Call signaling
4	flash-override	100	Video conferencing and streaming video
5	critical	101	Voice
6	internet (control)	110	Network control traffic (such as routing, which is typically precedence 6)
7	network (control)	111	

Do not use IP precedence 6 or 7 to mark packets, unless you are marking control 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 fa1/0/0
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 fa1/0/0
Router(config-if)# service-policy input priority50
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match protocol	Configures the match criteria for a class map on the basis of a specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set ip precedence	Sets the precedence value in the IP header.
show class-map	Displays all class maps and their matching criteria, or a specified class map and its matching criteria.

match protocol

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

match protocol *protocol-name*

no match protocol *protocol-name*

Syntax Description

protocol-name	Name of the protocol (for example, bgp) used as a matching criterion. See the "Usage Guidelines" for a list of protocols supported by most routers.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)

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 this release. The IPv6 protocol was added to support matching on IPv6 packets.
12.0(28)S	Support was added for IPv6.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.2(18)SXE	Support for this command was added on the Supervisor Engine 720.
12.4(6)T	This command was modified. The Napster protocol was removed because it is no longer supported.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series router.

Release	Modification
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY. This command was modified to enhance Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.
12.4(20)T	This command was implemented on the Cisco 1700, Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, Cisco 3800, Cisco 7200, and Cisco 7300 routers.
Cisco IOS XE Release 2.2	This command was implemented on Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 3.1S	This command was modified. Support for more protocols was added.

Usage Guidelines

Supported Platforms Other Than Cisco 7600 Routers and Cisco 10000 Series Routers

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria protocols, access control lists (ACLs), input interfaces, quality of service (QoS) labels, and Experimental (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.

The **match protocol ipx** command matches packets in the output direction only.

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**

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 configure NBAR to match protocol types that are supported by NBAR traffic, use the **match protocol** (NBAR) command.

Cisco 7600 Routers

The **match protocol** command in QoS class-map configuration configures NBAR and sends all traffic on the port, both ingress and egress, to be processed in the software on the Multilayer Switch Feature Card 2 (MSFC2).

For CBWFQ, you define traffic classes based on match criteria like protocols, ACLs, input interfaces, QoS labels, and Multiprotocol Label Switching (MPLS) 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.

If you want to use the **match protocol** command, you must first enter the **class-map** command to specify the name of the class to which you want to establish the match criteria.

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.

This command can be used to match protocols that are known to the NBAR feature. For a list of protocols supported by NBAR, see the "Classification" part of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Cisco 10000 Series Routers

For CBWFQ, you define traffic classes based on match criteria including protocols, 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.

The **match protocol ipx** command matches packets in the output direction only.

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.

If you are matching NBAR protocols, use the **match protocol** (NBAR) command.

Match Protocol Command Restrictions (Catalyst 6500 Series Switches Only)

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed.

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. For this release and platform, note the following restrictions for using policy maps and **match protocol** commands:

- A single traffic class can be configured to match a maximum of 8 protocols or applications.
- Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

Supported Protocols

Table 10 lists the protocols supported by most routers. Some routers support a few additional protocols. For example, the Cisco 7600 router supports the aarp and decnet protocols, while the Cisco 7200 router supports the directconnect and pppoe protocols. For a complete list of supported protocols, see the online help for the **match protocol** command on the router that you are using.

Table 10 Supported Protocols

Protocol Name	Description
802-11-iapp	IEEE 802.11 Wireless Local Area Networks Working Group Internet Access Point Protocol
ace-svr	ACE Server/Propagation
aol	America-Online Instant Messenger
appleqtc	Apple QuickTime
arp*	IP Address Resolution Protocol (ARP)
bgp	Border Gateway Protocol
biff	Bliff mail notification
bootpc	Bootstrap Protocol Client

Table 10 Supported Protocols (continued)

Protocol Name	Description
bootps	Bootstrap Protocol Server
bridge*	bridging
cddbp	CD Database Protocol
cdp*	Cisco Discovery Protocol
cifs	CIFS
cisco-fna	Cisco FNATIVE
cisco-net-mgmt	cisco-net-mgmt
cisco-svcs	Cisco license/perf/GDP/X.25/ident svcs
cisco-sys	Cisco SYSMAINT
cisco-tdp	cisco-tdp
cisco-tna	Cisco TNATIVE
citrix	Citrix Systems Metaframe
citriximaclient	Citrix IMA Client
clns*	ISO Connectionless Network Service
clns_es*	ISO CLNS End System
clns_is*	ISO CLNS Intermediate System
clp	Cisco Line Protocol
cmns*	ISO Connection-Mode Network Service
cmp	Cluster Membership Protocol
compressedtcp*	Compressed TCP
creativepartnr	Creative Partner
creativeserver	Creative Server
cuseeme	CU-SeeMe desktop video conference
daytime	Daytime (RFC 867)
dbase	dBASE Unix
dbcontrol_agent	Oracle Database Control Agent
ddns-v3	Dynamic DNS Version 3
dhcp	Dynamic Host Configuration
dhcp-failover	DHCP Failover
directconnect	Direct Connect
discard	Discard port
dns	Domain Name Server lookup
dnsix	DNSIX Security Attribute Token Map
echo	Echo port
edonkey	eDonkey
egp	Exterior Gateway Protocol

Table 10 Supported Protocols (continued)

Protocol Name	Description
eigrp	Enhanced Interior Gateway Routing Protocol
entrust-svc-handler	Entrust KM/Admin Service Handler
entrust-svcs	Entrust sps/aaas/aams
exec	Remote Process Execution
exchange	Microsoft RPC for Exchange
fasttrack	FastTrack Traffic (KaZaA, Morpheus, Grokster, and so on)
fcip-port	FCIP
finger	Finger
ftp	File Transfer Protocol
ftps	FTP over TLS/SSL
gdoi	Group Domain of Interpretation
giop	Oracle GIOP/SSL
gnutella	Gnutella Version 2 Traffic (BearShare, Shareeza, Morpheus, and so on)
gopher	Gopher
gre	Generic Routing Encapsulation
gtpv0	GPRS Tunneling Protocol Version 0
gtpv1	GPRS Tunneling Protocol Version 1
h225ras	H225 RAS over Unicast
h323	H323 Protocol
h323callsigalt	H323 Call Signal Alternate
hp-alarm-mgr	HP Performance data alarm manager
hp-collector	HP Performance data collector
hp-managed-node	HP Performance data managed node
hsrp	Hot Standby Router Protocol
http	Hypertext Transfer Protocol
https	Secure Hypertext Transfer Protocol
ica	ica (Citrix)
icabrowser	icabrowser (Citrix)
icmp	Internet Control Message Protocol
ident	Authentication Service
igmpv3lite	IGMP over UDP for SSM
imap	Internet Message Access Protocol
imap3	Interactive Mail Access Protocol 3
imaps	IMAP over TLS/SSL
ip*	IP (version 4)
ipass	IPASS

Table 10 Supported Protocols (continued)

Protocol Name	Description
ipinip	IP in IP (encapsulation)
ipsec	IP Security Protocol (ESP/AH)
ipsec-msft	Microsoft IPsec NAT-T
ipv6*	IP (version 6)
ipx	IPX
irc	Internet Relay Chat
irc-serv	IRC-SERV
ircs	IRC over TLS/SSL
ircu	IRCU
isakmp	ISAKMP
iscsi	iSCSI
iscsi-target	iSCSI port
kazaa2	Kazaa Version 2
kerberos	Kerberos
l2tp	Layer 2 Tunnel Protocol
ldap	Lightweight Directory Access Protocol
ldap-admin	LDAP admin server port
ldaps	LDAP over TLS/SSL
llc2*	llc2
login	Remote login
lotusmtap	Lotus Mail Tracking Agent Protocol
lotusnote	Lotus Notes
mgcp	Media Gateway Control Protocol
microsoft-ds	Microsoft-DS
msexch-routing	Microsoft Exchange Routing
msnmsgr	MSN Instant Messenger
msrpc	Microsoft Remote Procedure Call
ms-cluster-net	MS Cluster Net
ms-dotnetster	Microsoft .NETster Port
ms-sna	Microsoft SNA Server/Base
ms-sql	Microsoft SQL
ms-sql-m	Microsoft SQL Monitor
mysql	MySQL
n2h2server	N2H2 Filter Service Port
ncp	NCP (Novell)
net8-cman	Oracle Net8 Cman/Admin

