Classifying Network Traffic

Classifying network traffic allows you to organize traffic (that is, packets) into traffic classes or categories on the basis of whether the traffic matches specific criteria. Classifying network traffic is the foundation for enabling many quality of service (QoS) features on your network. This module contains conceptual information and the configuration tasks for classifying network traffic.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Classifying Network Traffic

Purpose of Classifying Network Traffic

Classifying network traffic allows you to see what kinds of traffic you have, organize traffic (that is, packets) into traffic classes or categories on the basis of whether the traffic matches specific criteria, and treat some types of traffic differently than others. Classifying network traffic is the foundation for enabling other QoS features such as traffic shaping and traffic policing on your network.

The goal of network traffic classification is to group traffic based on user-defined criteria so that the resulting groups of network traffic can then be subjected to specific QoS treatments. The QoS treatments might include faster forwarding by intermediate routers and switches or reduced probability of the traffic being dropped due to lack of buffering resources.

Identifying and categorizing network traffic into traffic classes (that is, classifying packets) enables distinct handling for different types of traffic, effectively separating network traffic into different categories. This classification can be associated with a variety of match criteria such as the IP Precedence value, differentiated services code point (DSCP) value, class of service (CoS) value, source and destination MAC addresses, input interface, or protocol type. You classify network traffic by using class maps and policy maps with the Modular Quality of Service Command-Line Interface (MQC). For example, you can configure class maps and policy maps to classify network traffic on the basis of the QoS group, Frame Relay DLCI number, Layer 3 packet length, or other criteria that you specify.

Restrictions for Classifying Network Traffic

- When access lists are used for classification in QoS policies, the following limitations are applicable:
  - The use of wildcards (For example, the any keyword, masks using zeros like 172.0.0.0, subnet masks) in source or destination addresses of permit or deny statements causes a greater consumption of memory on the device. This behavior is particularly important on devices that use software based classification (like Cisco ISR 4000 series devices or CSR1000v) and lower-end platforms with smaller memory capacities and ternary content-addressable memor (TCAMs).
  - The use of deny statements causes greater consumption of TCAM resources on systems that use HW-based classification (ASR1k).

Benefits of Classifying Network Traffic

Classifying network traffic allows you to see what kinds of traffic you have, organize the various kinds of network traffic into traffic classes, and treat some types of traffic differently than others. Identifying and organizing network traffic is the foundation for applying the appropriate QoS feature to that traffic, enabling you to allocate network resources to deliver optimal performance for different types of traffic. For example, high-priority network traffic or traffic matching specific criteria can be singled out for special handling, and thus, help to achieve peak application performance.

MQC and Network Traffic Classification

To configure network traffic classification, you use the Modular Quality of Service Command-Line Interface (MQC).

The MQC is a CLI structure that allows you to complete the following tasks:

- Specify the matching criteria used to define a traffic class.
- Create a traffic policy (policy map). The traffic policy defines the QoS policy actions to be taken for each traffic class.
- Apply the policy actions specified in the policy map to an interface, subinterface, or ATM permanent virtual circuit (PVC) by using the **service-policy** command.

Network Traffic Classification match Commands and Match Criteria

Network traffic classification allows you to group or categorize traffic on the basis of whether the traffic meets one or more specific criteria. For example, network traffic with a specific IP precedence can be placed into

one traffic class, while traffic with a specific DSCP value can be placed into another traffic class. The network traffic within that traffic class can be given the appropriate QoS treatment, which you can configure in a policy map later.

You specify the criteria used to classify traffic with a **match** command. The table below lists the available **match** commands and the corresponding match criterion.

