Control Plane Logging

First Published: February 27, 2006
Last Updated: February 27, 2006

The Cisco IOS Control Plane Protection features allow you to filter and rate-limit the packets that are going to the router's control plane, and discard malicious and or error packets. The addition of the Control Plane Logging feature enables logging of the packets that are dropped or permitted by these features. You can turn on logging for all or some packets that are processed by the control plane, without feature or class restrictions, or you can enable logging for specific Control Plane Protection features such as control plane policing, port-filtering, and queue-thresholding. The Control Plane Logging feature provides the logging mechanism that is needed to efficiently deploy, monitor, and troubleshoot Control Plane Protection features.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the Feature Information for Control Plane Logging, page 28.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Control Plane Logging

- You understand the principles of control plane policing and how to classify control-plane traffic.
- You understand the concepts and general configuration procedures for control plane protection, including control plane policing, port-filtering, and queue-threshold.
- You understand the concepts and general configuration procedure for applying QoS policies on a router (class map and policy map).

For information about control plane policing and its capabilities, see the *Control Plane Policing* section of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4.

For information about control plane protection and its capabilities, see the *Control Plane Protection* documentation.

For information about Cisco IOS QoS and the procedure for configuring QoS in your network using the modular QoS command-line interface (MQC), see the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4.

Restrictions for Control Plane Logging

- The Control Plane Logging feature logs control-plane packets only. This feature does not log data-plane traffic that traverses the router on non-control-plane interfaces.
- The Control Plane Logging feature logs IPv4 packets only. IPv6 packet logging is not supported.
- Control plane logging is supported only on platforms that support control plane protection.
- Packets permitted or dropped by the Management Plane Protection (MPP) feature can be logged only via the Global Control Plane Logging mechanism. Feature-specific or class-specific control plane logging cannot be used to log MPP traffic.
- Global control plane logging can log only dropped or error packets on the aggregate control-plane interface as a result of a control plane policing policy applied to the aggregate interface. To log allowed packets, you must apply the global control-plane logging policy to the host, transit, or cef-exception control-plane subinterface, or you must use feature-specific or class-specific logging.
- A packet that passes through the control plane can be logged only once using this feature. The state printed in the log message (PERMIT or DROP) is the final state of the packet on the control plane. For example, if there is a control-plane protection policy on the aggregate control-plane interface and another on the host control-plane subinterface, with logging enabled on both, a packet that is allowed by both features will be logged only once (with a state of PERMIT). So a state of PERMIT when logged for a packet means that the packet was allowed by all control-plane protection features.
- Although logging control-plane traffic provides valuable insight into the details of control-plane traffic, logging excessive control-plane traffic might result in an overwhelming number of log entries and possibly high router CPU usage. Use control plane logging for short periods of time and only when needed to help classify, monitor, and troubleshoot control-plane traffic and features.

Information About Control Plane Logging

To configure the Control Plane Logging feature, you should understand the following concepts:

Global Control Plane Logging

Global Control Plane Logging is a feature that allows logging of all or some packets processed by the control plane, without feature or class restrictions. This can be used to log all, or a subset of, traffic permitted or dropped by the Control Plane Protection Features. Packets to be logged can be filtered based on the basis of multiple match criteria (that is input interface, source IP address, or destination IP address). The list of supported match criteria can be found in the "How to Configure Logging on a Control Plane Interface" section on page 4.

Logging policies can also log packets on the basis of the action taken on them (that is, dropped or permitted) by control plane features (that is, control plane policing, port-filtering or per-protocol queue-thresholding). Packets that are dropped by the control-plane infrastructure because of checksum errors can also be filtered and logged. If you have not specified the kind of packet to be logged via the "permitted," "dropped," or "error" action match criteria, all packets (permitted, dropped, and error) will be considered for logging.

By default, the log messages contain source IP address, destination IP address, protocol name (IP/TCP/UDP), action (permit, drop, error), and port number. Additionally, there are options that can be configured with the log action that can enable logging of other fields in the IP header as well, such as TTL and packet length. There is also an option to configure the rate-limit interval for which log messages are created; that is, the interval between the logging of two messages.

The Global Control Plane Logging feature is configured using new MQC class-map, policy-map, and service-policy types and can be applied on the aggregate control-plane interface or on a specific control-plane subinterface (that is, host, transit, or cef-exception).

