Configuring QoS Classification

This chapter contains the following sections:

- Information About Traffic Classes, page 1
- Criteria for Mapping Classes, page 2
- Prerequisites for Classification, page 3
- Guidelines and Limitations for QoS Classification, page 3
- Classifying Traffic, page 3
- Verifying the Classification Configuration, page 14
- Configuration Example for QoS Classification, page 14
- Feature History for QoS Classification, page 14

Information About Traffic Classes

Traffic classes, or categories of traffic (packets) that are grouped on the basis of similarity of traffic, are called class maps. Classifying network traffic allows you to enable a quality of service (QoS) strategy in your network.

Figure 1: Criteria for Classifying Network Traffic

Classification Criteria:
- CoS
- IP precedence
- Differentiated Services Code Point (DSCP)
- Layer 2 to Layer 4 parameters
- Packet length
- ACL
- QoS Group
Identifying and categorizing network traffic into traffic classes (that is, classifying packets) enables you to handle different types of traffic by separating network traffic into different categories.

Classifying network traffic allows you to see the kinds of traffic you have and treat some types of traffic differently than others. Identifying and organizing network traffic allows you to allocate network resources to deliver the best performance for each type of traffic.

You can place network traffic with a specific IP precedence into one traffic class, while you place traffic with a specific differentiated services code point (DSCP) value into another traffic class. Each traffic class can be given a different QoS class, which you configure in a policy map later.

You define each class of traffic in a class map based upon criteria, such as the IP precedence or class of service (CoS). The allowable criteria for mapping classes of traffic is available and you can match the criteria to your traffic as follows:

- Matching all
- Matching or not matching one
- Matching or not matching multiple
- Matching or not matching another class map

Some of the criteria used in traffic class maps relates only to one direction of traffic—either ingress or egress. For example, the internal label QoS group has no meaning on ingress traffic because it has not yet been assigned a value.

Traffic that fails to match any traffic class in a QoS policy map is assigned to a default class of traffic called class-default. The class-default can be referenced in a QoS policy map to select this unmatched traffic.

## Criteria for Mapping Classes

The allowable criteria for the mapping traffic classes are as follows:

<table>
<thead>
<tr>
<th>Class Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoS</td>
<td>Class of service (CoS) field in the IEEE 802.1Q header.</td>
</tr>
<tr>
<td>IP precedence</td>
<td>Precedence value within the type of service (ToS) byte of the IP header.</td>
</tr>
<tr>
<td></td>
<td>For details, see the <a href="#">IP Precedence Values</a> table.</td>
</tr>
<tr>
<td>Differentiated Services Code Point (DSCP)</td>
<td>DSCP value within the DiffServ field of the IP header. The standard DSCP values are listed in <a href="#">Commonly Used DSCP Values</a>.</td>
</tr>
<tr>
<td>QoS group</td>
<td>Locally significant QoS values that can be manipulated and matched within the system. The range is from 0 to 126.</td>
</tr>
<tr>
<td>Discard class</td>
<td>Locally significant values that can be matched and manipulated within the system. The range is from 0 to 63.</td>
</tr>
</tbody>
</table>
### Prerequisites for Classification

You are logged in to the CLI in EXEC mode.

### Guidelines and Limitations for QoS Classification

- You can specify a maximum of 32 match criteria in a class map.
- You can configure a maximum of 64 classes for use in a single policy map if no policers are configured.

**Note**

Tunneled IP packets are not matched unless the tunneling protocol is also IP, and then the match applies to the outer IP header and not the encapsulated IP header.

### Classifying Traffic

#### Classifying ACL Traffic

You can classify traffic by matching packets based on existing access control lists (ACLs).

---

<table>
<thead>
<tr>
<th>Class Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>IP access control list (ACL) or MAC ACL name. If you configure the class to match-all and ACL as match-criteria, no other match criteria, except the packet length, can be specified. If you configure the class to match-any and ACL as match-criteria, you can also match ACLs and any other match criteria.</td>
</tr>
<tr>
<td>Packet length</td>
<td>Size range of Layer 3 packet lengths.</td>
</tr>
<tr>
<td>IP RTP</td>
<td>Applications that are using the Real-time Transport Protocol (RTP) are identified by UDP port number range.</td>
</tr>
<tr>
<td>Class map</td>
<td>Criteria that are specified in a named class-map object.</td>
</tr>
</tbody>
</table>
Before You Begin

