Configuring Classification

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 the classification criteria in the following table:

Table 1: Classification Criteria

Classification 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.
Differentiated Services Code Point (DSCP)	DSCP value within the DiffServ field of the IP header.
ACL	IP, IPv6, or MAC ACL name.
Packet length	Size range of Layer 3 packet lengths.
IP RTP	Identify applications using Real-time Transport Protocol (RTP) by UDP port number range.
MPLS experimental	EXP field value.

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.

Note However, if you match on an ACL, no other match criteria, except the packet length, can be specified in a match-all class. In a match-any class, you can match on ACLs and any other match criteria.

Traffic that fails to match any 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.

You can reuse class maps when defining the QoS policies for different interfaces that process the same types of traffic.

Prerequisites for Classification

Classification has the following prerequisites:

- You must be familiar with using modular QoS CLI.

- You are logged on to the device.

Guidelines and Limitations

Classification has the following configuration guidelines and limitations:

- **show** commands with the **internal** keyword are not supported.

- You can specify a maximum of 1024 match criteria in a class map.

- You can configure a maximum of 128 classes for use in a single policy map.

- When you match on an ACL, the only other match you can specify is the Layer 3 packet length in a match-all class.

- The **match-all** option in the **class-map type qos match-all** command is not supported. The match criteria of this command becomes the same as in the **class-map type qos match-any** command. The **class-map type qos match-all** command yields the same results as the **class-map type qos match-any** command.

- You can classify traffic on Layer 2 ports based on the port policy of the incoming packet but not both. If both are present, the device acts on the port policy.

- A QoS policy with a MAC-based ACL as a match in the class map does not work for IPv6 traffic. For QoS, IPv6 traffic needs to be matched based on IPv6 addresses and not on MAC addresses.

- A QoS policy that references an ACL that contains a match for ICMP type or code is not supported.

- A QoS Policy that references an ACL that contains a match for TCP flags is not supported.

Configuring Traffic Classes

Configuring ACL Classification

You can classify traffic by matching packets based on existing ACLs. The permit and deny ACL keywords are ignored in the matching. QoS does not use the permit-deny functions of ACLs. You can classify by either IPv4, IPv6, or MAC address.

Step 1   Enter global configuration mode.

switch# **configure terminal**

Step 2   Create or access the class map named class-name and enters class-map mode. The class map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters. (**match-any** is the default when no option is selected and multiple match statements are entered.)

switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*

Step 3   Configure the traffic class by matching packets based on the *acl-name*. The **permit** and **deny** ACL keywords are ignored in the matching.

switch(config-cmap-qos)# **match access-group name** *acl-name*

Example: Configuring ACL Classification

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
    class-map class_acl
    match access-group name my_acl
```

This example shows how to display the ACL class-map configuration:

```
show class-map class_acl
```

Configuring DSCP Classification

You can classify traffic based on the DSCP value in the DiffServ field of the IP header. The standard DSCP values are listed in the following table:

Table 2: Standard DSCP Values

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

Value	List of DSCP Values
af13	AF13 dscp (001110)—decimal value 14
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	AF40 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

Step 1 Enter global configuration mode.

switch# **configure terminal**

Step 2 Create or access the class map named class-name and enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.

switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*

Step 3 Configure the traffic class by matching packets based on dscp-values. The standard DSCP values are shown in the following table.

switch(config-cmap-qos)# **match** [**not**] **dscp** *dscp-values*

Step 4 Exit global class-map queuing mode and enters global configuration mode.

switch(config-cmap-qos)# **exit**

Step 5   (Optional) Save the running configuration to the startup configuration.

switch(config)# **copy running-config startup-config**

Example

This example shows how to display the DSCP class-map configuration:

```
show class-map class_dscp
```

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.

Note   The DSCP value is trust on the Layer 3 port of a Cisco NX-OS device.

The precedence values are listed in the following:

Table 3: Precedence Values

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

Step 1   Enter global configuration mode.

configure terminal

Step 2   Create or accesses the class map named class-name and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.

class-map [**type qos**] [**match-any** | **match-all**] *class-name*

Step 3 Configure the traffic class by matching packets based on *precedence-values*. Values are shown in the following table. Use the **not** keyword to match on values that do not match the specified range.

match [**not**] **precedence** *precedence-values*

Step 4 Exit global class-map queuing mode and enters global configuration mode.

exit

Step 5 (Optional) Save the running configuration to the startup configuration.

copy running-config startup-config

Example: Configuring IP Precedence Classification

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
    class-map class_ip_precedence
    match precedence 1-2, 5-7
    exit
```

This example shows how to display the IP precedence class-map configuration:

```
show class-map class_ip_precedence
```

Configuring Protocol Classification

For Layer 3 protocol traffic, you can use the ACL classification match.