Table 1: match Commands and Corresponding Match Criterion

match Commands[1]	Match Criterion
match access group	Access control list (ACL) number
match any	Any match criteria
match atm clp	ATM cell loss priority (CLP)
match class-map	Traffic class name
match cos	Layer 2 class of service (CoS) value
match destination-address mac	MAC address
match discard-class	Discard class value
match dscp	DSCP value
match field	Fields defined in the protocol header description files (PHDFs)
match fr-de	Frame Relay discard eligibility (DE) bit setting
match fr-dlci	Frame Relay data-link connection identifier (DLCI) number
match input-interface	Input interface name
match ip rtp	Real-Time Transport Protocol (RTP) port
match mpls experimental	Multiprotocol Label Switching (MPLS) experimental (EXP) value
match mpls experimental topmost	MPLS EXP value in the topmost label
match not	Single match criterion value to use as an unsuccessful match criterion
match packet length (class-map)	Layer 3 packet length in the IP header
match port-type	Port type
match precedence	IP precedence values
match protocol	Protocol type
match protocol (NBAR)	Protocol type known to network-based application recognition (NBAR)
match protocol citrix	Citrix protocol
match protocol fasttrack	FastTrack peer-to-peer traffic

match Commands[1]	Match Criterion
match protocol gnutella	Gnutella peer-to-peer traffic
match protocol http	Hypertext Transfer Protocol
match protocol rtp	RTP traffic
match qos-group	QoS group value
match source-address mac	Source Media Access Control (MAC) address
match start	Datagram header (Layer 2) or the network header (Layer 3)
match tag (class-map)	Tag type of class map
match vlan (QoS)	Layer 2 virtual local-area network (VLAN) identification number

[1] Cisco match commands can vary by release and platform. For more information, see the command documentation for the Cisco release and platform that you are using.

Traffic Classification Compared with Traffic Marking

Traffic classification and traffic marking are closely related and can be used together. Traffic marking can be viewed as an additional action, specified in a policy map, to be taken on a traffic class.

Traffic classification allows you to organize into traffic classes on the basis of whether the traffic matches specific criteria. For example, all traffic with a CoS value of 2 is grouped into one class, and traffic with a DSCP value of 3 is grouped into another class. The match criteria are user-defined.

After the traffic is organized into traffic classes, traffic marking allows you to mark (that is, set or change) an attribute for the traffic belonging to that specific class. For instance, you may want to change the CoS value from 2 to 1, or you may want to change the DSCP value from 3 to 2.

The match criteria used by traffic classification are specified by configuring a **match** command in a class map. The marking action taken by traffic marking is specified by configuring a **set** command in a policy map. These class maps and policy maps are configured using the MQC.

The table below compares the features of traffic classification and traffic marking.

Table 2: Traffic Classification Compared with Traffic Marking

Feature	Traffic Classification	Traffic Marking
Goal	Groups network traffic into specific traffic classes on the basis of whether the traffic matches the user-defined criterion.	After the network traffic is grouped into traffic classes, modifies the attributes for the traffic in a particular traffic class.
Configuration Mechanism	Uses class maps and policy maps in the MQC.	Uses class maps and policy maps in the MQC.

Feature	Traffic Classification	Traffic Marking
CLI	In a class map, uses **match** commands (for example, **match cos**) to define the traffic matching criteria.	Uses the traffic classes and matching criteria specified by traffic classification. In addition, uses **set** commands (for example, **set cos**) in a policy map to modify the attributes for the network traffic.

How to Classify Network Traffic

Creating a Class Map for Classifying Network Traffic

Note In the following task, the **matchfr-dlci**command is shown in Step 4. The **matchfr-dlci**command matches traffic on the basis of the Frame Relay DLCI number. The **matchfr-dlci**command is just an example of one of the **match** commands that can be used. For a list of other **match** commands, see the Network Traffic Classification match Commands and Match Criteria section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name* [**match-all**| **match-any**]
4. **match fr-dlci** *dlci-number*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** *class-map-name* [**match-all**| **match-any**] **Example:** `Router(config)# class-map class1`	Creates a class map to be used for matching traffic to a specified class, and enters class-map configuration mode. • Enter the class map name.