- QoS does not use the permit-deny functions of ACLs. The **permit** and **deny** ACL keywords are ignored when matching.
- QoS does not support the **not** form of this command.
- If you configure the class to match-all and ACL as match-criteria, no other match criteria, except the packet length, can be specified.
- If you configure the class to match-any and ACL as match-criteria, you can match ACLs and any other match criteria also.
- You are logged in to the CLI in EXEC mode.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 | switch(config)# class-map [type qos] [match-any | match-all] class_map_name | Places you into class map QoS configuration mode for the specified class map and configures and saves the map name in the running configuration.  
The **class_map_name** argument is a unique alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters. The map name must be unique across class-maps and policy-maps. For example, you cannot have a class-map and a policy-map with the same name of HR_Map.  
**Note** The **permit** and **deny** keywords are ignored when matching the ACL.  
The **not** form of this command is not supported.  |
|        | switch(config-cmap-qos)# match access-group name acl-name | Configures and saves the access group to match for this class in the running configuration.  
**Note** The **permit** and **deny** keywords are ignored when matching the ACL.  
The **not** form of this command is not supported.  |
| Step 4 | switch(config-cmap-qos)# show class-map class_map_name | Displays the class map configuration.  |
| Step 5 | switch(config-cmap-qos)# copy running-config startup-config | (Optional)  
Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.  |

This example shows how to classify the ACL traffic:

```sh
switch# configure terminal
switch(config)# class-map class_acl
switch(config-cmap-qos)# match access-group name my_acl
switch(config-cmap-qos)# show class-map class_acl
Type qos class-maps
-------------------------

class-map type qos match-all class_acl
```
class-map type qos match-all class_dscp
match dscp 18,28
switch(config-cmap-qos)# copy running-config startup-config

Classifying DSCP Traffic

You can classify traffic based on the DSCP value in the DiffServ field of the IP header. The standard DSCP values are found in the Commonly Used DSCP Values and IP Precedence Values.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch(config)# class-map [type qos] [match-any</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switch(config-cmap-qos)# match [not] dscp dscp_list</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>switch(config-cmap-qos)# show class-map class_map_name</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>switch(config-cmap-qos)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

This example shows how to classify DSCP traffic:

```
switch# configure terminal
switch(config)# class-map class_dscp
switch(config-cmap-qos)# match dscp af21 af32
switch(config-cmap-qos)# show class-map class_dscp
Type qos class-maps
-------------------------
  class-map type qos match-all class_dscp
    match dscp 18,28

switch(config-cmap-qos)# copy running-config startup-config
```
Configuring IP Precedence Classification

You can classify traffic based on the precedence value in the type of service (ToS) byte field of the IP header. Precedence values can be found in the Commonly Used DSCP Values and IP Precedence Values tables.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch(config)# class-map [type qos] [match-any</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switch(config-cmap-qos)# match [not] precedence values</td>
</tr>
<tr>
<td></td>
<td><strong>Value</strong></td>
</tr>
<tr>
<td></td>
<td>000 (0)</td>
</tr>
<tr>
<td></td>
<td>001 (1)</td>
</tr>
<tr>
<td></td>
<td>010 (2)</td>
</tr>
<tr>
<td></td>
<td>011 (3)</td>
</tr>
<tr>
<td></td>
<td>100 (4)</td>
</tr>
<tr>
<td></td>
<td>101 (5)</td>
</tr>
<tr>
<td></td>
<td>110 (6)</td>
</tr>
<tr>
<td></td>
<td>111 (7)</td>
</tr>
<tr>
<td></td>
<td><strong>Step 4</strong></td>
</tr>
</tbody>
</table>

Cisco Nexus 1000V for VMware vSphere Quality of Service Configuration Guide, Release 5.x
### Configuring QoS Group Classification

You can classify traffic based on the QoS group internal label, which is not part of the packet payload or any packet header. You can set the value of the QoS group within a policy map using the `set qos-group` command as described in the Creating a QoS Group Policy.