Table 10 Supported Protocols (continued)

Protocol Name	Description
netbios	Network Basic Input/Output System
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS Session Service
netshow	Microsoft Netshow
netstat	Variant of systat
nfs	Network File System
nntp	Network News Transfer Protocol
novadigm	Novadigm Enterprise Desktop Manager (EDM)
ntp	Network Time Protocol
oem-agent	OEM Agent (Oracle)
oracle	Oracle
oracle-em-vp	Oracle EM/VP
oraclenames	Oracle Names
orasrv	Oracle SQL*Net v1/v2
ospf	Open Shortest Path First
pad*	Packet assembler/disassembler (PAD) links
pcanywhere	Symantec pcANYWHERE
pcanywheredata	pcANYWHEREdata
pcanywherestat	pcANYWHEREstat
pop3	Post Office Protocol
pop3s	POP3 over TLS/SSL
pppoe	Point-to-Point Protocol over Ethernet
pptp	Point-to-Point Tunneling Protocol
printer	Print spooler/ldp
pwdgen	Password Generator Protocol
qmtp	Quick Mail Transfer Protocol
radius	RADIUS & Accounting
rcmd	Berkeley Software Distribution (BSD) r-commands (rsh, rlogin, rexec)
rdb-dbs-disp	Oracle RDB
realmedia	RealNetwork's Realmedia Protocol
realsecure	ISS Real Secure Console Service Port
rip	Routing Information Protocol
router	Local Routing Process
rsrb*	Remote Source-Route Bridging
rsvd	RSVD

Table 10 Supported Protocols (continued)

Protocol Name	Description
rsvp	Resource Reservation Protocol
rsvp-encap	RSVP ENCAPSULATION-1/2
rsvp_tunnel	RSVP Tunnel
rtc-pm-port	Oracle RTC-PM port
rtelnet	Remote Telnet Service
rtp	Real-Time Protocol
rtsp	Real-Time Streaming Protocol
r-winsock	remote-winsock
secure-ftp	FTP over Transport Layer Security/Secure Sockets Layer (TLS/SSL)
secure-http	Secured HTTP
secure-imap	Internet Message Access Protocol over TLS/SSL
secure-irc	Internet Relay Chat over TLS/SSL
secure-ldap	Lightweight Directory Access Protocol over TLS/SSL
secure-nntp	Network News Transfer Protocol over TLS/SSL
secure-pop3	Post Office Protocol over TLS/SSL
secure-telnet	Telnet over TLS/SSL
send	SEND
shell	Remote command
sip	Session Initiation Protocol
sip-tls	Session Initiation Protocol-Transport Layer Security
skinny	Skinny Client Control Protocol
sms	SMS RCINFO/XFER/CHAT
smtp	Simple Mail Transfer Protocol
snapshot	Snapshot routing support
snmp	Simple Network Protocol
snmptrap	SNMP Trap
socks	Sockets network proxy protocol (SOCKS)
sqlnet	Structured Query Language (SQL)*NET for Oracle
sqlserv	SQL Services
sqlsrv	SQL Service
sqlserver	Microsoft SQL Server
ssh	Secure shell
sshell	SSLshell
ssp	State Sync Protocol
streamwork	Xing Technology StreamWorks player
stun	cisco Serial Tunnel

Table 10 Supported Protocols (continued)

Protocol Name	Description
sunrpc	Sun remote-procedure call (RPC)
syslog	System Logging Utility
syslog-conn	Reliable Syslog Service
tacacs	Login Host Protocol (TACACS)
tacacs-ds	TACACS-Database Service
tarantella	Tarantella
tcp	Transport Control Protocol
telnet	Telnet
telnets	Telnet over TLS/SSL
tftp	Trivial File Transfer Protocol
time	Time
timed	Time server
tr-rsrb	cisco RSRB
tto	Oracle TTC/SSL
udp	User Datagram Protocol
uucp	UUCPD/UUCP-RLOGIN
vdolive	VDOLive streaming video
vofr*	Voice over Frame Relay
vqp	VLAN Query Protocol
webster	Network Dictionary
who	Who’s service
wins	Microsoft WINS
x11	X Window System
xdmcp	XDM Control Protocol
xwindows*	X-Windows remote access
ymsgr	Yahoo! Instant Messenger

* This protocol is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine.

