



# Configuring Classification

This chapter contains the following sections:

- [Information About Classification, page 1](#)
- [Ingress Classification Policies, page 2](#)
- [Licensing Requirements for Classification, page 2](#)
- [Configuring Classification, page 2](#)
- [Verifying the Classification Configuration, page 10](#)

## Information About Classification

Classification is the separation of packets into traffic classes. You configure the device to take a specific action on the specified classified traffic, such as policing or marking down, or other actions.

You can create class maps to represent each traffic class by matching packet characteristics with classification criteria.

**Table 1: Classification Criteria**

Classification Criteria	Description
Class map	Criteria specified in a named class-map object.
Precedence	Precedence value within the Type of Service (ToS) byte of the IP Header.
Differentiated Services Code Point (DSCP)	DSCP value within the DiffServ field of the IP Header.
Protocol	Selected set of protocols, including Address Resolution Protocol (ARP) and Connectionless Network Service (CLNS).
IP RTP	Identify applications using Real-time Transport Protocol (RTP) by UDP port number range.

Classification Criteria	Description
ACL	Traffic is classified by the criteria defined in the access control list (ACL).

Table 2: Supported RFCs

RFC	Title
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

## Ingress Classification Policies

You use classification to partition traffic into classes. You classify the traffic based on the packet property (CoS field) or the packet header fields that include IP precedence, Differentiated Services Code Point (DSCP), and Layer 2 to Layer 4 parameters. The values used to classify traffic are called match criteria.

Traffic that fails to match any class is assigned to a default class of traffic called class-default.

## Licensing Requirements for Classification

This feature does not require a license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

## Configuring Classification

### Configuring Class Maps

You can create or modify a class map with the **class-map** command. The class map is a named object that represents a class of traffic. In the class map, you specify a set of match criteria for classifying the packets. You can then reference class maps in policy maps.


**Note**

The class map type default is type qos and its match criteria default is match-all.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	switch(config)# <b>class-map</b> [type { <b>network-qos</b>   <b>qos</b>   <b>queuing</b> }] <i>class-map name</i>	<p>Creates or accesses a named object that represents the specified class of traffic.</p> <p>Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.</p> <p>The three class-map configuration modes are as follows:</p> <ul style="list-style-type: none"> <li>• <b>network-qos</b>—Network-wide (global) mode. CLI prompt: switch(config-cmap-nq)#</li> <li>• <b>qos</b>—Classification mode; this is the default mode. CLI prompt: switch(config-cmap-qos)#</li> <li>• <b>queuing</b>—Queuing mode. CLI prompt: switch(config-cmap-que)#</li> </ul>
<b>Step 3</b>	switch(config)# <b>class-map</b> [type <b>qos</b> ] [ <b>match-all</b>   <b>match-any</b> ] <i>class-map name</i>	<p>(Optional)</p> <p>Specifies that packets must match any or all criteria that is defined for a class map.</p> <ul style="list-style-type: none"> <li>• <b>match-all</b>—Classifies traffic if packets match all criteria that is defined for a specified class map (for example, if both the defined CoS and the ACL criteria match).</li> <li>• <b>match-any</b>—Classifies traffic if packets match any criteria that is defined for a specified class map (for example, if either the CoS or the ACL criteria matches).</li> </ul> <p>Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.</p>
<b>Step 4</b>	switch(config)# <b>no class-map</b> [type { <b>network-qos</b>   <b>qos</b>   <b>queuing</b> }] <i>class-name</i>	<p>(Optional)</p> <p>Deletes the specified class map.</p> <p><b>Note</b> You cannot delete the two system-defined class maps: class-fcoe and class-default.</p> <p>Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.</p>

## 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*.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>class-map type qos</b> <i>class-name</i>	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
<b>Step 3</b>	switch(config-cmap-qos)# <b>match cos</b> <i>cos-value</i>	Specifies the CoS value to match for classifying packets into this class. You can configure a CoS value in the range of 0 to 7.
<b>Step 4</b>	switch(config-cmap-qos)# <b>no match</b> <b>cos</b> <i>cos-value</i>	(Optional) Removes the match from the traffic class.