	Command or Action	Purpose
Step 4	**match fr-dlci** *dlci-number* **Example:** `Router(config-cmap)# match fr-dlci 500`	(Optional) Specifies the match criteria in a class map. **Note** The **matchfr-dlci** command classifies traffic on the basis of the Frame Relay DLCI number. The **matchfr-dlci**command is just an example of one of the **match** commands that can be used. For a list of other **match** commands, see the Network Traffic Classification match Commands and Match Criteria section.
Step 5	**end** **Example:** `Router(config-cmap)# end`	(Optional) Returns to privileged EXEC mode.

Creating a Policy Map for Applying a QoS Feature to Network Traffic

Note In the following task, the **bandwidth** command is shown at Step 5. The **bandwidth** command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature that you want to use.

Note Configuring bandwidth on policies that have the class-default class is supported on physical interfaces such as Gigabit Ethernet (GigE), Serial, Mobile Location Protocol (MLP), and Multilink Frame-Relay (MFR).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*bandwidth-kbps*| **remaining percent** *percentage*| **percent** *percentage*}
6. **end**
7. **show policy-map**
8.
9. **show policy-map** *policy-map* **class** *class-name*
10. Router# show policy-map
11.
12. Router# show policy-map policy1 class class1
13. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map policy1`	Specifies the name of the policy map to be created and enters policy-map configuration mode. • Enter the policy map name.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class class1`	Specifies the name of the class and enters policy-map class configuration mode. This class is associated with the class map created earlier. • Enter the name of the class or enter the **class-default**keyword.
Step 5	**bandwidth** {*bandwidth-kbps*| **remaining percent** *percentage*| **percent** *percentage*} **Example:** `Router(config-pmap-c)# bandwidth percent 50`	(Optional) Specifies or modifies the bandwidth allocated for a class belonging to a policy map. • Enter the amount of bandwidth as a number of kbps, a relative percentage of bandwidth, or an absolute amount of bandwidth. **Note** The **bandwidth** command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature that you want to use.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Returns to privileged EXEC mode.
Step 7	**show policy-map**	(Optional) Displays all configured policy maps.
Step 8		or
Step 9	**show policy-map** *policy-map* **class** *class-name* **Example:**	(Optional) Displays the configuration for the specified class of the specified policy map. • Enter the policy map name and the class name.

	Command or Action	Purpose
Step 10	Router# show policy-map	
Step 11		
Step 12	Router# show policy-map policy1 class class1	
Step 13	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

What to Do Next

Create and configure as many policy maps as you need for your network. To create and configure additional policy maps, repeat the steps in the "Creating a Policy Map for Applying a QoS Feature to Network Traffic" section. Then attach the policy maps to the appropriate interface, following the instructions in the "Attaching the Policy Map to an Interface" section.

Attaching the Policy Map to an Interface

Note Depending on the needs of your network, policy maps can be attached to an interface, a subinterface, or an ATM PVC.

Note A policy with the command **match fr-dlic** can only be attached to a Frame Relay main interface with point-to-point connections.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**name-tag**]
4. **pvc** [*name*] *vpi*/*vci* [**ilmi**|**qsaal**|**smds**| **l2transport**]
5. **exit**
6. **service-policy** {**input** | **output**}*policy-map-name*
7. **end**
8. **show policy-map interface** *type number*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [**name-tag**] **Example:** `Router(config)# interface serial4/0/0`	Configures an interface type and enters interface configuration mode. • Enter the interface type and number.
Step 4	**pvc** [*name*] *vpi/vci* [**ilmi**|**qsaal**|**smds**| **l2transport**] **Example:** `Router(config-if)# pvc cisco 0/16`	(Optional) Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters ATM virtual circuit configuration mode. • Enter the PVC name, the ATM network virtual path identifier, and the network virtual channel identifier. **Note** This step is required only if you are attaching the policy map to an ATM PVC. If you are not attaching the policy map to an ATM PVC, advance to .
Step 5	**exit** **Example:** `Router(config-atm-vc)# exit`	(Optional) Returns to interface configuration mode. **Note** This step is required only if you are attaching the policy map to an ATM PVC and you completed Step 4. If you are not attaching the policy map to an ATM PVC, advance to Step 6.
Step 6	**service-policy** {**input** | **output**}*policy-map-name* **Example:** `Router(config-if)# service-policy input policy1`	Attaches a policy map to an input or output interface. • Enter the policy map name. **Note** Policy maps can be configured on ingress or egress routers. They can also be attached in the input or output direction of an interface. The direction (input or output) and the router (ingress or egress) to which the policy map should be attached varies according your network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for your network configuration.