Examples

The following example shows how to specify a class map called ftp and configures the ftp protocol as a match criterion:

```
Router(config)# class-map ftp
Router(config-cmap)# match protocol ftp
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
match access-group	Configures the match criteria for a class map based on the specified ACL.

Command	Description
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified value of the experimental field as a match criterion.
match precedence	Identifies IP precedence values as match criteria.
match protocol (NBAR)	Configures NBAR to match traffic by a protocol type known to NBAR.
match qos-group	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 that is 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

protocol-name	Particular protocol type that is known to NBAR. These known protocol types can be used to match traffic. For a list of protocol types that are known to NBAR, see Table 11 in “Usage Guidelines.”
variable-field-name	(Optional and usable only with custom protocols) Predefined variable that was created when you created a custom protocol. The value for the *variable-field-name* argument will match the *field-name* variable entered when you created the custom protocol using the **ip nbar custom** command.
value	(Optional and usable only with custom protocols) Specific value in the custom payload to match. A value can be entered along with a value for the *variable-field-name* argument only. The value can be expressed in decimal or hexadecimal format.

Command Default

Traffic is not matched by a protocol type that is known to NBAR.

Command Modes

Class map configuration (config-cmap)

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, and the *variable-field-name value* argument was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)T	This command was implemented on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.4(2)T	This command was modified to include support for additional protocols, such as the BitTorrent protocol.
12.4(4)T	This command was modified to include support for additional protocols, such as the Skype and DirectConnect protocols.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY. This command was modified to enhance NBAR functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine.
12.2(18)ZYA	This command was modified to integrate NBAR and Firewall Service Module (FWSM) functionality on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine and to recognize additional protocols as noted in Table 11 in "Usage Guidelines."
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.2(18)ZYA1	This command was modified to recognize additional protocols as noted in Table 11 in "Usage Guidelines."
Cisco IOS XE Release 2.3	This command was modified to recognize additional protocols as noted in Table 11 in "Usage Guidelines."
12.2(18)ZYA2	This command was modified to recognize additional protocols, such as the TelePresence protocol.
Cisco IOS XE Release 2.5	This command was modified to recognize additional protocols as noted in Table 11 in "Usage Guidelines."
12.2XN 12.4(24)T 12.4(24)MDA	This command was modified to recognize additional protocols as noted in Table 11 in "Usage Guidelines."

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-TCP IP protocols
- TCP and UDP protocols that use statically assigned port numbers
- TCP and UDP protocols that use statically assigned port numbers but still require stateful inspection
- TCP and UDP protocols that dynamically assign port numbers and therefore require stateful inspection

Table 11 lists the NBAR-supported protocols available in Cisco IOS software, sorted by category. The table also provides information about the protocol type, the well-known port numbers (if applicable), and the syntax for entering the protocol in NBAR. The table is modified as new protocols are added or supported by different releases.

Note Table 11 includes the NBAR-supported protocols available with the 12.2(18)ZY and 12.2(18)ZYA releases. Protocols included in the 12.2(18)ZY and 12.2(18)ZYA releases are supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine.

Table 11 NBAR-Supported Protocols

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Enterprise Application	Citrix ICA	TCP/ UDP	TCP: 1494, 2512, 2513, 2598 UDP: 1604	Citrix ICA traffic	citrix citrix app citrix ica-tag	12.1(2)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5
	Exchange[1]	TCP	135	MS-RPC for Exchange	exchange	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZY 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.5
	MAPI	TCP	135	Messaging Application Programming Interface	mapi	12.2(18)ZYA 12.2(18)ZYA1
	Novadigm	TCP/ UDP	3460–3465	Novadigm Enterprise Desktop Manager (EDM)	novadigm	12.1(2)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Oracle	TCP	1525	Oracle	ora-serv	Cisco IOS XE Release 2.3
	PCAnywhere	TCP/ UDP	TCP: 5631, 65301 UDP: 22, 5632	Symantic PCAnywhere	pcanywhere	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SAP	TCP	3300–3315 (sap-pgm. pdlm) 3200–3215 (sap-app. pdlm) 3600–3615 (sap-msg. pdlm)	Application server to application server traffic (sap-pgm.pdlm) Client to application server traffic (sap-app.pdlm) Client to message server traffic (sap-msg.pdlm)	sap	12.1E 12.2T 12.3 12.3T 12.2(18)ZYA1 Cisco IOS XE Release 2.5

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Routing Protocol	BGP	TCP/ UDP	179	Border Gateway Protocol	bgp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	EGP	IP	8	Exterior Gateway Protocol	egp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol	eigrp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	OSPF	IP	89	Open Shortest Path First	ospf	12.3(8)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	RIP	UDP	520	Routing Information Protocol	rip	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
Database	CIFS	TCP	139, 445	Common Internet File System	cifs	12.2(18)ZYA 12.2(18)ZYA1
	MS-SQLServer	TCP	1433	Microsoft SQL Server Desktop Videoconferencing	sqlserver	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1
	SQL-exec	TCP/ UDP	9088	SQL Exec	sqlexec	Cisco IOS XE Release 2.3
	SQL*NET	TCP/ UDP	1521	SQL*NET for Oracle	sqlnet	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Health	DiCom	TCP	Dynamically assigned	Digital Imaging and Communications in Medicine	dicom	12.2(18)ZYA 12.2(18)ZYA1
	HL7	TCP	Dynamically assigned	Health Level Seven	hl7	12.2(18)ZYA 12.2(18)ZYA1
Financial	FIX	TCP	Dynamically assigned	Financial Information Exchange	fix	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.5
Security and Tunneling	GRE	IP	47	Generic Routing Encapsulation	gre	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	IPINIP	IP	4	IP in IP	ipinip	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	IPsec	IP	50, 51	IP Encapsulating Security Payload/ Authentication-Header	ipsec	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	L2TP	UDP	1701	L2F/L2TP Tunnel	l2tp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	PPTP	TCP	1723	Point-to-Point Tunneling Protocol for VPN	pptp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SFTP	TCP	990	Secure FTP	secure-ftp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Security and Tunneling (continued)	SHTTP	TCP	443	Secure HTTP	secure-http	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3
	SIMAP	TCP/ UDP	585, 993	Secure IMAP	secure-imap	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SIRC	TCP/ UDP	994	Secure IRC	secure-irc	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SLDAP	TCP/ UDP	636	Secure LDAP	secure-ldap	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SNNTP	TCP/ UDP	563	Secure NNTP	secure-nntp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SOCKS	TCP	1080	Firewall Security Protocol	socks	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SPOP3	TCP/ UDP	995	Secure POP3	secure-pop3	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Security and Tunneling (continued)	SSH	TCP	22	Secured Shell	ssh	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	STELNET	TCP	992	Secure Telnet	secure-telnet	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
Network Management	ICMP	IP	1	Internet Control Message Protocol	icmp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SNMP	TCP/ UDP	161, 162	Simple Network Management Protocol	snmp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Syslog	UDP	514	System Logging Utility	syslog	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Network Mail Services	IMAP	TCP/ UDP	143, 220	Internet Message Access Protocol	imap	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Notes	TCP/ UDP	1352	Lotus Notes	notes	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	POP3	TCP/ UDP	110	Post Office Protocol	pop3	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3
	SMTP	TCP	25	Simple Mail Transfer Protocol	smtp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Directory	DHCP/ BOOTP	UDP	67, 68	Dynamic Host Configuration Protocol/Bootstrap Protocol	dhcp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1
	DNS	TCP/ UDP	53	Domain Name System	dns	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1
	Finger	TCP	79	Finger User Information Protocol	finger	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Kerberos	TCP/ UDP	88, 749	Kerberos Network Authentication Service	kerberos	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	LDAP	TCP/ UDP	389	Lightweight Directory Access Protocol	ldap	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Streaming Media	CU-SeeMe	TCP/ UDP	TCP: 7648, 7649 UDP: 24032	Desktop Video Conferencing	cuseeme	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1
	MGCP	TCP/ UDP	2427, 2428, 2727	Media Gateway Control Protocol	mgcp	12.2(18)ZYA1 12.3(7)T
	Netshow	TCP/ UDP	Dynamically assigned	Microsoft Netshow	netshow	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1
	RealAudio	TCP/ UDP	Dynamically assigned	RealAudio Streaming Protocol	realaudio	12.0(5)XE2 12.1(1)E 12.1(5)T
	RTSP	TCP/ UDP	Dynamically assigned	Real Time Streaming Protocol	rtsp	12.2(18)ZYA1 12.3(11)T Cisco IOS XE Release 2.1
	StreamWorks	UDP	Dynamically assigned	Xing Technology Stream Works Audio and Video	streamwork	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1
	VDOLive	TCP/ UDP	Static (7000) with inspection	VDOLive Streaming Video	vdolive	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1
	YouTube[2]	TCP	Both static (80) and dynamically assigned	Online Video-Sharing Website	youtube	12.2(18)ZYA 12.2(18)ZYA1

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Internet	FTP	TCP	Dynamically assigned	File Transfer Protocol	ftp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1
	Gopher	TCP/ UDP	70	Internet Gopher Protocol	gopher	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	HTTP	TCP	80[3]	Hypertext Transfer Protocol	http	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.5
	IRC	TCP/ UDP	194	Internet Relay Chat	irc	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	NNTP	TCP/ UDP	119	Network News Transfer Protocol	nntp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Telnet	TCP	23	Telnet Protocol	telnet	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1
	TFTP	UDP	Static (69) with inspection	Trivial File Transfer Protocol	tftp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Signaling	AppleQTC	TCP/ UDP	458	Apple Quick Time	appleqtc	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Chargen	TCP/ UDP	19	Character Generator	chargen	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	ClearCase	TCP/ UDP	371	Clear Case Protocol Software Informer	clearcase	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Corba	TCP/ UDP	683, 684	Corba Internet Inter-Orb Protocol (IIOP)	corba-iiop	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Daytime	TCP/ UDP	13	Daytime Protocol	daytime	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Doom	TCP/ UDP	666	Doom	doom	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Echo	TCP/ UDP	7	Echo Protocol	echo	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	IBM DB2	TCP/ UDP	523	IBM Information Management	ibm-db2	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	IPX	TCP/ UDP	213	Internet Packet Exchange	server-ipx	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	ISAKMP	TCP/ UDP	500	Internet Security Association and Key Management Protocol	isakmp	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Signaling (continued)	ISI-GL	TCP/ UDP	55	Interoperable Self Installation Graphics Language	isi-gl	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	KLogin	TCP	543	KLogin	klogin	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	KShell	TCP	544	KShell	kshell	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	LockD	TCP/ UDP	4045	LockD	lockd	12.2(18)ZYA Cisco IOS XE Release 2.3
	MSSQL	TCP	1433	Microsoft Structured Query Language (SQL) Server	mssql	Cisco IOS XE Release 2.3
	RSVP	UDP	1698, 1699	Resource Reservation Protocol	rsvp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
RPC	AOL-messenger	TCP	5190, 443	AOL Instant Messenger Chat Messages	aol-messenger	12.2(18)ZYA 12.2(18)ZYA1
	MSN-messenger	TCP	1863	MSN Messenger Chat Messages[4]	msn-messenger	12.2(18)ZYA 12.2(18)ZYA1
	NFS	TCP/ UDP	2049	Network File System	nfs	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1
	Sunrpc	TCP/ UDP	Dynamically assigned	Sun Remote Procedure Call	sunrpc	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5
	Yahoo-messenger	TCP	5050, 5101	Yahoo Messenger Chat Messages	yahoo-messenger	12.2(18)ZYA 12.2(18)ZYA1

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Non-IP and LAN/ Legacy	Microsoft-DS	TCP/ UDP	445	Microsoft Directory Services	microsoftds	12.2(18)ZYA 12.2(18)ZYA1
	NetBIOS	TCP/ UDP	137, 138, 139	NetBIOS over IP (MS Windows)	netbios	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Nickname	TCP/ UDP	43	Nickname	nickname	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	NPP	TCP/ UDP	92	Network Payment Protocol	npp	12.2(18)ZY 12.2(18)ZYA1 Cisco IOS XE Release 2.3
Miscellaneous	Cisco-phone[5]	UDP	5060	Cisco IP Phones and PC-Based Unified Communicators	cisco-phone	12.2(18)ZYA 12.2(18)ZYA1
	NTP	TCP/ UDP	123	Network Time Protocol	ntp	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	ORASRV	TCP	1525	ORASRV	ora-srv	12.2(18)ZYA 12.2(18)ZYA1
	Printer	TCP/ UDP	515	Printer	printer	12.1(2)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	r-commands	TCP	Dynamically assigned	rsh, rlogin, rexec	rcmd	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Miscellaneous (continued)	RCP	TCP/ UDP	469	Rate Control Protocol	rcp	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	RTelnet	TCP/ UDP	107	Remote Telnet Service	rtelnet	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	SQLExec	TCP/ UDP	9088	SQL Exec	sqlexec	12.2(18)ZYA 12.2(18)ZYA1
	Systat	TCP/ UDP	11	System Statistics	systat	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	TACACS	TCP/ UDP	49, 65	Terminal Access Controller Access Control System	tacacs	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Time	TCP/ UDP	37	Time	time	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	VNC	UDP	5800, 5900, 5901	Virtual Network Computing	vnc	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	Whois++	TCP/ UDP	63	Whois++	whois++	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	XDMCP	UDP	177	X Display Manager Control Protocol	xdmcp	12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	X Windows	TCP	6000–6003	X11, X Windows	xwindows	12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Voice	Google Talk VoIP	TCP/ UDP	Dynamically assigned	Google Talk VoIP Protocol	gtalk-voip	12.2XN 12.4(24)MDA
	H.323	TCP	Dynamically assigned	H.323 Teleconferencing Protocol	h323	12.3(7)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3
	MSN VoIP	UDP	Dynamically assigned	MSN Messenger Protocol	msn-voip	12.4(24)T 12.4(24)MDA
	RTCP	TCP/ UDP	Dynamically assigned	Real-Time Control Protocol	rtcp	12.1E 12.2T 12.2(18)ZYA1 12.3 12.3T
	RTP	TCP/ UDP	Dynamically assigned	Real-Time Transport Protocol Payload Classification	rtp	12.2(8)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5
	SCCP/Skinny	TCP	2000, 2001, 2002	Skinny Client Control Protocol	skinny	12.2(18)ZYA1 12.3(7)T
	SIP	TCP/ UPD	5060	Session Initiation Protocol	sip	12.3(7)T Cisco IOS XE Release 2.1 12.2(18)ZYA1 Cisco IOS XE Release 2.3
	STUN	UDP	Dynamically assigned	Simple Traversal of UDP through NAT (STUN)	stun-nat	12.4(24)T 12.4(24)MDA
	Skype[6]	TCP/ UDP	Dynamically assigned	Peer-to-Peer VoIP Client Software	skype	12.2(18)ZYA1 12.4(4)T Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.5
	TelePresence	TCP/ UDP	Dynamically assigned	Cisco TelePresence System	telepresence-media telepresence-control	12.2(18)ZYA2
	Yahoo VoIP	TCP/ UDP	Dynamically assigned	Yahoo Messenger VoIP Protocol	yahoo-voip	12.4(24)T 12.4(24)MDA

Table 11 NBAR-Supported Protocols (continued)

Category	Protocol	Type	Well-Known Port Number	Description	Syntax	Cisco IOS Release
Peer-to-Peer File-Sharing Applications	BitTorrent	TCP	Dynamically Assigned or 6881–6889	BitTorrent File Transfer Traffic	bittorrent	12.2(18)ZYA1 12.4(2)T Cisco IOS XE Release 2.5
	Direct Connect	TCP/ UDP	411	Direct Connect File Transfer Traffic	directconnect	12.2(18)ZYA1 12.4(4)T Cisco IOS XE Release 2.5
	eDonkey/eMule	TCP	4662	eDonkey File-Sharing Application eMule traffic is also classified as eDonkey traffic in NBAR.	edonkey	12.2(18)ZYA1 12.3(11)T Cisco IOS XE Release 2.5
	FastTrack	N/A	Dynamically Assigned	FastTrack	fasttrack	12.1(12c)E 12.2(18)ZYA1 Cisco IOS XE Release 2.5
	Gnutella	TCP	Dynamically Assigned	Gnutella	gnutella	12.1(12c)E 12.2(18)ZYA1 Cisco IOS XE Release 2.5
	KaZaA	TCP/ UPD	Dynamically Assigned	KaZaA Note that earlier KaZaA version 1 traffic can be classified using FastTrack.	kazaa2	12.2(8)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5
	WinMX	TCP	6699	WinMX Traffic	winmx	12.2(18)ZYA1 12.3(7)T Cisco IOS XE Release 2.5

[1] For Release 12.2(18)ZYA and Cisco IOS XE Release 2.5 Cisco supports Exchange 03 and 07 only. MS client access is recognized, but web client access is not recognized.

[2] For Release 12.2(18)ZYA, access to YouTube via HTTP only is recognized.

[3] In 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 to identify HTTP traffic that is traversing these ports. For Cisco IOS XE Release 2.1, classification of HTTP traffic by URL or hostname is not supported. Cisco IOS XE Release 2.5 supports classification of HTTP traffic by URL or hostname.

[4] For Release 12.2(18)ZYA, messages (“chat”) from Yahoo, MSN, and AOL are recognized. Messages from Lotus and SameTime are not recognized. Video and voice from Instant Messaging are not recognized.

[5] For Release 12.2(18)ZYA, only SIP and Skinny telephone connections (cisco-phone traffic connections) are recognized. H.323 telephone connections are not recognized.

[6] Skype was introduced in Cisco IOS Release 12.4(4)T. As a result of this introduction, Skype is native in (included with) the Cisco IOS software and uses the NBAR infrastructure new to Cisco IOS Release 12.4(4)T. Cisco software supports Skype 1.0, 2.5, and 3.0. For Cisco IOS XE Release 2.1, Skype is supported in the TCP type only. Note that certain hardware platforms do not support Skype. For instance, Skype is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor/PISA engine. Cisco IOS XE Release 2.5 supports Skype in the TCP and UDP type.

Custom Protocols Created with the ip nbar custom Command

The *variable-field-name* argument 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 traffic on the basis of 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 that has the value "804" at byte 125 entering or leaving TCP ports 5001 to 5000.

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.