Table 4: match Command Protocol Arguments

Argument	Description
arp	Address Resolution Protocol (ARP)
bridging	Bridging
cdp	Cisco Discovery Protocol (CDP)
dhcp	Dynamic Host Configuration (DHCP)
isis	Intermediate system to intermediate system (IS-IS)
lldp	Link Layer Discovery Protocol
lacp	Link Aggregation Control Protocol

Step 1 Enter global configuration mode.

switch# **configure terminal**

Step 2   Create or access the class map named class-name and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.

switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*

Step 3   Configure the traffic class by matching packets based on the specified protocol.

switch(config-cmap-qos)# **match protocol** {**arp** | **bridging** | **cdp** | **dhcp** | **isis**}

Step 4   Exit global class-map queuing mode and enters global configuration mode.

switch(config-cmap-qos)# **exit**

Step 5   (Optional) Save the running configuration to the startup configuration.

switch(config)# **copy running-config startup-config**

Example: Configuring Protocol Classification

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
     class-map class_protocol
     match protocol isis
     exit
```

This example shows how to display the protocol class-map configuration:

```
show class-map class_protocol
```

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.

Step 1   Enter global configuration mode.

switch# **configure terminal**

Step 2   Create or access the class map named class-name and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.

switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-name*

Step 3   Configure the traffic class by matching packets based on the 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.

switch(config-cmap-qos)# **match** [**not**] **cos** *cos-list*

Step 4   Exit global class-map queuing mode and enters global configuration mode.

```
switch(config-cmap-qos)# exit
```

Step 5   (Optional) Save the running configuration to the startup configuration.

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

Example: Configuring CoS Classification

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
    class-map class_cos
    match cos 4,5-6
    exit
```

This example shows how to display the CoS class-map configuration:

```
show class-map class_cos
```

Configuring IP RTP Classification

The IP Real-time Transport Protocol (RTP) is a transport protocol for real-time applications that transmit 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 uses an even-numbered port and the next higher odd-numbered 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.

Step 1   Enter global configuration mode.

```
switch# configure terminal
```

Step 2   Create or access the class map named class-name and then enters class-map mode. The class-map name can contain alphabetic, hyphen, or underscore characters, and can be up to 40 characters.

```
switch(config)# class-map [type qos] [match-any | match-all] class-name
```

Step 3   Configure the traffic class by matching packets based on a range of lower and upper UDP port numbers, which is likely to target applications using RTP. Values can range from 2000 to 65535.

```
switch(config-cmap-qos)#  match ip rtp udp-port-value
```

Step 4   Exit global class-map queuing mode and enters global configuration mode.

```
switch(config-cmap-qos)# exit
```

Step 5   (Optional) Save the running configuration to the startup configuration.

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

Example: Configuring IP RTP Classification

The following is a running configuration example. Replace the placeholders with relevant values for your setup.

```
configure terminal
    class-map class_rtp
    match ip rtp 2000-2100, 4000-4100
    exit
    copy running-config
    startup-config
```

This example shows how to display the RTP class-map configuration:

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

Configuring MPLS Experimental Classification

Step 1 Enter global configuration mode.

switch# **configure terminal**

Step 2 Access the class-mpls.

switch(config)# **class-map type qos match-any class-mpls**

Step 3 Configure the traffic class by matching mpls experimental.

switch(config-cmap-qos)# **match mpls experimental topmost** *number*

Example: Configuring MPLS Experimental Classification

```
configure terminal
    class-map type qos match-any class-mpls
    match match mpls experimental topmost 2, 5-7
```

Verifying the Classification Configuration

Use the **show class-map** command to verify the class-map configuration. This command displays all class maps.

Configuration Examples for Classification

The following example shows how to configure classification for two classes of traffic:

```
class-map class_dscp
match dscp af21, af32
exit
```

```
class-map class_cos
match cos 4, 5-6
exit
```