Feature-Specific or Class-Specific Logging

Feature-specific or class-specific logging tracks only packets that match a specific class and that are acted upon by a specific control plane protection feature (that is, control plane policing, port-filtering, or per-protocol queue-thresholding). This type of logging differs from global logging, which allows you to log all packets on a control-plane interface. With global logging, traffic that matches individual classes within a control plane protection feature policy cannot be distinguished. Global logging, for example, can log only all packets dropped on a control-plane interface as a whole. However, with feature-specific or class-specific logging, packets that match a specific class and that are acted upon by a specific control plane protection feature will be separated out. Feature-specific or class-specific logging may be most valuable during the initial stages of control plane protection deployment, when there is a need to know details about packets that match a specific class. For example, knowing what traffic is hitting your class-default class would help in modifying your class maps or policy maps to account for stray packets or for determining characteristics of an attack.

Feature-specific or class-specific logging provides feature-specific logging, making it possible to log packets for a specific feature on a specific control-plane interface (for example, port-filtering on the control-plane host interface).

Feature-specific or class-specific logging allows logging of packets that pass through a class map in a control plane protection feature service policy applied to a control-plane interface. When a feature, such as control plane policing, is applied on a control-plane interface, feature-specific or class-specific logging can be added as one of the actions to be performed on a class defined in the feature policy map. When logging is added as an action for a class inside a policy map, all packets that match that class will be logged. The only packets filtered are those that the feature class map supports. There is no further classification done for logging specifically. The **log** action keyword can be added by itself without any other policing actions defined in the class, or it can be added in addition to the police or drop action defined in the class. When the **log** keyword is added as an action for a class inside a policy map, all packets (permitted and/or dropped) that match the class will be logged.

By default, the log messages contain source IP address, destination IP address, protocol name (IP/TCP/UDP), action (permit, drop, error), and port number. Additionally, there are options that can be configured with the log action that can enable logging of other fields in the IP header as well, such as TTL and packet length. There is also an option to configure the rate-limit interval for which log messages are created; that is, the interval between the logging of two messages.

How to Configure Logging on a Control Plane Interface

You can configure control plane logging for global logging and/or for feature-specific or class-specific logging.

- Configuring Global Logging, page 4
- Configuring Feature-Specific or Class-Specific Logging, page 9
- Verification Examples for Control Plane Logging, page 11

Configuring Global Logging

To support global control plane logging, new MQC class-map, policy-map, and service-policy types were created. Policy-map type logging is used only for global control plane logging policies. Class-map type logging is used to classify what type of control-plane traffic you want to log. The logging type class maps support a subset of generic QoS match criteria and some control-plane-specific match criteria. The supported match criteria are as follows:

- input-interface
- IPv4 source IP address
- IPv4 destination IP address
- packets dropped
- packets permitted
- packets error

If one of the packet-action filters, packets dropped, packets permitted, or packets error, is not specified, all matching packets will be logged irrespective of the action taken on them (permitted or dropped).

Also, in a logging type policy map, the only action supported is log. The configuration and behavior of the **log** action keyword are the same in global logging and feature-specific or class-specific logging. The available options for the **log** action keyword are as follows:

- interval—Sets packet logging interval.
- ttl—Logs ttl for IPv4 packets.
- total-length—Logs packet length for IPv4 packets.

The tasks for configuring global logging include the following:

- Defining Packet Logging Classification Criteria, page 5 (required)
- Defining the Logging Policy Map, page 6 (required)
- Creating a Logging Service Policy on a Control Plane Interface, page 7 (required)

Note Logging policies can be applied to the control plane, control-plane host, control-plane transit, and control-plane cef-exception interfaces.

Defining Packet Logging Classification Criteria

When configuring global logging, you must first define the packet logging classification criteria.

Restrictions

You can apply global logging policies on control plane interfaces only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging**}] [**match-all** | **match-any**] *class-map-name*
4. **match** [**input-interface** | **ipv4 source-address** | **ipv4 destination-address** | **not input-interface** | **packets permitted** | **packets dropped** | **packets error**]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**class-map** [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging**}] [**match-all** | **match-any**] *class-map-name* **Example:** `Router(config)# class-map type logging match-all log-class`	Creates a class map used to match packets to a specified class and enters class-map configuration mode. The following keywords and arguments can be used for control plane logging: • **type**—(Optional) Identifies the class-map type. Use the **logging** keyword for control plane logging configurations. • **match-all**—(Optional) Performs a logical AND on the match criteria. • **match-any**—(Optional) Performs a logical OR on the match criteria. • *class-map name*—Name of a class. The name can be a maximum of 40 alphanumeric characters.
Step 4	**match** [**input-interface** | **ipv4 source-address** | **ipv4 destination-address** | **not input-interface** | **packets permitted** | **packets dropped** | **packets error**] **Example:** `Router(config-cmap)# match packets dropped`	Defines the match criteria for the logging class map.
Step 5	**end** **Example:** `Router(config-cmap)# end`	Exits class-map configuration mode and returns to privileged EXEC mode.