```
Router(config)# ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005
Router(config)# class-map active-craft
Router(config-cmap)# match protocol ftdd scid 0x15
Router(config-cmap)# match protocol ftdd scid 0x21

Router(config)# class-map passive-craft
Router(config-cmap)# match protocol ftdd scid 0x11
Router(config-cmap)# match protocol ftdd scid 0x22
```

match protocol Command Restrictions (Catalyst 6500 Series Switches Only)

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed.

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. For this release and platform, note the following restrictions for using policy maps and **match protocol** commands:

- A single traffic class can be configured to match a maximum of eight protocols or applications.
- Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

Examples

The following example shows how to configure NBAR to match FTP traffic:

```
Router(config-cmap)# match protocol ftp
```

The following example shows how to create a custom protocol called ftdd by 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 that has the value "804" at byte 125 entering or leaving TCP ports 5001 to 5005. The variable scid is 2 bytes in length:

```
Router(config)# ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005

Router(config)# class-map matchscidinftdd
Router(config-cmap)# match protocol ftdd scid 804
```

The following example shows that the command can also be written using hexadecimal values in the class map:

```
Router(config)# ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005

Router(config)# class-map matchscidinftdd
Router(config-cmap)# match protocol ftdd scid 0x324
```

The following example shows how to use the **variable** keyword while you create 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:

```
Router(config)# ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005

Router(config)# class-map active-craft
Router(config-cmap)# match protocol ftdd scid 0x15
Router(config-cmap)# match protocol ftdd scid 0x21
Router(config-cmap)# match protocol ftdd scid 0x27

Router(config)# class-map passive-craft
Router(config-cmap)# match protocol ftdd scid 0x11
Router(config-cmap)# match protocol ftdd scid 0x22
Router(config-cmap)# match protocol ftdd scid 0x25
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
ip nbar custom	Extends the capability of NBAR Protocol Discovery to classify and monitor additional static port applications, or allows NBAR to classify nonsupported 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*] [**ica-tag** *ica-tag-value*]

no match protocol citrix [**app** *application-name-string*] [**ica-tag** *ica-tag-value*]

Syntax Description

app	(Optional) Specifies matching of an application name string.
application-name-string	(Optional) Specifies the string to be used as the subprotocol parameter.
ica-tag	(Optional) Specifies tagging of Independent Computing Architecture (ICA) packets.
ica-tag-value	(Optional) Specifies the priority tag of ICA packets. Priority tag values can be in the range of 0 to 3.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)

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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.4(2)T	This command was modified to include the **ica-tag** keyword and the *ica-tag-value* argument.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

Entering the **match protocol citrix** command with the **ica-tag** keyword prioritizes Citrix ICA traffic. The priority tag values can be a number from 0 to 3, with 0 having the highest priority and 3 the lowest.