	Command or Action	Purpose
Step 7	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Step 8	**show policy-map interface** *type number*
	Example:
	`Router#`
	`show policy-map interface serial4/0/0`
		(Optional) Displays the traffic statistics of all traffic classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
		• Enter the type and number.

Step 9	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

Configuration Examples for Classifying Network Traffic

Example Creating a Class Map for Classifying Network Traffic

The following is an example of creating a class map to be used for traffic classification. In this example, a traffic class called class1 has been created. Traffic with a Frame Relay DLCI value of 500 will be put in this traffic class.

```
Router> enable

Router# configure terminal

Router(config)# class-map class1

Router(config-cmap)# match fr-dlci 500

Router(config-cmap)# end
```

Note This example uses the **matchfr-dlci** command. The **matchfr-dlci** command is just an example of one of the **match** commands that can be used. For a list of other **match** commands, see Network Traffic Classification match Commands and Match Criteria.

A policy with match fr-dlic can only be attached to a Frame Relay main interface with point-to-point connections.

Example Creating a Policy Map for Applying a QoS Feature to Network Traffic

The following is an example of creating a policy map to be used for traffic classification. In this example, a policy map called policy1 has been created, and the **bandwidth** command has been configured for class1. The **bandwidth** command configures the QoS feature CBWFQ.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# end
Router#
show policy-map policy1 class class1
Router# exit
```

Note This example uses the **bandwidth** command. The **bandwidth** command configures the QoS feature class-based weighted fair queuing (CBWFQ). CBWFQ is just an example of a QoS feature that can be configured. Use the appropriate command for the QoS feature that you want to use.

Example Attaching the Policy Map to an Interface

The following is an example of attaching the policy map to an interface. In this example, the policy map called policy1 has been attached in the input direction of serial interface 4/0.

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/0/0
Router(config-if)# service-policy input policy1
Router(config-if)# end
Router#
show policy-map interface serial4/0/0
Router# exit
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
MQC	"Applying QoS Features Using the MQC" module
Marking network traffic	"Marking Network Traffic" module

Related Topic	Document Title
IPsec and VPNs	"Configuring Security for VPNs with IPsec" module
NBAR	"Classifying Network Traffic Using NBAR" module
IPv6 QoS	“IPv6 Quality of Service” module
IPv6 MQC Packet Classification	“IPv6 QoS: MQC Packet Classification” module

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS XE Software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Classifying Network Traffic

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for Classifying Network Traffic

Feature Name	Releases	Feature Information
Packet Classification Using Frame Relay DLCI Number	12.2(13)T Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.12	The Packet Classification Using the Frame Relay DLCI Number feature allows customers to match and classify traffic based on the Frame Relay data-link connection identifier (DLCI) number associated with a packet. This new match criteria is in addition to the other match criteria, such as the IP Precedence, differentiated services code point (DSCP) value, class of service (CoS), currently available. The following commands were added or modified:**matchfr-dlci**
QoS: Local Traffic Matching Through MQC	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
QoS: Match ATM CLP	Cisco IOS XE Release 2.3	The QoS: Match ATM CLP features allows you to classify traffic on the basis of the ATM cell loss priority (CLP) value. The following command was introduced or modified: **matchatm-clp**.
QoS: MPLS EXP Bit Traffic Classification	Cisco IOS XE Release 2.3	The QoS: MPLS EXP Bit Traffic Classification feature allows you to classify traffic on the basis of the Multiprotocol Label Switching (MPLS) experimental (EXP) value. The following command was introduced or modified: **matchmplsexperimental**.