**Note**

You match on the QoS group only in egress policies because its value is undefined until you set it in an ingress policy.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 2** | switch(config)# class-map [type qos] [match-any | match-all] class_map_name | Places you into class map QoS configuration mode for the specified class map and configures and saves the map name in the running configuration.  
*The class_map_name argument is a unique alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters. The map name must be unique across class-maps and policy-maps. For example, you cannot have a class-map and a policy-map with the same name of HR_Map.* |
| **Step 3** | switch(config-cmap-qos)# match [not] qos-group multi-range-qos-group-values | Configures the traffic class by matching packets that are based on a list of QoS group values. Values can range from 0 to 126. The default QoS group value is 0. Use the `not` keyword to match on values that do not match the specified range. |

This example shows how to configure the IP precedence classification:

```text
switch# configure terminal
switch(config)# class-map class_ip_precedence
switch(config-cmap-qos)# match precedence 1-2, 5-7
switch(config-cmap-qos)# show class-map class_ip_precedence
  Type qos class-maps
  ----------------------
  class-map type qos match-all class_ip_precedence
  match precedence 1-2,5-7

switch(config-cmap-qos)# copy running-config startup-config
```
### Configuring Discard Class Classification

You can classify traffic based on the value of the discard class internal label, which is not part of the packet payload or any packet header. You can set the value of the discard class within a policy map by using the `set discard-class` command as described in the Creating a Discard Class Policy.

#### Note

You match on the discard class only in egress policies because its value is undefined until you set it in an ingress policy.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>switch(config)# class-map [type qos] [match-any</td>
</tr>
</tbody>
</table>
### Configuring QoS Classification

**Purpose**

Configure the traffic class by matching packets that are based on a list of discard-class values. Values can range from 0 to 63. The default discard class value is 0. Use the `not` keyword to match on values that do not match the specified range.

**Command or Action**

| Step 3 | switch(config-cmap-qos)# match [not] discard-class multi-range-discard-group-values |

**Description**

The `not` keyword is used to match on values that do not match the specified range. The `multi-range-discard-group-values` command is used to define multiple discard class values.

**Purpose**

Displays the class map configuration for the specified traffic class name.

**Command or Action**

| Step 4 | switch(config-cmap-qos)# show class-map class_map_name |

**Description**

The `show class-map class_map_name` command is used to display the class map configuration for the specified traffic class name.

**Purpose**

Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

**Command or Action**

| Step 5 | switch(config-cmap-qos)# copy running-config startup-config |

This example shows how to configure discard class classification:

```
switch# configure terminal
switch(config)# class-map class_discard_class
switch(config-cmap-qos)# match discard-class 4, 60-62
switch(config-cmap-qos)# show class-map class_discard_class
```

```
Class-map type qos match-all class_discard_class
match discard-class 4,60-62
switch(config-cmap-qos)# copy running-config startup-config
```

### Configuring Layer 3 Packet Length Classification

You can classify Layer 3 traffic based on various packet lengths.

**Note**

This feature is designed for IP packets only.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# class-map [type qos] [match-any</td>
</tr>
</tbody>
</table>

The `class_map_name` argument is a unique alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters. The map name must be unique across class-maps and policy-maps. For example, you cannot have a class-map and a policy-map with the same name of HR_Map.
Configuring CoS Classification

Traffic classification allows you to organize traffic (packets) into traffic classes or categories on the basis of whether the traffic matches the criteria that you specify. The values used to classify traffic are called match criteria. When you define a traffic class, you can specify multiple match criteria, you can choose to not match on a particular criterion, or you can determine the traffic class by matching any or all criteria.

You can classify traffic based on the class of service (CoS) in the IEEE 1Q header. This 3-bit field is defined in IEEE.802.1p to support QoS traffic classes. CoS refers to three bits in a 802.1Q header that is used to indicate the priority of the Ethernet frame as it passes through a switch network.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# class-map [type qos] [match-any</td>
<td>match-all] class_map_name</td>
</tr>
</tbody>
</table>

The class_map_name argument is a unique alphabetic string that can be up to 40 case-sensitive characters long, including hyphen (-) and underscore (_) characters. The map name must be unique across class-maps and policy-maps. For example,
### Configuring QoS Classification

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>you cannot have a class-map and a policy-map with the same name of HR_Map.</td>
</tr>
<tr>
<td>switch(config-cmap-qos)# match [not] cos cos-list</td>
<td>Configures the traffic class by matching packets that are based on a list of CoS values. Values can range from 0 to 7. Use the not keyword to match on values that do not match the specified range.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Displays the class map configuration for the specified traffic class name.</td>
</tr>
<tr>
<td>switch(config-cmap-qos)# show class-map class_map_name</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.</td>
</tr>
<tr>
<td>switch(config-cmap-qos)# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to configure CoS classification:

```
switch# configure terminal
switch(config)# class-map class_cos
switch(config-cmap-qos)# match cos 4, 5-6
switch(config-cmap-qos)# show class-map class_cos
Type qos class-maps
==============
  class-map type qos match-all class_cos
  match cos 4-6
switch(config-cmap-qos)# copy running-config startup-config
```

### Configuring IP RTP Classification

The IP Real-time Transport Protocol (RTP) is a transport protocol for real-time applications that transmits data such as audio or video and is defined by RFC 3550. Although RTP does not use a common TCP or UDP port, you typically configure RTP to use ports 16384 to 32767. UDP communications use an even port and the next higher odd port is used for RTP Control Protocol (RTCP) communications.

