Configuring Classification

This chapter describes how to configure classification on the Cisco NX-OS device.

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your 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 "New and Changed Information"chapter or the Feature History table in this chapter.

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 the classification criteria in the table below.

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.

Classification Criteria	Description
QoS group	Locally significant QoS values that can be manipulated and matched within the system. The range is from 1 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 ACL or MAC ACL name.
Protocol	Standard Layer 2 protocol such as Address Resolution Protocol (ARP) or Connectionless Network Service (CLNS).
Packet length	Size range of Layer 3 packet lengths.
IP RTP	Identify applications using Real-time Transport Protocol (RTP) by UDP port number range.
Class map	Criteria specified in a named class-map object.

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.

Some match criteria relate only to ingress or egress traffic. 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 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.

When you configure match all for a QoS class map by entering the **class-map type qos match-all** command, the match-all option does not work. Instead, the match criteria is always treated as match any.

You can reuse class maps within the same virtual device context (VDC) when defining the QoS policies for different interfaces that process the same types of traffic.

Note For more information on class maps, see “Using Modular QoS CLI”.

Prerequisites for Classification

Classification has the following prerequisites:

- You must be familiar with the concepts in “Using Modular QoS CLI”.

- You are logged on to the switch.
- You are in the correct VDC. A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.

Guidelines and Limitations

Classification has the following configuration guidelines and limitations:

- You can specify a maximum of 1024 match criteria in a class map.
- You can configure a maximum of 4096 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 either the port policy or VLAN policy of the incoming packet but not both. Either the port policy or the VLAN policy takes effect but not both. If both are present, the device acts on the port policy and ignores the VLAN policy.
- The **match cos** command is not supported in the egress direction.
- When you configure an access-list (ACL) using the **fragments deny-all** command and reference that ACL in a quality of service (QOS) policy, the fragments are dropped. To avoid this fragments droppage, use the **fragments permit-all**command. This will ensure smooth traffic and fragments are not dropped and the defined action in the QOS policy is performed.
- If a QoS policy is configured with one type of match criteria, a different type of match criteria cannot be used. The following error message will be returned:

```
ERROR: Unable to perform the action due to incompatibility:
Module 1, 2, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16, 17, 18 returned status
"Policies with classes containing combined 'match dscp', 'match cos',
'match precedence' or 'match qos-group' are not supported.
Only the same match type is supported between classes.
```

- When you display the queuing statistics, the statistics for cbqosmib is shown per action, not per class level.
- Queuing cbqosmib will only be pulled when the following actions are configured: queue-limit, random-detect, bandwidth, and priority.
- For F1 module proxy-forwarded traffic, ACL classification is matched against the layer 3 protocols shown in the following table.
- **show policy-map interface** *[interface type]* **type queuing** uses L2 MTU (Frame length) and counts as a full packet length.
- **show policy-map interface** *[interface type]* **type qos** uses L3 MTU (Packet length).

Table 1: Protocol Number and Associated Layer 3 Protocol

Protocol Number	Layer 3 Protocol
1	ICMP
2	IGMP
4	IPv4 Encapsulation
6	TCP
17	UDP

Note Layer 3 protocols not listed in the table are classified as protocol number 4 (IPv4 Encapsulation).

Configuring Traffic Classes

Configuring ACL Classification

Note The device does not support the **no** form of the **match access-group name** command.

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 or IPv6.

Support is available for controlling deny access control entry ([**no**] **hardware access-list allow deny ace**) in the CLI. For more information about this support, see the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide*.

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic,

	Command or Action	Purpose
		hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match access-group name** *acl-name*	Configures the traffic class by matching packets based on the acl-name. The **permit** and **deny** ACL keywords are ignored in the matching. The device does not support the **no** form of this command.

Example

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

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

Configuring a Deny ACE

You can configure the device to support deny access control entries (ACEs) in a sequence for the following sequence-based features: VACL, policy-based routing (PBR), and QoS. When deny ACEs are enabled, the traffic that matches a deny ACE (an ACL rule with the **deny** keyword) in a class-map-acl is recursively matched against subsequent class-map-acls until it hits a permit ACE.