This example shows how to classify traffic by matching packets based on a defined CoS value:

```
switch# configure terminal
switch(config)# class-map type qos match-any class_cos
switch(config-cmap-qos)# match cos 4, 5-6
```

Use the **show class-map** command to display the CoS value class-map configuration:

```
switch# show class-map class_cos
```

## Configuring Precedence Classification

You can classify traffic based on the precedence value in the type of service (ToS) byte field of the IP header (either IPv4 or IPv6). The following table shows the precedence values:

**Table 3: Precedence Values**

<b>Value</b>	<b>List of Precedence Values</b>
<0-7>	IP precedence value
critical	Critical precedence (5)
flash	Flash precedence (3)
flash-override	Flash override precedence (4)
immediate	Immediate precedence (2)
internet	Internetwork control precedence (6)
network	Network control precedence (7)

Value	List of Precedence Values
priority	Priority precedence (1)
routine	Routine precedence (0)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>class-map type qos match-any class-name</b>	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
<b>Step 3</b>	switch(config-cmap-qos)# <b>match precedence precedence-values</b>	Configures the traffic class by matching packets based on precedence values. For a list of precedence values, see the Precedence Values table.
<b>Step 4</b>	switch((config-cmap-qos)# <b>no match precedence precedence-values</b>	(Optional) Removes the match from the traffic class. For a list of precedence values, see the Precedence Values table.

This example shows how to classify traffic by matching packets based on the precedence value in the ToS byte field of the IP header:

```
switch# configure terminal
switch(config)# class-map type qos match-any class_precedence
switch(config-cmap-qos)# match precedence 1-2, critical
```

Use the **show class-map** command to display the IP precedence value class-map configuration:

```
switch# show class-map class_precedence
```

## Configuring DSCP Classification

You can classify traffic based on the Differentiated Services Code Point (DSCP) value in the DiffServ field of the IP header (either IPv4 or IPv6).

**Table 4: Standard DSCP Values**

Value	List of DSCP Values
af11	AF11 dscp (001010)—decimal value 10
af12	AF12 dscp (001100)—decimal value 12
af13	AF13 dscp (001110)—decimal value 14

<b>Value</b>	<b>List of DSCP Values</b>
af21	AF21 dscp (010010)—decimal value 18
af22	AF22 dscp (010100)—decimal value 20
af23	AF23 dscp (010110)—decimal value 22
af31	AF31 dscp (011010)—decimal value 26
af32	AF32 dscp (011100)—decimal value 28
af33	AF33 dscp (011110)—decimal value 30
af41	AF41 dscp (100010)—decimal value 34
af42	AF42 dscp (100100)—decimal value 36
af43	AF43 dscp (100110)—decimal value 38
cs1	CS1 (precedence 1) dscp (001000)—decimal value 8
cs2	CS2 (precedence 2) dscp (010000)—decimal value 16
cs3	CS3 (precedence 3) dscp (011000)—decimal value 24
cs4	CS4 (precedence 4) dscp (100000)—decimal value 32
cs5	CS5 (precedence 5) dscp (101000)—decimal value 40
cs6	CS6 (precedence 6) dscp (110000)—decimal value 48
cs7	CS7 (precedence 7) dscp (111000)—decimal value 56
default	Default dscp (000000)—decimal value 0
ef	EF dscp (101110)—decimal value 46

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<code>switch# configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<code>switch(config)# class-map type qos class-name</code>	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
<b>Step 3</b>	<code>switch(config-cmap-qos)# match dscp dscp-list</code>	Configures the traffic class by matching packets based on the values in the <code>dscp-list</code> variable. For a list of DSCP values, see the Standard DSCP Values table.
<b>Step 4</b>	<code>switch(config-cmap-qos)# no match dscp dscp-list</code>	(Optional) Removes the match from the traffic class. For a list of DSCP values, see the Standard DSCP Values table.