You can configure classification based on UDP port ranges, which are likely to target applications using RTP.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Places you into class map QoS configuration mode for the specified class map and configures and saves the map name in the running configuration.</td>
</tr>
<tr>
<td>switch(config)# class-map [type qos] [match-any</td>
<td>match-all] class_map_name</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>you cannot have a class-map and a policy-map with the same name of HR_Map.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

```
switch(config-cmap-qos)# match [not] ip rtp udp-port-values
```

Configures the traffic class by matching packets that are based on the range of lower and upper UDP port numbers, which is likely to target applications using RTP. Values can range from 2000 to 65535. Use the `not` keyword to match on values that do not match the specified range.

**Step 4**

```
switch(config-cmap-qos)# show class-map class_map_name
```

Displays the class map configuration for the specified traffic class name.

**Step 5**

```
switch(config-cmap-qos)# copy running-config startup-config
```

(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This example shows how to configure IP RTP classification:

```
switch# configure terminal
switch(config)# class-map class_rtp
switch(config-cmap-qos)# match ip rtp 2000-2100, 4000-4100
switch(config-cmap-qos)# show class-map class-rtp
```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class-map type qos match-all class_rtp match ip rtp 2000-2100, 4000-4100</td>
<td></td>
</tr>
</tbody>
</table>

```
switch(config-cmap-qos)# copy running-config startup-config
```

### Configuring Class Map Classification

You can classify traffic based on the match criteria in another class map.

**Before You Begin**

- The referenced class map must be created prior to its reference.
- You can reference the same class map in multiple policies.
- You can configure only one level of nesting of class maps. You cannot reference a class map that references another class map.
- Before you delete a referenced class map, you should delete all references to that class map.
- To perform a logical OR with the class map that is specified in the `match class-map` command, use the `match-any` keyword. The `match-any` or `match-all` specification of the matched class map is ignored.
- To perform a logical AND with the class map that is specified in the `match class-map` command, use the `match-all` keyword. The `match-any` or `match-all` specification of the matched class map is ignored.
**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>switch(config)# class-map [type qos] [match-any</td>
</tr>
<tr>
<td>Step 3</td>
<td>switch(config-cmap-qos)# match [not] class-map class_map_name</td>
</tr>
<tr>
<td>Step 4</td>
<td>switch(config-cmap-qos)# show class-map class_map_name</td>
</tr>
<tr>
<td>Step 5</td>
<td>switch(config-cmap-qos)# copy running-config startup-config</td>
</tr>
</tbody>
</table>

This example shows how to configure the class map classification:

```
switch# configure terminal
switch(config)# class-map class_class_map
switch(config-cmap-qos)# match class-map class-map3
switch(config-cmap-qos)# show class-map class_class_map
Type qos class-maps
-----------------------------
  class-map type qos match-all class_class_map
  match class-map class-map

switch(config-cmap-qos)# show class-map class-map
Type qos class-maps
-----------------------------
  class-map type qos match-all class-class_map
  match dscp 10,12

switch(config-cmap-qos)# copy running-config startup-config
```

Cisco Nexus 1000V for VMware vSphere Quality of Service Configuration Guide, Release 5.x
Verifying the Classification Configuration

To verify the classification configuration, use the commands in the following table.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show class-map name</code></td>
<td>Displays the class map configuration for all class maps or for a specified class map.</td>
</tr>
<tr>
<td><code>show ip access-lists name</code></td>
<td>Displays all IPv4 access control lists (ACLs) or a specific IPv4 ACL.</td>
</tr>
</tbody>
</table>

Configuration Example for QoS Classification

This example shows how to configure classification for the class map named cmap1, which matches DSCP traffic AF21 and AF32:

```
switch(config)# class-map type qos match-all cmap1
Type qos class-maps
------------------------
class-map type qos match-all cmap1
match dscp 18,28
switch(config-cmap-qos)# match dscp af21 af32
switch(config-cmap-qos)# exit
```

Note

A Class-map that does not have any match criteria configured will not match any packets. The only exception to this rule is the default class-map (class-default).

Feature History for QoS Classification

This section provides the QoS Classification release history.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS Classification</td>
<td>4.0.</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>