Before you begin

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **hardware access-list allow deny ace**	Enables support for deny ACEs in a sequence.
Step 3	(Optional) switch(config)# **show running-config aclmgr**	Displays the ACL configuration.
Step 4	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

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 table below:

Table 2: Standard DSCP Values

Value	List of DSCP Values
af11	AF11 dscp (001010)—decimal value 10
af12	AF12 dscp (001100)—decimal value 12
af12	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
af31	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

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **dscp** *dscp-list*	Configures the traffic class by matching packets based on dscp-values. The standard DSCP values are shown in the table above. Use the **not** keyword to match on values that do not match the specified range.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

```
switch# 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. The table below shows the precedence values.

Table 3: Precedence Values

Value	List of Precedence Values
0-7	IP precedence value
critical	Critical precedence (5)
flash	Flash precedence (3)

Value	List of Precedence Values
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)

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **precedence** *precedence-values*	Configures the traffic class by matching packets based on precedence-values. Values are shown in the table above. Use the **not** keyword to match on values that do not match the specified range.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

```
switch# show class-map class_ip_precedence
```

Configuring Protocol Classification

For Layer 3 protocol traffic, you can use the ACL classification match. For more information, see the "Configuring ACL Classification" section.

You can classify traffic based on the protocol arguments described in the table below.

Table 4: match Command Protocol Arguments

Argument	Description
arp	Address Resolution Protocol (ARP)
bridging	Bridging
cdp	Cisco Discovery Protocol (CDP)
clns	Connectionless Network Service (CLNS)
clns_es	CLNS End Systems
clns_is	CLNS Intermediate System
dhcp	Dynamic Host Configuration (DHCP)
isis	Intermediate system to intermediate system (IS-IS)
ldp	Label Distribution Protocol (LDP)
netbios	NetBIOS Extended User Interface (NetBEUI)

A maximum of eight different protocols (in the table above) can be matched at a time.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **protocol** {**arp** | **bridging** | **clns** | **clns_is** | **dhcp** | **isis** | **netbios** | **cdp** | **clns_es** | **ldp**}	Configures the traffic class by matching packets based on the specified protocol. Use the not keyword to match on protocols that do not match the protocol specified.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

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

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 by using the **set qos-group** command as described in the "Configuring QoS Group Marking" section.

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

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **qos-group** *multi-range-qos-group-values*	Configures the traffic class by matching packets based on a list of QoS group values. Values can range from 1 to 126. Use the **not** keyword to match on values that do not match the specified range.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

```
switch# show class-map class_qos_group
```

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 "Configuring Discard Class Marking" section.

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **discard-class** *multi-range-discard-class-values*	Configures the traffic class by matching packets based on the 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.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

```
switch# show class-map class_discard_class
```

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

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **packet length** *packet-length-list*	Configures the traffic class by matching packets based on various packet lengths. Values can range from 1 to 9198. Use the **not** keyword to match on values that do not match the specified range.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

```
switch# show class-map class_packet_length
```

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.

Note The **match cos** command is not supported in the egress direction.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic,

	Command or Action	Purpose
		hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **cos** *cos-list*	Configures the traffic class by matching packets based on 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.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

```
switch# 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.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **ip rtp** *udp-port-value*	Configures 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.

	Command or Action	Purpose
		Use the **not** keyword to match on values that do not match the specified range.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

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

Configuring Class Map Classification

You must create a referenced class map prior to its reference. 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.

You can classify traffic based on the match criteria in another class map. You can reference the same class map in multiple policies.

Follow these guidelines while configuring the class-map classification:

- To perform a logical OR with the class map 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 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

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*	Creates or accesses the class map named class-map-name and enters class-map mode. The *class map name* can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.
Step 3	switch(config-cmap-qos)# **match** [**not**] **class-map** *class-map-name*	Configures the traffic class by matching packets based on the match criteria in another class map. Because **match-all** is the default for the **class-map** command, the match criteria specified in class_map3 are ANDed with the match criteria in class_class_map.

	Command or Action	Purpose
		Use the **not** keyword to match on values that do not match the specified range.
Step 4	switch(config-cmap-qos)# **exit**	Exits global class-map queuing mode, and enters configuration mode.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves this configuration change.

Example

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

```
switch# show class-map class_class_map
```

Verifying the Classification Configuration

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

```
switch# show class-map
...
```

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
```

Feature History for Classification

The table below summarizes the new and changed features for this document and shows the releases in which each feature is supported. Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 5: Feature History for Classification

Feature Name	Release	Feature Information
No changes from Release 4.2(1)	5.1(1)	—
Classification	4.2(1)	You can now match IPv4 and IPv6 ACLs.