



# CHAPTER 2

## Configuring QoS Classification

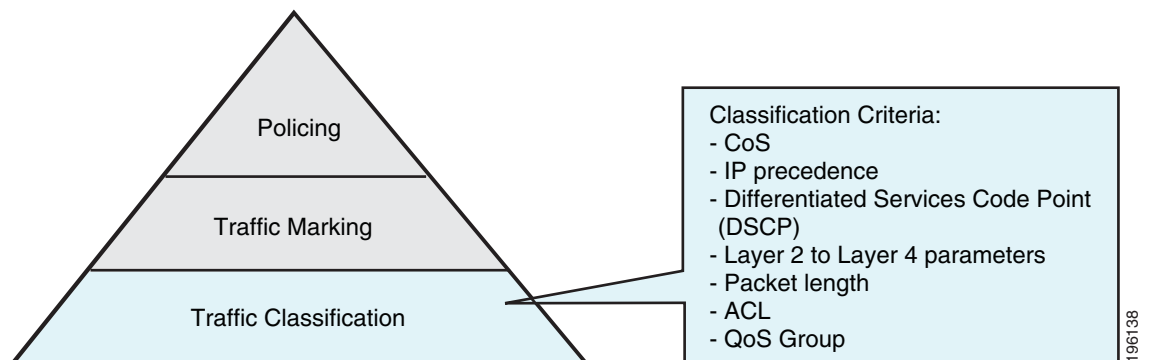
This chapter describes how to create and map classes of traffic for QoS on Cisco Nexus 1000V.

### Information About Traffic Classes

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

Figure 2-1 shows the criteria that you use to classify network traffic.

**Figure 2-1** Criteria for Classifying Network Traffic



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 treatment, 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 listed in Table 2-1. 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.

[Table 2-1](#) lists and describes the allowable criteria used for mapping traffic classes.

**Table 2-1 Traffic Class Criteria**

Class Criteria	Description
CoS	Class of service (CoS) field in the IEEE 802.1Q header.
IP precedence	Precedence value within the type of service (ToS) byte of the IP header.  The IP precedence values are shown in the <a href="#">“IP Precedence Values”</a> section on page 7-2.
Differentiated Services Code Point (DSCP)	DSCP value within the Diffserv field of the IP header.  The standard DSCP values are listed in the <a href="#">“Commonly Used DSCP Values”</a> section on page 7-1.
QoS group	Locally significant QoS values that can be manipulated and matched within the system. The range is from 0 to 126.
Discard class	Locally significant values that can be matched and manipulated within the system. The range is from 0 to 63.
ACL	IP access control list (ACL) or MAC ACL name.  If you configure the class to match-all and ACL used as match-criteria, then no other match criteria, except the packet length, can be specified.  If you configure the class to match-any and ACL used as match-criteria, then you can match ACLs and any other match criteria also.
Packet length	Size range of Layer 3 packet lengths.
IP RTP	Applications that are using the Real-time Transport Protocol (RTP) are identified by UDP port number range.
Class map	Criteria that are specified in a named class-map object.

# Prerequisites for Classification

Classification has the following prerequisites:

- You are logged in to the CLI in EXEC mode.

## Guidelines and Limitations

Classification has the following guidelines and limitations:

- 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.
- When you match on an ACL, the only other match that you can specify is the Layer 3 packet length in a match-all class.
- You can classify traffic on Layer 2 ports based on the port policy of the incoming packet.

## Classifying Traffic

This section describes how to classify traffic.

### Classifying ACL Traffic

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

#### BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- 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 used as match-criteria, then no other match criteria, except the packet length, can be specified.
- If you configure the class to match-any and ACL used as match-criteria, then you can match ACLs and any other match criteria also.
- You are logged in to the CLI in EXEC mode.
- 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.