Defining the Logging Policy Map

After you define packet logging criteria for global logging, you must define the logging policy map.

To configure global logging policy maps, use the new **policy-map type logging** configuration command. Then, use the **class** command, to associate a logging class-map that was configured with the **class-map type logging** command, with the logging policy map. Use the **log** keyword to configure the log action for the class that you associated with the policy map. The **class** command must be issued after entering the policy-map configuration mode. After entering the **class** command, you are automatically in policy-map class configuration mode. The action log can be configured while in policy-map class configuration mode.

Restrictions

You can apply global logging policies on control plane interfaces only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging**}] *policy-map-name*
4. **class** *class-name*

5. **log** [**interval** *seconds* | **total-length** | **ttl**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging**}] *policy-map-name* **Example:** `Router(config)# policy-map type logging log-policy`	Creates the logging service policy and enters policy-map configuration mode. • **type**—(Optional) Identifies the policy-map type. Use the **logging** keyword for control plane logging configurations. • *policy-map-name*—Name of a policy map. The name can be a maximum of 40 alphanumeric characters.
Step 4	**class** *class-name* **Example:** `Router(config-pmap)# class log-class`	Associates a class with a policy map and enters class-map configuration mode. • *class-name*—Name of a class of type logging. The name can be a maximum of 40 alphanumeric characters.
Step 5	**log** [**interval** *seconds* | **total-length** | **ttl**] **Example:** `Router(config-pmap-c)# log interval 1000`	Applies the log action to the logging class. With this command, you can enter the following optional parameters: • **interval** *seconds*—(Optional) Sets packet logging interval. • **total-length**—(Optional) Logs packet length for IPv4 packets. • **ttl**—(Optional) Logs ttl for IPv4 packets.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Exits from class-map configuration mode and returns to privileged EXEC mode.

Creating a Logging Service Policy on a Control Plane Interface

After you define the logging service policy, you must apply the policy to a specific control plane interface.

Restrictions

You can apply global logging policies on control plane interfaces only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane** [**host** | **transit** | **cef-exception** | **cr**]
4. **service-policy type logging input** *logging-policy-map-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**control-plane** [**host** | **transit** | **cef-exception** | **cr**] **Example:** `Router(config)# control-plane host`	Enters control-plane configuration mode. • **host**—(Optional) Applies policies to control-plane host subinterface. • **transit**—(Optional) Applies policies to control-plane transit subinterface. • **cef-exception**—(Optional) Applies policies to control-plane cef-exception subinterface. • **cr**—(Optional) Applies policies to all control-plane interfaces.
Step 4	**service-policy type logging input** *logging-policy-map-name* **Example:** `Router(config-cp)# service-policy type logging input log-policy`	Applies a logging policy to a control-plane interface. • **input**—Applies the specified service policy to packets received on the control plane. • *logging-policy-map-name*—Name of a logging policy map (created by using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters.
Step 5	**end** **Example:** `Router(config-cp)# end`	Exits control-plane configuration mode and returns to privileged EXEC mode.

Configuring Feature-Specific or Class-Specific Logging

Feature-specific or class-specific control plane logging is implemented as an integrated part of Cisco's Control Plane Protection features, such as per-protocol queue-thresholding, port-filter, or control plane policing, as an action within their respective policy maps. To enable feature-specific or class-specific control plane logging, the log action should be added to the existing Control Plane Protection feature policy map.

The default behavior for a policy with the log action is to log matching packets. By default, the log messages contain source IP address, destination IP address, protocol name (IP/TCP/UDP), action (permit, drop, error), and port number. Additionally, there are options that can be configured with the log action that can enable logging of other fields in the IP header as well, such as TTL and packet length. There is also an option to configure the rate-limit interval for which log messages are created, that is the interval between the logging of two messages.

The additional options for the **log** action keyword are as follows:

- interval—Sets packet logging interval.
- ttl—Logs ttl for Ipv4 packets.
- total-length—Logs packet length for IPv4 packets.