Examples

The following example shows how to configure NBAR to match all Citrix traffic:

```
match protocol citrix
```

The following example shows how to configure NBAR to match Citrix traffic with the application name of packet1:

```
match protocol citrix app packet1
```

The following example shows how to configure NBAR to give Citrix ICA traffic a priority of 1:

```
match protocol citrix ica-tag-1
```

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.
"*regular-expression***"**	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.

Command Default

NBAR is not configured to match FastTrack peer-to-peer traffic.

Command Modes

Class-map configuration (config-cmap)

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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To specify that all FastTrack traffic be identified by the traffic class, use "*" as the regular expression.

Applications that use FastTrack include KaZaA, Grokster, and Morpheus (although newer versions of Morpheus use Gnutella).

Examples

The following example shows how to configure NBAR to match all FastTrack traffic:

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

The following example shows how to classify all FastTrack files that have the “.mpeg” extension into class map nbar:

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

The following example shows how to configure 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.

Command Default

No behavior or values are predefined.

Command Modes

Class-map configuration (config-cmap)

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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 shows how to configure NBAR to match all Gnutella traffic:

```
match protocol gnutella file-transfer “*”
```

The following example shows how to classify all Gnutella files that have the “.mpeg” extension into class map nbar:

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

The following example shows how to classify only Gnutella traffic that contains the characters “cisco”:

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

match protocol http

To configure Network-Based Application Recognition (NBAR) to match HTTP traffic by URL, host, Multipurpose Internet Mail Extension (MIME) type, or fields in HTTP packet headers, use the **match protocol http** command in class-map configuration mode. To disable NBAR from matching HTTP traffic by URL, host, or MIME type, or fields in HTTP packet headers, use the **no** form of this command.

Cisco IOS Release 12.4(24)T and Earlier Releases, Cisco IOS Release 12.2(33)SRA, Cisco IOS Release 12.2(14)S and Later Releases

match protocol http [**url** *url-string* | **host** *hostname-string* | **mime** *MIME-type* | **c-header-field** *c-header-field-string* | **s-header-field** *s-header-field-string*]

no match protocol http [**url** *url-string* | **host** *hostname-string* | **mime** *MIME-type* | **c-header-field** *c-header-field-string* | **s-header-field** *s-header-field-string*]

Cisco IOS Release 15.1(2)T, Cisco IOS XE Release 3.1S and Later Releases and Catalyst 6500 Series Switch Equipped with the Supervisor 32/PISA Engine

match protocol http [**content-encoding** *content-encoding-name-string* | **from** *from-address-string* | **host** *hostname-string* | **location** *location-name-string* | **mime** *MIME-type* | **referer** *referer-address-string* | **server** *server-software-name-string* | **url** *url-string* | **user-agent** *user-agent-software-name-string*]

no match protocol http [**content-encoding** *content-encoding-name-string* | **from** *from-address-string* | **host** *hostname-string* | **location** *location-name-string* | **mime** *MIME-type* | **referer** *referer-address-string* | **server** *server-software-name-string* | **url** *url-string* | **user-agent** *user-agent-software-name-string*]

Syntax Description

url	(Optional) Specifies matching by a URL.
url-string	(Optional) User-specified URL of HTTP traffic to be matched.
host	(Optional) Specifies matching by a hostname.
hostname-string	(Optional) User-specified hostname to be matched.
mime	(Optional) Specifies matching by a MIME text string.
MIME-type	(Optional) User-specified MIME text string to be matched.
c-header-field	(Optional) Specifies matching by a string in the header field in HTTP client messages. **Note** HTTP client messages are often called HTTP request messages.
c-header-field-string	(Optional) User-specified text string within the HTTP client message (HTTP request message) to be matched.
s-header-field	(Optional) Specifies matching by a string in the header field in the HTTP server messages **Note** HTTP server messages are often called HTTP response messages.
s-header-field-string	(Optional) User-specified text within the HTTP server message (HTTP response message) to be matched.

Cisco IOS 15.1(2)T and Later Releases and Catalyst 6500 Series Switch Equipped with the Supervisor 32/PISA Engine	
content-encoding	(Optional) Specifies matching by the encoding mechanism used to package the entity body.
content-encoding-name-string	(Optional) User-specified content-encoding name.
from	(Optional) Specifies matching by the e-mail address of the person controlling the user agent.
from-address-string	(Optional) User-specified e-mail address.
location	(Optional) Specifies matching by the exact location of the resource from request.
location-name-string	(Optional) User-specified location of the resource.
referer	(Optional) Specifies matching by the address from which the resource request was obtained.
referer-address-name-string	(Optional) User-specified address of the referer resource.
server	(Optional) Specifies matching by the software used by the origin server handling the request.
server-software-name-string	(Optional) User-specified software name.
user-agent	(Optional) Specifies matching by the software used by the agent sending the request.
user-agent-software-name-string	(Optional) User-specified name of the software used by the agent sending the request.

Command Default

NBAR does not match HTTP traffic by URL, host, MIME type, or fields in HTTP packet headers.

Command Modes

Class-map configuration (config-cmap)

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	This command was modified to include the *hostname-string* argument.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command became available on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T, and the NBAR Extended Inspection for HTTP Traffic feature was introduced. This feature allows NBAR to scan TCP ports that are not well known and to identify HTTP traffic traversing these ports.
12.4(2)T	The command was integrated into Cisco IOS Release 12.4(2)T and was modified to include the **c-header-field** *c-header-field-string* and **s-header-field** *s-header-field-string* keywords and arguments.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)ZY2	This command was integrated into Cisco IOS Release 12.2(18)ZY2, and support was provided for the Catalyst 6500 series switch that is equipped with the Supervisor 32/PISA engine. **Note** For this Cisco IOS release and this platform, the **c-header-field** *c-header-field-string* and **s-header-field** *s-header-field-string* keywords and arguments are not available. To achieve the same functionality, use the individual keywords and arguments as shown in the syntax for the Catalyst 6500 series switch.
15.1(2)T	This command was modified. Support for the **c-header-field** *c-header-field-string* and **s-header-field** *s-header-field-string* keywords and arguments was removed. The **content-encoding**, **from**, **location**, **referrer**, and **user-agent** keywords and respective arguments were added.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

Classification of HTTP Traffic by Host, URL, or MIME

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 that 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. See the following web page for the IANA-registered MIME types:

http://www.iana.org/assignments/media-types/

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

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

HTTP client request matching supports GET, PUT, HEAD, POST, DELETE, OPTIONS, CONNECT, 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 that follows the www.*hostname.domain* in the **match** statement. For example, for the URL www.cisco.com/latest/whatsnew.html, include only /latest/whatsnew.html with the **match** statement (for instance, **match protocol http url /latest/whatsnew.html**).

Note For Cisco IOS Release 12.2(18)ZY2 (and later releases) on the Cisco Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA, up to 56 parameters or subclassifications per protocol per router can be specified with the **match protocol http** command. These parameters or subclassifications can be a combination of any of the available match choices, such as host matches, MIME matches, server matches, and URL matches. For other Cisco IOS releases and platforms, the maximum is 24 parameters or subclassifications per protocol per router.

To match the www.*anydomain*.com portion, use the hostname matching feature. The parameter specification strings can take the form of a regular expression with the following options.

Option	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 cisco.(gif | jpg) matches either cisco.gif or cisco.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.

Classification of HTTP Header Fields

In Cisco IOS Release 12.3(11)T, NBAR introduced expanded ability for users to classify HTTP traffic using information in the HTTP Header Fields.

HTTP works using a client/server model: HTTP clients open connections by sending a request message to an HTTP server. The HTTP server then returns a response message to the HTTP client (this response message is typically the resource requested in the request message from the HTTP client). After delivering the response, the HTTP server closes the connection and the transaction is complete.