#### SUMMARY STEPS

1. **config t**
2. **class-map [type qos] [match-any | match-all] class\_map\_name**
3. **match access-group name acl\_name**

4. `show class-map class_map_name`
5. `copy running-config startup-config`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code>  <b>Example:</b> n1000v# <code>config t</code> n1000v(config)#	Places you into global configuration mode.
Step 2	<code>class-map [type qos] [match-any   match-all] class_map_name</code>  <b>Example:</b> n1000v(config)# <code>class-map class_acl</code> n1000v(config-cmap-qos)#	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 <i>class_map_name</i> argument is an alphabetic string that can be up to 40 case-insensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	<code>match access-group name acl-name</code>  <b>Example:</b> n1000v(config-cmap-qos)# <code>match access-group name my_acl</code>	Configures and saves the access group to match for this class in the running configuration.  <b>Note</b> The <b>permit</b> and <b>deny</b> keywords are ignored when matching the ACL.  <b>Note</b> The <b>not</b> form of this command is not supported.
Step 4	<code>show class-map class_map_name</code>  <b>Example:</b> n1000v(config-cmap-qos)# <code>show class-map class_acl1</code>	Displays the class map configuration.
Step 5	<code>copy running-config startup-config</code>  <b>Example:</b> n1000v(config-cmap-qos)# <code>copy running-config startup-config</code>	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

## 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 “[DSCP and Precedence Values](#)” section on page 7-1.



### 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.

## SUMMARY STEPS

1. `config t`
2. `class-map [type qos] [match-any | match-all] class_map_name`

3. `match [not] dscp dscp_list`
4. `show class-map class_map_name`
5. `copy running-config startup-config`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code>  <b>Example:</b> n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	<code>class-map [type qos] [match-any   match-all] class_map_name</code>  <b>Example:</b> n1000v(config)# class-map class_dscp n1000v(config-cmap-qos)#	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 <i>class_map_name</i> argument is an alphabetic string that can be up to 40 case-insensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	<code>match [not] dscp dscp_list</code>  <b>Example:</b> n1000v(config-cmap-qos)# match dscp af21, af32	Configures the traffic class by matching packets that are based on <i>dscp-values</i> . The standard DSCP values are listed in the “ <a href="#">DSCP and Precedence Values</a> ” section on page 7-1.  Use the <b>not</b> keyword to match on values that do not match the specified range.
Step 4	<code>show class-map class_map_name</code>  <b>Example:</b> n1000v(config-cmap-qos)# show class-map class_dscp	Displays the class map configuration.
Step 5	<code>copy running-config startup-config</code>  <b>Example:</b> n1000v(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.

## 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 “[DSCP and Precedence Values](#)” section on page 7-1.



### 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.

## SUMMARY STEPS

1. `config t`
2. `class-map [type qos] [match-any | match-all] class_map_name`
3. `match [not] precedence values`
4. `show class-map class_map_name`
5. `copy running-config startup-config`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code>  <b>Example:</b> n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	<code>class-map [type qos] [match-any   match-all] class_map_name</code>  <b>Example:</b> n1000v(config)# class-map class_ip_precedence n1000v(config-cmap-qos)#	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 <i>class_map_name</i> argument is an alphabetic string that can be up to 40 case-insensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	<code>match [not] precedence values</code>  <b>Example:</b> n1000v(config-cmap-qos)# match precedence 1-2, 5-7	Configures the traffic class by matching packets that are based on <i>precedence-values</i> . Values are listed in the “ <a href="#">DSCP and Precedence Values</a> ” section on <a href="#">page 7-1</a> . Use the <b>not</b> keyword to match on values that do not match the specified range.
Step 4	<code>show class-map class_map_name</code>  <b>Example:</b> n1000v(config-cmap-qos)# show class-map class_ip_precedence	Displays the class map configuration.
Step 5	<code>copy running-config startup-config</code>  <b>Example:</b> n1000v(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.

## Configuring QoS Group Classification

You can classify traffic based on the value of 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](#)” section on [page 3-8](#).