This example shows how to classify traffic by matching packets based on the DSCP value in the DiffServ field of the IP header:

```
switch# configure terminal
switch(config)# class-map type qos match-any class_dscp
switch(config-cmap-qos)# match dscp af21, af32
```

Use the **show class-map** command to display the DSCP class-map configuration:

```
switch# show class-map class_dscp
```

## Configuring Protocol Classification

You can classify traffic based on the IPv4 Protocol field or the IPv6 Next Header field in the IP header. The following table shows the protocol arguments:

**Table 5: Protocol Arguments**

<b>Argument</b>	<b>Description</b>
arp	Address Resolution Protocol (ARP)
clns_es	CLNS End Systems
clns_is	CLNS Intermediate System
dhcp	Dynamic Host Configuration (DHCP)
ldp	Label Distribution Protocol (LDP)
netbios	NetBIOS Extended User Interface (NetBEUI)

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters configuration mode.
<b>Step 2</b>	switch(config)# <b>class-map type qos</b> <i>class-name</i>	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
<b>Step 3</b>	switch(config-cmap-qos)# <b>match protocol</b> {arp   clns_es   clns_is   dhcp   ldp   netbios}	Configures the traffic class by matching packets based on the specified protocol.
<b>Step 4</b>	switch(config-cmap-qos)# <b>no match</b> <b>protocol</b> {arp   clns_es   clns_is   dhcp   ldp   netbios}	(Optional) Removes the match from the traffic class.

This example shows how to classify traffic by matching packets based on the protocol field:

```
switch# configure terminal
switch(config)# class-map type qos class_protocol
switch(config-cmap-qos)# match protocol arp
```

Use the **show class-map** command to display the protocol class-map configuration:

```
switch# show class-map class_protocol
```

## 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 classify based on UDP port ranges, which are likely to target applications using RTP.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>class-map type qos</b> <i>class-name</i>	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
<b>Step 3</b>	switch(config-cmap-qos)# <b>match ip</b> <b>rtp</b> <i>port-number</i>	Configures the traffic class by matching packets based on a range of lower and upper UDP port numbers, which



	Command or Action	Purpose
		is likely to target applications using RTP. Values can range from 2000 to 65535.
<b>Step 4</b>	switch(config-cmap-qos)# <b>no match ip rtp</b> <i>port-number</i>	(Optional) Removes the match from the traffic class.

The following example shows how to classify traffic by matching packets based on UDP port ranges that are typically used by RTP applications:

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

Use the **show class-map** command to display the RTP class-map configuration:

```
switch# show class-map class_rtp
```

## Configuring ACL Classification

You can classify traffic by matching packets based on an existing access control list (ACL). Traffic is classified by the criteria defined in the ACL. The **permit** and **deny** ACL keywords are ignored in the matching; even if a match criteria in the access-list has a **deny** action, it is still used for matching for this class.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	switch(config)# <b>class-map type qos</b> <i>class-name</i>	Creates a named object that represents a class of traffic. Class-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
<b>Step 3</b>	switch(config-cmap-qos)# <b>match access-group name</b> <i>acl-name</i>	Configures a traffic class by matching packets based on the <i>acl-name</i> . The <b>permit</b> and <b>deny</b> ACL keywords are ignored in the matching.  <b>Note</b> You can only define a single ACL in a class map. You cannot add any other match criteria to a class with a <b>match access-group</b> defined.
<b>Step 4</b>	switch(config-cmap-qos)# <b>no match access-group name</b> <i>acl-name</i>	(Optional) Removes the match from the traffic class.

This example shows how to classify traffic by matching packets based on existing ACLs:

```
switch# configure terminal
switch(config)# class-map type qos class_acl
switch(config-cmap-qos)# match access-group name acl-01
```

Use the **show class-map** command to display the ACL class-map configuration:

```
switch# show class-map class_acl
```

## Verifying the Classification Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
<b>show class-map</b>	Displays the class maps defined on the switch.
<b>show policy-map</b> [ <i>name</i> ]	Displays the policy maps defined on the switch. Optionally, you can display the named policy only.
<b>running-config ipqos</b>	Displays information about the running configuration for QoS.
<b>startup-config ipqos</b>	Displays information about the startup configuration for QoS.