HTTP header fields are used to provide information about HTTP request and response messages. HTTP has numerous header fields. For additional information on HTTP headers, see section 14 of RFC 2616: *Hypertext Transfer Protocol—HTTP/1.1*. This document can be read at the following URL:

http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

For request messages (client to server), the following HTTP header fields can be identified by using NBAR:

- User-Agent
- Referer

For response messages (server to client), the following header fields can be identified by using NBAR:

- Server
- Location
- Content-Encoding
- Content-Base

Note Use of the Content-Base field has not been implemented by the HTTP community. (See RFC 2616 for details.) Therefore, the Content-Base field is not identified by NBAR on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine.

Within NBAR, the **match protocol http c-header-field** command is used to specify request messages (the "c" in the **c-header-field** portion of the command is for client). The **match protocol http s-header-field** command is used to specify response messages (the "s" in the **s-header-field** portion of the command is for server).

It is important to note that combinations of URL, host, MIME type, and HTTP headers can be used during NBAR configuration. These combinations provide customers with more flexibility to classify specific HTTP traffic based on their network requirements.

Note For Cisco IOS Release 12.2(18)ZY2 and later releases on the Cisco Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA, and for Cisco IOS Release 15.1(2)T and later releases, the **c-header-field** and **s-header-field** keywords and associated arguments in the **match protocol http** command are not available.

Examples

The following example shows how to classify, within class map 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 shows how to classify, within class map class2, packets based on any hostname containing the string cisco followed by zero or more characters:

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

The following example shows how to classify, within class map class3, packets based on the JPEG MIME type:

```
class-map class3
 match protocol http mime "*jpeg"
```

In the following example, any response message that contains "gzip" in the Content-Base (if available), Content-Encoding, Location, or Server header fields will be classified by NBAR. Typically, the term "gzip" would be found in the Content-Encoding header field of the response message:

```
class-map class4
 match protocol http s-header-field "gzip"
```

The following example shows how to combine HTTP header fields with a URL to classify traffic. In this example, traffic with a User-Agent field of "CERN-LineMode/3.0" and a Server field of "CERN/3.0", along with URL "www.cisco.com/routers", will be classified using NBAR:

```
class-map match-all c-http
 match protocol http c-header-field "CERN-LineMode/3.0"
 match protocol http s-header-field "CERN/3.0"
 match protocol http url "www.cisco.com/routers"
```

Catalyst 6500 Series Router Equipped with a Supervisor 32/PISA Engine Example

In the following two examples, the individual keywords and associated arguments are used to specify traffic (instead of the **c-header-field** and the **s-header-field** keywords).

In the first example, the **user-agent**, **referrer**, and **from** keywords are specified. In the second example, the server, location, content-encoding keywords are specified:

```
class-map match-all test1
 match protocol http user-agent Mozilla
 match protocol http referrer *10.0.10.50"
 match protocol http from *example.com"

class-map match-all test2
 match protocol http server Apache
 match protocol http location *example.com"
 match protocol http content-encoding compress
 match protocol http match protocol http content-base *exmaple.com"
```

Related Commands

Command	Description
show ip nbar protocol-discovery	Displays the statistics gathered by the NBAR Protocol Discovery feature.

match protocol pppoe-discovery

To match and classify PPP over Ethernet (PPPoE) control packets that are sent to the control plane, use the **match protocol pppoe-discovery** command in class-map configuration mode. To remove this match criterion, use the **no** form of this command.

match protocol pppoe-discovery

no match protocol pppoe-discovery

Syntax Description

This command has no arguments or keywords.

Command Default

PPPoE control packets sent to the control plane are not matched or classified.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Release 2.3	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **match protocol pppoe-discovery** command is associated with control-plane-related features such as Control Plane Policing (CoPP).

When used in a class map, the **match protocol pppoe-discovery** command can classify either ingress PPPoE control-plane packets or egress PPPoE control-plane packets and include them in a specified traffic class. That class can then be configured in a policy map and can receive the desired quality of service (QoS) feature (such as traffic policing).

Examples

The following is an example of the **match protocol pppoe-discovery** command configured in a class-map called copplass-pppoe-discovery. PPPoE control-plane traffic identified as meeting the match criterion is placed in a class called coppclass-pppoe-discovery.

The coppclass-pppoe-discovery class is then configured in a policy map called copp-policy-pppoe-discovery, and the QoS traffic policing feature is applied using the **police** command.

```
Router> enable
Router# configure terminal
Router(config)# class-map match-all coppclass-pppoe-discovery
Router(config-cmap)# match protocol pppoe-discovery
Router(config-cmap)# exit
Router(config)# class-map match-all coppclass-pppoe-discovery
Router(config-cmap)# exit
Router(config)# policy-map copp-policy-pppoe-discovery
Router(config-pmap)# class coppclass-pppoe-discovery
Router(config-pmap-c)# police rate 8000 bps conform-action transmit exceed-action drop
Router(config-pmap-c)# end
```

Related Commands

Command	Description
control-plane	Enters control-plane configuration mode, which allows users to associate or modify attributes or parameters (such as a service policy) that are associated with the control plane of the device.
match protocol	Configures the match criterion for a class map on the basis of the specified protocol.
show policy-map control-plane	Displays the configuration and statistics for a traffic class or all traffic classes in the policy maps attached to the control plane for aggregate or distributed control-plane services.
show pppoe session	Displays information about currently active PPPoE sessions.

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

audio	(Optional) Specifies matching by audio payload-type values in the range of 0 to 23. These payload-type values are reserved for audio traffic.
video	(Optional) Specifies matching by video payload-type values in the range of 24 to 33. These payload-type values are reserved for video traffic.
payload-type	(Optional) Specifies matching by a specific payload-type value, providing more granularity than is available with the **audio** or **video** keywords.
payload-string	(Optional) User-specified string that contains the specific payload-type values. A *payload-string* argument can contain commas to separate payload-type values and hyphens to indicate a range of payload-type values. A *payload-string* 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.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.1(11b)E	This command was integrated into Cisco IOS Release 12.1(11b)E.
12.1(13)E	This command was implemented on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 shows how to configure NBAR to match all RTP traffic:

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

The following example shows how to configure 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*

Syntax Description

qos-group-value	The exact value from 0 to 99 used to identify a QoS group value.

Command Default

No match criterion is specified.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
11.1CC	This command was introduced.
12.05(XE)	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

The **match qos-group** 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.

The *qos-group-value* argument is used as a marking 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 QoS 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.

This command can be used with the **random-detect discard-class-based** command.

Examples

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.

```
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
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
random-detect discard-class-based	Bases WRED on the discard class value of a packet.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set precedence	Specifies an IP precedence value for packets within a traffic class.
set qos-group	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 QoS class-map configuration mode. To remove a previously specified source MAC address as a match criterion, use the **no** form of this command.

match source-address mac *address-destination*

no match source-address mac *address-destination*

Syntax Description

address-destination	The source destination MAC address to be used as a match criterion.

Command Default

No default behavior or values

Command Modes

QoS 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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command can be used only on an input interface with a MAC address, for example, Fast Ethernet and Ethernet interfaces.

This command cannot be used on output interfaces with no MAC address, such as serial and ATM interfaces.

Examples

The following example uses the MAC address mac 0.0.0 as a match criterion:

```
Router(config)# class-map matchsrcmac
Router(config-cmap)# match source-address mac 0.0.0
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.

match start

To configure the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3), use the **match start** command in class-map configuration mode. To remove the specified match criteria, use the **no** form of this command.

match start {**l2-start** | **l3-start**} **offset** *number* **size** *number*
{**eq** | **neq** | **gt** | **lt** | **range** *range* | **regex** *string*} {*value* [*value2*] | [*string*]}

no match start {**l2-start** | **l3-start**} **offset** *number* **size** *number*
{**eq** | **neq** | **gt** | **lt** | **range** *range* | **regex** *string*} {*value* [*value2*] | [*string*]}

Syntax Description

l2-start	Match criterion starts from the datagram header.
l3-start	Match criterion starts from the network header.
offset *number*	Match criterion can be made according to any aribitrary offset.
size *number*	Number of bytes in which to match.
eq	Match criteria is met if the packet is equal to the specified value or mask.
neq	Match criteria is met if the packet is not equal to the specified value or mask.
mask	(Optional) Can be used when the **eq** or the **neq** keywords are issued.
gt	Match criteria is met if the packet is greater than the specified value.
lt	Match criteria is met if the packet is less than the specified value.
range *range*	Match critera is based upon a lower and upper boundary protocol field range.
regex *string*	Match critera is based upon a string that is to be matched.
value	Value for which the packet must be in accordance with.