**Note**

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

## SUMMARY STEPS

1. `config t`
2. `class-map [type qos] [match-any | match-all] class_map_name`
3. `match [not] qos-group multi-range-qos-group-values`
4. `show class-map class_map_name`
5. `copy running-config startup-config`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code>  <b>Example:</b> n1000v# <code>config t</code> n1000v(config)#	Places you into global configuration mode.
Step 2	<code>class-map [type qos] [match-any   match-all] class_map_name</code>  <b>Example:</b> n1000v(config)# <code>class-map class_qos_group</code> n1000v(config-cmap-qos)#	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 <code>class_map_name</code> argument is an alphabetic string that can be up to 40 case-insensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	<code>match [not] qos-group multi-range-qos-group-values</code>  <b>Example:</b> n1000v(config-cmap-qos)# <code>match qos-group 4, 80-90</code>	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 <b>not</b> keyword to match on values that do not match the specified range.
Step 4	<code>show class-map class_map_name</code>  <b>Example:</b> n1000v(config-cmap-qos)# <code>show class-map class_qos_group</code>	Displays the class map configuration for the specified traffic class name.
Step 5	<code>copy running-config startup-config</code>  <b>Example:</b> n1000v(config-cmap-qos)# <code>copy running-config startup-config</code>	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

## 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 using the `set discard-class` command as described in the “[Creating a Discard Class Policy](#)” section on [page 3-9](#).

**Note**

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

## SUMMARY STEPS

1. `config t`
2. `class-map [type qos] [match-any | match-all] class_map_name`
3. `match [not] discard-class multi-range-discard-class-values`
4. `show class-map class_map_name`
5. `copy running-config startup-config`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code>  <b>Example:</b> n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	<code>class-map [type qos] [match-any   match-all] class_map_name</code>  <b>Example:</b> n1000v(config)# class-map class_discard_class n1000v(config-cmap-qos)#	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 <i>class_map_name</i> argument is an alphabetic string that can be up to 40 case-insensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	<code>match [not] discard-class multi-range-discard-class-values</code>  <b>Example:</b> n1000v(config-cmap-qos)# match discard-class 4, 60-62 n1000v(config-cmap-qos)#	Configures the traffic class by matching packets that are based on the list of discard-class values. Values can range from 0 to 63. The default discard class value is 0. Use the <b>not</b> keyword to match on values that do not match the specified range.
Step 4	<code>show class-map class_map_name</code>  <b>Example:</b> n1000v(config-cmap-qos)# show class-map class_discard_class n1000v(config-cmap-qos)#	Displays the specified class map configuration.
Step 5	<code>copy running-config startup-config</code>  <b>Example:</b> n1000v(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.

## 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.



## SUMMARY STEPS

1. `config t`
2. `class-map [type qos] [match-any | match-all] class_map_name`
3. `match [not] packet length packet-length-list`
4. `show class-map class_map_name`
5. `copy running-config startup-config`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code>  <b>Example:</b> n1000v# <code>config t</code> n1000v(config)#	Places you into global configuration mode.
Step 2	<code>class-map [type qos] [match-any   match-all] class_map_name</code>  <b>Example:</b> n1000v(config)# <code>class-map class_packet_length</code>	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 <code>class_map_name</code> argument is an alphabetic string that can be up to 40 case-insensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	<code>match [not] packet length packet-length-list</code>  <b>Example:</b> n1000v(config-cmap-qos)# <code>match packet length 2000</code>	Configures the traffic class by matching packets that are based on various packet lengths. Values can range from 1 to 9198. Use the <b>not</b> keyword to match on values that do not match the specified range.
Step 4	<code>show class-map class_map_name</code>  <b>Example:</b> n1000v(config-cmap-qos)# <code>show class-map class_packet_length</code> n1000v(config-cmap-qos)#	Displays the specified class map configuration.
Step 5	<code>copy running-config startup-config</code>  <b>Example:</b> n1000v(config-cmap-qos)# <code>copy running-config startup-config</code>	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

## Configuring CoS Classification

You can classify traffic based on the class of service (CoS) in the IEEE 802.1Q header. This 3-bit field is defined in IEEE 802.1p to support QoS traffic classes. CoS is encoded in the high order 3 bits of the VLAN ID Tag field and is referred to as `user_priority`.

## SUMMARY STEPS

1. `config t`
2. `class-map [type qos] [match-any | match-all] class_map_name`

3. `match [not] cos cos-list`
4. `show class-map class_map_name`
5. `copy running-config startup-config`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>config t</code>  <b>Example:</b> n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	<code>class-map [type qos] [match-any   match-all] class_map_name</code>  <b>Example:</b> n1000v(config)# class-map class_cos	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 <i>class_map_name</i> argument is an alphabetic string that can be up to 40 case-insensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	<code>match [not] cos cos-list</code>  <b>Example:</b> n1000v(config-cmap-qos)# match cos 4, 5-6	Configures the traffic class by matching packets that are based on the list of CoS values. Values can range from 0 to 7. Use the <b>not</b> keyword to match on values that do not match the specified range.
Step 4	<code>show class-map class_map_name</code>  <b>Example:</b> n1000v(config-cmap-qos)# show class-map class_cos n1000v(config-cmap-qos)#	Displays the specified class map configuration.
Step 5	<code>copy running-config startup-config</code>  <b>Example:</b> n1000v(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.

## 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.

## SUMMARY STEPS

1. `config t`
2. `class-map [type qos] [match-any | match-all] class_map_name`

3. **match [not] ip rtp *udp-port-values***
4. **show class-map *class\_map\_name***
5. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>config t</b>  <b>Example:</b> n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	<b>class-map [type qos] [match-any   match-all] <i>class_map_name</i></b>  <b>Example:</b> n1000v(config)# class-map class_rtp n1000v(config-cmap-qos)#	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 <i>class_map_name</i> argument is an alphabetic string that can be up to 40 case-insensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	<b>match [not] ip rtp <i>udp-port-values</i></b>  <b>Example:</b> n1000v(config-cmap-qos)# match ip rtp 2000-2100, 4000-4100	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 <b>not</b> keyword to match on values that do not match the specified range.
Step 4	<b>show class-map <i>class_map_name</i></b>  <b>Example:</b> n1000v(config-cmap-qos)# show class-map class_rtp	Displays the specified class map configuration.
Step 5	<b>copy running-config startup-config</b>  <b>Example:</b> n1000v(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.

## Configuring Class Map Classification

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

### BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- 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.

## SUMMARY STEPS

1. **config t**
2. **class-map [type qos] [match-any | match-all] class\_map\_name**
3. **match [not] class-map class\_map\_name**
4. **show class-map class\_map\_name**
5. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>config t</b>  <b>Example:</b> n1000v# config t n1000v(config)#	Places you into global configuration mode.
Step 2	<b>class-map [type qos] [match-any   match-all] class_map_name</b>  <b>Example:</b> n1000v(config)# class-map class_class_map n1000v(config-cmap-qos)#	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 <i>class_map_name</i> argument is an alphabetic string that can be up to 40 case-insensitive characters long, including hyphen (-) and underscore (_) characters.
Step 3	<b>match [not] class-map class_map_name</b>  <b>Example:</b> n1000v(config-cmap-qos)# match class-map class_map3	Configures the traffic class by matching packets that are based on the match criteria in another class map. Because match-all is the default for the <b>class-map</b> command, the match criteria that is specified in class_map3 are ANDed with match criteria in class_class_map. Use the <b>not</b> keyword to match on values that do not match the specified range.
Step 4	<b>show class-map class_map_name</b>  <b>Example:</b> n1000v(config-cmap-qos)# show class-map class_class_map	Displays the specified class map configuration.
Step 5	<b>copy running-config startup-config</b>  <b>Example:</b> n1000v(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.

## Verifying the Classification Configuration

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

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

## 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:

```
n1000v(config)# class-map type qos match-all cmap1
n1000v(config-cmap-qos)# match dscp af21 af32
n1000v(config-cmap-qos)# exit
n1000v(config)#
```

## Feature History for QoS Classification

This section provides the QoS Classification release history.

Feature Name	Releases	Feature Information
QoS Classification	4.0	This feature was introduced.