Defaults

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA).

Usage Guidelines

To the match criteria that is to be used for flexible packet matching, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. Thereafter, you can enter one of the following commands:

- **match-field** (which configures the match criteria for a class map on the basis of the fields defined in the protocol header description files [PHDFs])
- **match-start** (which can be used if a PHDF is not loaded onto the router)

Examples

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf

class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp

class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp

class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030

class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030

class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030

policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop

policy-map type access-control fpm-udp-policy
 class blaster3
 drop

policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy

interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.

Command	Description
load protocol	Loads a PHDF onto a router.
match field	Configures the match criteria for a class map on the basis of the fields defined in the PHDFs.

match tag (class-map)

To specify the tag to be matched for a tag type of class map, use the **match tag** command in class-map configuration mode. To delete the tag, use the **no** form of this command.

match tag *tag-name*

no match tag *tag-name*

Syntax Description

tag-name	Name of the tag.

Command Default

No match tags are defined.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The access control server (ACS) sends the tag attribute to the network access device (NAD) using the Cisco attribute-value (AV) pair. (The tag attribute can also be sent to the NAD using the IETF attribute 88.)

Examples

The following example shows that the tag to be matched is named "healthy":

```
Router(config)# class-map type tag healthy_class
Router(config-cmap)# match tag healthy
Router(config-cmap)# end
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.

match vlan (QoS)

To match and classify traffic on the basis of the virtual local-area network (VLAN) identification number, use the **match vlan** command in class-map configuration mode. To remove a previously specified VLAN identification number as a match criterion, use the **no** form of this command.

match vlan *vlan-id-number*

no match vlan *vlan-id-number*

Syntax Description

vlan-id-number	VLAN identification number, numbers, or range of numbers. Valid VLAN identification numbers must be in the range of 1 to 4095.

Command Default

Traffic is not matched on the basis of the VLAN identification number.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.2(31)SB2	This command was introduced for use on Cisco 10000 series routers only.

Usage Guidelines

Specifying VLAN Identification Numbers

You can specify a single VLAN identification number, multiple VLAN identification numbers separated by spaces (for example, 2 5 7), or a range of VLAN identification numbers separated by a hyphen (for example, 25-35).

Support Restrictions

The following restrictions apply to the **match vlan** command:

- The **match vlan** command is supported for IEEE 802.1q and Inter-Switch Link (ISL) VLAN encapsulations only.
- As of Cisco IOS Release 12.2(31)SB2, the **match vlan** command is supported on Cisco 10000 series routers only.

Examples

In the following sample configuration, the **match vlan** command is enabled to classify and match traffic on the basis of a range of VLAN identification numbers. Packets with VLAN identification numbers in the range of 25 to 50 are placed in the class called class1.

```
Router> enable
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match vlan 25-50
Router(config-cmap)# end
```

Note Typically, the next step would be to configure class1 in a policy map, enable a quality of service (QoS) feature (for example, class-based weighted fair queueing [CBWFQ]) in the policy map, and attach the policy map to an interface. To configure a policy map, use the **policy-map** command. To enable CBWFQ, use the **bandwidth** command (or use the command for the QoS feature that you want to enable). To attach the policy map to an interface, use the **service-policy** command. For more information about classifying network traffic on the basis of a match criterion, see the "Classification" part of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4T.

Related Commands

Command	Description
bandwidth (policy-map class)	Specify or modifies the bandwidth allocated for a class belonging to a policy map.
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces.
service-policy	Attached a policy map to an interface.

match vlan inner

To configure a class map to match the innermost VLAN ID in an 802.1q tagged frame, use the **match vlan inner** command in ATM interface configuration mode. To remove matching on the innermost VLAN ID of an 802.1q tagged frame, use the **no** form of this command.

match vlan inner *vlan-ids*

no match vlan inner *vlan-ids*

Syntax Description

vlan-ids	One or more VLAN IDs to be matched. The valid range for VLAN IDs is from 1 to 4095, and the list of VLAN IDs can include one or all of the following: • Single VLAN IDs, separated by spaces. For example: 100 200 300 • One or more ranges of VLAN IDs, separated by spaces. For example: 1-1024 2000-2499

Command Default

Packets are not matched on the basis of incoming dot1q VLAN inner IDs.

Command Modes

Class map configuration (config-cmap)

Command History

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF	This command was implemented on Cisco 7600 series routers.

Examples

The following example shows how to create a class map that matches packets with a VLAN IDs of 100 to 300.

```
Router(config)# class-map match-all vlan100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# class-map match-all vlan200
Router(config-cmap)# match vlan inner 200
Router(config-cmap)# exit
Router(config)# class-map match-all vlan300
Router(config-cmap)# match vlan inner 300
```

Related Commands

Command	Description
clear cef linecard	Clears Cisco Express Forwarding (CEF) information on one or more line cards, but does not clear the CEF information on the main route processor (RP). This forces the line cards to synchronize their CEF information with the information that is on the RP.
match qos-group	Identifies a specified QoS group value as a match criterion.
mls qos trust	Sets the trusted state of an interface to determine which incoming QoS field on a packet, if any, should be preserved.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
show platform qos policy-map	Displays the type and number of policy maps that are configured on the router.

maximum (local policy)

To set the limits for Resource Reservation Protocol (RSVP) resources, use the **maximum** command in local policy configuration mode. To delete the limits, use the **no** form of this command.

maximum [**bandwidth** [**group** | **single**] *bandwidth* | **senders** *maximum-senders*]

no maximum [**bandwidth** [**group** | **single**] | **senders**]

Syntax Description

bandwidth	(Optional) Indicates bandwidth limits for RSVP reservations.
group	(Optional) Specifies the amount of bandwidth, in kbps, that can be requested by all the reservations covered by a local policy.
single	(Optional) Specifies the maximum bandwidth, in kbps, that can be requested by any specific RSVP reservation covered by a local policy.
bandwidth	Maximum limit for the requested bandwidth, in kbps. Range is from 1 to 10000000.
senders	(Optional) Limits the number of RSVP senders affected by a local policy that can be active at the same time on a router.
maximum-senders	Maximum number of senders the specified policy allows. Range is from 1 to 50000; the default is 1000.

Command Default

No maximum bandwidth limit is set and no RSVP senders are configured.

Command Modes

Local policy configuration (config-rsvp-local-if-policy)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.4(6)T	This command was modified to apply to RESV messages.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

As part of the application ID enhancement, the **maximum bandwidth** command applies to RESV messages. This change has the following benefits:

- Allows the local policy bandwidth limit to be used by RSVP's admission control process for both shared and nonshared reservations. Releases that performed group bandwidth checks on PATH messages could not account for bandwidth sharing and, as a result, you had to account for sharing by creating a larger maximum group bandwidth for the policy.
- Allows a local policy to trigger preemption during the admission control function if there is insufficient policy bandwidth to meet the needs of an incoming RESV message.

Examples

The following example shows how to specify the maximum bandwidth for a group of reservations and for a single reservation, respectively:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 1/0
Router(config-if)# ip rsvp policy local identity video
Router(config-rsvp-local-policy)# maximum bandwidth group 500
Router(config-rsvp-local-policy)# maximum bandwidth single 50
```

Related Commands

Command	Description
ip rsvp policy local	Determines how to perform authorization on RSVP requests.

maximum bandwidth ingress

To configure the bandwidth parameters for the ingress policy pool, use the **maximum bandwidth ingress** command in local policy configuration mode or local policy interface configuration mode. To disable the bandwidth configuration for the ingress policy pool, use the **no** form of this command.

Command Syntax in Local Policy Configuration Mode

maximum bandwidth ingress {**group** | **single**} *bandwidth*

no maximum bandwidth ingress {**group** | **single**}

Command Syntax in Local Policy Interface Configuration Mode

maximum bandwidth ingress {**group** *bandwidth* | **percent** {**group** | **single**} *percent* | **single** *bandwidth*}

no maximum bandwidth ingress {**group** | **percent** {**group** | **single**} | **single**}

Syntax Description

group	Specifies the maximum ingress bandwidth, in kb/s, that can be requested by all the reservations covered by a local policy.
single	Specifies the maximum ingress bandwidth, in kb/s, that can be requested by any specific RSVP reservation covered by a local policy.
bandwidth	Maximum limit for the requested ingress bandwidth, in kb/s.
percent {**group** | **single**}	Specifies a percentage of the ingress bandwidth of an interface as the maximum bandwidth available to a group of flows or a single flow.
percent	Maximum limit for the requested bandwidth, in percent.

Command Default

RSVP is disabled by default; therefore, maximum bandwidth limit is not set.

Command Modes

Local policy configuration (config-rsvp-local-policy)
Local policy interface configuration (config-rsvp-local-if-policy)

Command History

Release	Modification
15.1(3)T	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

You can use the **maximum bandwidth ingress** command to configure the maximum bandwidth for a given policy. You can also configure a percentage of the RSVP ingress bandwidth of an interface as the maximum bandwidth available to a group of flows, or a single flow matching the policy. The percentages of the RSVP bandwidth to be configured as the maximum bandwidth are not available for global-based RSVP policies, but are available for interface RSVP policies.

The **maximum bandwidth ingress percent** command is mutually exclusive with the **maximum bandwidth ingress group** and **maximum bandwidth ingress single** commands. That is, if you configure the maximum percentage of RSVP ingress bandwidth using the **maximum bandwidth ingress percent** command, any configurations made using the **maximum bandwidth ingress group** and **maximum bandwidth ingress single** commands are removed.

Examples

The following example shows how to configure the maximum ingress bandwidth for a group of reservations and for a single reservation respectively, in a global-based RSVP policy:

```
Router> enable
Router# configure terminal
Router(config)# ip rsvp policy local identity rsvp-video
Router(config-rsvp-local-policy)# maximum bandwidth ingress group 200
Router(config-rsvp-local-policy)# maximum bandwidth ingress single 100
```

The following example shows how to configure the maximum percentage of RSVP ingress bandwidth of an interface for a group of reservations and for a single reservation, respectively:

```
Router> enable
Router# configure terminal
Router(config)# interface tunnel 0
Router(config-if)# ip rsvp policy local identity rsvp-video
Router(config-rsvp-local-if-policy)# maximum bandwidth ingress percent group 50
Router(config-rsvp-local-if-policy)# maximum bandwidth ingress single 50
```

Related Commands

Command	Description
show ip rsvp ingress	Displays information about the RSVP ingress bandwidth configured on interfaces.

maximum bandwidth percent

To configure the percentage of the Resource Reservation Protocol (RSVP) bandwidth of an interface as the maximum bandwidth available to a group of flows or a single flow, use the **maximum bandiwidth percent** command in local policy configuration mode. To disable this configuration, use the **no** form of this command.

maximum bandwidth percent {**group** | **single**} *bandwidth-percentage*

no maximum bandwidth percent {**group** | **single**}

Syntax Description

group	Specifies the amount of bandwidth, in kb/s, that can be requested by all the reservations covered by a local policy.
single	Specifies the maximum bandwidth, in kb/s, that can be requested by any specific RSVP reservation covered by a local policy.
bandwidth-percentage	Maximum limit for the requested bandwidth, in kb/s.

Command Default

RSVP is disabled by default; therefore, no percentage bandwidth is set.

Command Modes

Local policy configuration (config-rsvp-local-if-policy)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **maximum bandwidth percent** command is mutually exclusive with the **maximum bandwidth group** and **maximum bandwidth single** commands. That is, if you configure the maximum percentage of RSVP using the **maximum bandwidth percent** command, any configurations made using the **maximum bandwidth group** and **maximum bandwidth single** commands are removed. The **maximum bandwidth percent** command is not present in the global RSVP policy.

This maximum percentage of RSVP bandwidth configured for a group of flows is used to do RSVP Call Admission Control (CAC) for the flows matching with the policy. The **maximum bandwidth percent** command allows oversubscription. That is, you can configure more than 100 percent of the RSVP bandwidth as the maximum bandwidth for group reservations or as the maximum bandwidth for a single reservation.

Examples

The following example shows how to conifgure the maximum percentage of RSVP bandwidth of an interface for a group of reservations and for a single reservation, respectively:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 1/0
Router(config-if)# ip rsvp policy local identity video
Router(config-rsvp-local-policy)# maximum bandwidth percent group 50
Router(config-rsvp-local-policy)# maximum bandwidth single 50
```

Related Commands

Command	Description
ip rsvp policy local	Determines how to perform authorization on RSVP requests.
maximum (local policy)	Sets the limits for RSVP resources.

maximum header

To specify the maximum size of the compressed IP header, use the **maximum header** command in IPHC-profile configuration mode. To return the maximum size of the compressed IP header to the default size, use the **no** form of this command.

maximum header *number-of-bytes*

no maximum header

Syntax Description

number-of-bytes	The maximum header size, in bytes. Valid entries are numbers from 20 to 168. Default is 168.

Command Default

The maximum size of the compressed IP header is 168 bytes.

Command Modes

IPHC-profile configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **maximum header** command allows you to define the maximum size of the IP header of a packet to be compressed. Any packet with an IP header that exceeds the maximum size is sent uncompressed.

Use the *number-of-bytes* argument of the **maximum header** command to restrict the size of the IP header to be compressed.

Intended for Use with IPHC Profiles

The **maximum header** command is intended for use as part of an IPHC profile. An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the “Header Compression” module and the “Configuring Header Compression Using IPHC Profiles” module of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4T.

Prerequisite

Before using the **maximum header** command, you must enable either TCP header compression or non-TCP header compression. To enable TCP header compression, use the **tcp** command. To enable non-TCP header compression, use the **non-tcp** command.

Examples

The following is an example of an IPHC profile called profile2. In this example, the maximum size of the compressed IP header is set to 75 bytes.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# maximum header 75
Router(config-iphcp)# end
```

Related Commands

Command	Description
iphc-profile	Creates an IPHC profile.
non-tcp	Enables non-TCP header compression within an IPHC profile.
tcp	Enables TCP header compression within an IPHC profile.

max-reserved-bandwidth

Note Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **max-reserved bandwidth** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **max-reserved bandwidth** command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

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, Frame Relay PVC Interface Priority Queueing (PIPQ), or hierarchical queueing framework (HQF), 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

percent	Amount of interface bandwidth allocated for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, Frame Relay PIPQ, and HQF.

Command Default

75 percent on all supported platforms except the Cisco 7500 series routers, which do not have this restriction.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(20)T	Support was added for HQF using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). **Note** This is the last T release in which the command is supported.

Release	Modification
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

The **max-reserved-bandwidth** command is not supported in Cisco IOS Release 12.2SR or in 12.2SX. It is supported in 12.4T, but only up to the 12.4(20)T release in which HQF functionality was integrated.

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, Frame Relay PIPQ, or HQF, you can use the **max-reserved-bandwidth** command. The *percent* argument specifies the maximum percentage of the total interface bandwidth that can be used.

If you do use the **max-reserved-bandwidth** command, make sure that not too much bandwidth is taken away from best-effort and control traffic.

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
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
ip rtp priority	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
show policy-map	Displays the configuration of all classes comprising the specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

mls ip pbr

To enable the multilayer switching (MLS) support for policy-routed packets, use the **mls ip pbr** command in global configuration mode. To disable the MLS support for policy-routed packets, use the **no** form of this command.

mls ip pbr [**null0**]

no mls ip pbr

Syntax Description

null0	(Optional) Enables the hardware support for the interface null0 in the route-maps.

Command Default

MLS support for policy-routed packets is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17d)SXB	This command was introduced on the Supervisor Engine 2 and introduced into Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed to support the **null0** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Note Do not enable PBR and SLB on the same interface; PBR-based packets are not forwarded correctly.

When you enable the hardware-policy routing by entering the **mls ip pbr** command, all policy routing occurs in the hardware and is applied to all interfaces, regardless of which interface was configured for policy routing.

Use the **null0** keyword when you have routed traffic only to enable the hardware support for the **set interface null0** in the route maps.

Examples

This example shows how to enable the MLS support for policy-routed packets:

```
Router(config)# mls ip pbr
```

Related Commands

Command	Description
show tcam interface vlan acl	Displays information about the interface-based TCAM.