Restrictions

The log action can be added only to policy maps of control-plane protection features, which are control plane policing, port-filtering, and queue-thresholding.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging**}] *policy-map-name*
4. **class** *class-name*
5. **log** [**interval** *seconds* | **total-length** | **ttl**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**policy-map** [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging**}] *policy-map-name* **Example:** `Router(config)# policy-map type queue-threshold qt-policy`	Creates a policy map and enters policy-map configuration mode. • **type**—(Optional) Specifies the service policy type. • **port-filter**—(Optional) Enters the policy map for the port-filter feature. • **queue-threshold**—(Optional) Enters the policy map for the queue-threshold feature. • **logging**—(Optional) Enters policy-map configuration mode for the control plane logging feature. • *policy-map-name*—Name of the policy map. The name can be a maximum of 40 alphanumeric characters.
Step 4	**class** *class-name* **Example:** `Router(config-pmap)# class qt-host`	Associates a class with a policy and enters class map configuration mode.
Step 5	**log** [**interval** *seconds* | **total-length** | **ttl**] **Example:** `Router(config-pmap-c)# log interval 1000`	Applies the log action to the service-policy class. You can configure the following additional parameters: • **interval** *seconds*—(Optional) Sets packet logging interval. • **total-length**—(Optional) Logs packet length for IPv4 packets. • **ttl**—(Optional) Logs ttl for IPv4 packets.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Exits class-map configuration mode and returns to privileged EXEC mode.

Verifying Control Plane Logging Information

You can verify control plane logging for both global logging configurations and feature-specific or class-specific configurations.

To display active control plane logging information for global logging, perform the following optional steps.

SUMMARY STEPS

1. **enable**
2. **show policy-map type logging control-plane** [**host** | **transit** | **cef-exception** | **cr**]
3. **show policy-map** [**type** *policy-type*] **control-plane** [**host** | **transit** | **cef-exception** | **all** | **cr**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show policy-map type logging control-plane** [**host** | **transit** | **cef-exception** | **cr**] **Example:** `Router# show policy-map type logging control-plane host`	Display information for global control plane logging.
Step 3	**show policy-map** [**type** *policy-type*] **control-plane** [**host** | **transit** | **cef-exception** | **all** | **cr**] **Example:** `Router# show policy-map type logging control-plane host`	Display information for feature-specific or class-specific control plane logging. **Note** The example shows feature-specific or class-specific logging enabled on a port-filter policy.

Verification Examples for Control Plane Logging

This section provides the following examples:

- Sample Output for a Global Logging Configuration: Example, page 11
- Sample Output for a Feature-Specific or Class-Specific Configuration: Example, page 12
- Sample Log Output: Example, page 12

Sample Output for a Global Logging Configuration: Example

The following output displays the global logging service policy that was just added to the control-plane host feature path interface:

```
Router# show policy-map type logging control-plane host
 Control Plane Host
  Service-policy logging input: cpplog-host-policy
    Class-map: cpplog-host-map (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  packets dropped
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match:  packets permitted
        0 packets, 0 bytes
        5 minute rate 0 bps


    Class-map: class-default (match-any)
      0 packets, 0 bytes
```

```
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Sample Output for a Feature-Specific or Class-Specific Configuration: Example

The following output displays the logging policy map that was just added to the control-plane host feature path interface:

```
Router# show policy-map cpp-policy
  Policy Map cpp-policy
    Class cppclass-igp
    Class cppclass-management
     police rate 250 pps burst 61 packets
       conform-action transmit
       exceed-action drop
    Class cppclass-monitoring
     police rate 100 pps burst 24 packets
    conform-action transmit
       exceed-action drop
  Class cppclass-undesirable
      drop
      log interval 5000
    Class class-default
     police rate 50 pps burst 12 packets
       conform-action transmit
       exceed-action drop
```

Sample Log Output: Example

The following example shows log output for a configuration that sends IP traffic to the router:

```
Router#
%CP-6-IP: PERMIT ttl=59 length=20 209.165.200.225 -> 209.165.200.254
%CP-6-IP: PERMIT ttl=59 length=20 209.165.200.225 -> 209.165.200.254
%CP-6-IP: PERMIT ttl=59 length=20 209.165.200.225 -> 209.165.200.254
%CP-6-IP: PERMIT ttl=59 length=20 209.165.200.225 -> 209.165.200.254
```

The following is a description of the log information displayed in the preceeding example:

- IP denotes the kind of traffic received.
- PERMIT means that no control-plane feature dropped the packet.
- ttl gives the ttl value in the IP header.
- length gives the total-length field in the IP header.
- 209.165.200.225 is the source IP address.
- 209.165.200.254 is the destination IP address.

The following example shows log output for a configuration that sends TCP traffic to the router:

```
Router#
%CP-6-TCP: PERMIT ttl=59 length=40 209.165.200.225(18611) -> 209.165.200.254(23)
%CP-6-TCP: PERMIT ttl=59 length=40 209.165.200.225(18611) -> 209.165.200.254(23)
%CP-6-TCP: PERMIT ttl=59 length=40 209.165.200.225(18611) -> 209.165.200.254(23)
%CP-6-TCP: PERMIT ttl=59 length=40 209.165.200.225(18611) -> 209.165.200.254(23)
```

The following is a description of the log information displayed in the preceding example:

- TCP denotes the kind of traffic received.
- PERMIT means that no control-plane feature dropped the packet.
- ttl gives the ttl value in the IP header.
- length gives the total-length field in the IP header.
- 209.165.200.225 is the source IP address.
- 18611 is the source TCP port.
- 209.165.200.254 is the destination IP address.
- 23 is the destination TCP port.

Configuration Examples for Control Plane Logging

This section provides the following configuration examples:

- Configuring Global Control Plane Logging for Dropped and Permitted Packets: Example, page 13
- Configuring Global Control Plane Logging for Dropped Packets: Example, page 14
- Configuring Logging for a Specific Class: Example, page 15
- Configuring Logging for a Port-Filter Policy Map: Example, page 16

Configuring Global Control Plane Logging for Dropped and Permitted Packets: Example

The following example shows how to configure a global control-plane logging service policy to log all dropped and permitted packets that hit the control-plane host feature path only, regardless of the interface from which the packets enter the router. Also, the router rate-limits the log messages to one every 5 seconds.

```
! Define a class map of type logging to specify what packets will be logged.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map type logging match-any cpplog-host-map
Router(config-cmap)# match packets dropped
Router(config-cmap)# match packets permitted
Router(config-cmap)# exit
! Define a policy map of type logging using your logging class map and rate-limit log
messages to one every 5 seconds.
Router(config)# policy-map type logging cpplog-host-policy
Router(config-pmap)# class cpplog-host-map
Router(config-pmap-c)# log interval 5000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Apply the new logging policy map to the control-plane host feature path interface.
Router(config)# control-plane host
Router(config-cp)# service-policy type logging input cpplog-host-policy
```

```
Router(config-cp)# end
Router#
Aug  8 17:57:57.359: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
```

The following output displays the logging policy map that was just added to the control-plane host feature path interface:

```
Router# show policy-map type logging control-plane host
 Control Plane Host
  Service-policy logging input: cpplog-host-policy
    Class-map: cpplog-host-map (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:  packets dropped
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match:  packets permitted
        0 packets, 0 bytes
        5 minute rate 0 bps
      log interval 5000
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Configuring Global Control Plane Logging for Dropped Packets: Example

The following example shows how to configure a global control-plane logging service policy to log all dropped packets that come from GigabitEthernet interface 0/3 that hit the aggregate control-plane interface.

```
! Define a class map of type logging to specify what packets will be logged.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map type logging match-all cpplog-gig
Router(config-cmap)# match input-interface gigabitethernet 0/3
Router(config-cmap)# match packets dropped
Router(config-cmap)# exit
! Define a policy map of type logging using your logging type class map.
Router(config)# policy-map type logging cpplog-gig-policy
Router(config-pmap)# class cpplog-gig
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Apply the new logging policy map to the aggregate control-plane interface.
Router(config)# control-plane
```

```
Router(config-cp)# service-policy type logging input cpplog-gig-policy
Router(config-cp)# end
Router#
Aug  8 12:53:08.618: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
```

The following output displays the logging policy map that was just added to the aggregate control-plane interface:

```
Router# show policy-map type logging control-plane
 Control Plane
  Service-policy logging input: cpplog-gig-policy
    Class-map: cpplog-gig (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: input-interface GigabitEthernet0/3
      Match:  dropped-packets
      log
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Configuring Logging for a Specific Class: Example

The following example shows how to configure class-specific control plane logging for a specific class configured in a control plane policing service policy. This example also shows how to configure rate-limiting of logs to output only one log message every 5 seconds. For this example, you have a control plane policing service policy with classes defined for Interior Gateway Protocol (IGP), management, monitoring and, undesirable traffic. The undesirable class is configured to match packets that are destined to the router on UDP port 1434. The service policy is configured to drop all packets that hit the undesirable class (in this case, packets that are destined for port 1434). For this example, you want to log all packets being dropped by the undesirable class, so that you will be aware that you are being attacked by 1434 packets.

In this example, you have the following control plane policing service policy configured:

```
Router# show policy-map cpp-policy
  Policy Map cpp-policy
    Class cppclass-igp
    Class cppclass-management
     police rate 250 pps burst 61 packets
       conform-action transmit
       exceed-action drop
    Class cppclass-monitoring
     police rate 100 pps burst 24 packets
       conform-action transmit
       exceed-action drop
    Class cppclass-undesirable
      drop
```

```
    Class class-default
     police rate 50 pps burst 12 packets
       conform-action transmit
       exceed-action drop
```

To log all traffic for the undesirable class in the above service policy, perform the following steps:

```
! Enter control plane policing policy-map configuration mode.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map cpp-policy
! Enter policy-map class configuration mode for the undesirable class.
Router(config-pmap)# class cppclass-undesirable
! Configure the log keyword with a rate limit of one log message every 5 seconds.
Router(config-pmap-c)# log interval 5000
Router(config-pmap-c)# end
```

Use the following command to verify that the log action has been added to the policy map under the undesirable class:

```
Router# show policy-map cpp-policy
  Policy Map cpp-policy
    Class cppclass-igp
    Class cppclass-management
     police rate 250 pps burst 61 packets
       conform-action transmit
       exceed-action drop
    Class cppclass-monitoring
     police rate 100 pps burst 24 packets
    conform-action transmit
       exceed-action drop
  Class cppclass-undesirable
      drop
      log interval 5000
    Class class-default
     police rate 50 pps burst 12 packets
       conform-action transmit
       exceed-action drop
```

Configuring Logging for a Port-Filter Policy Map: Example

The following example shows how to configure class-specific control plane logging for a specific class configured in a Control Plane Protection port-filter policy map. This example also shows how to configure logging to display the packet-length field from the IP header for each packet that hits the port-filter class. For this example, you have a port-filter policy map configured to drop all traffic that is destined to closed TCP/UDP ports. For this example, you want to log all packets that are being dropped or allowed by the port-filter class.

In this example, you have the following port-filter service policy configured and applied to your control-plane host feature path. This policy blocks all traffic that is destined to closed or unlistened TCP/UDP ports:

```
Router# show policy-map type port-filter
  Policy Map type port-filter pf-closed-port-policy
    Class pf-closed-ports
      Drop
```

The corresponding port-filter type class map that is used in the above port-filter policy map is configured as follows:

```
Router# show class-map type port-filter
Class Map type port-filter match-all pf-closed-ports (id 19)
   Match  closed-ports
```

To log all traffic that is processed by the above pf-closed-ports class map in the above pf-closed-port-policy port-filter policy map, perform the following steps:

```
! Enter port-filter policy-map configuration mode.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map type port-filter pf-closed-port-policy
! Enter port-filter policy-map class configuration mode for the undesirable class.
Router(config-pmap)# class pf-closed-ports
! Configure the log keyword with the option to log the packet-length field in the IP
header.
Router(config-pmap-c)# log total-length
Router(config-pmap-c)# end
```

Use the following command to verify that the log action has been added to the port-filter policy map under the appropriate class:

```
Router# show policy-map type port-filter
  Policy Map type port-filter pf-closed-port-policy
    Class pf-closed-ports
    drop
      log interval 1000 total-length
```

Additional References

The following sections provide references related to the Control Plane Logging feature.

Related Documents

Related Topic	Document Title
QoS information and configuration tasks	*Cisco IOS Quality of Service Solutions Configuration Guide*

Related Topic	Document Title
Additional QoS commands	*Cisco IOS Quality of Service Solutions Command Reference*, Release 12.4T
Control Plane Protection	*Cisco IOS Control Plane Protection* feature documentation, Release 12.4(4)T

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents only modified commands.

- **class-map**
- **debug control-plane**
- **policy-map**

class-map

To create a class map to be used for matching packets to a specified class, use the **class-map** command in global configuration mode. The **class-map** command enters class-map configuration mode in which you can enter one of the **match** commands to configure the match criteria for this class. To remove an existing class map from the router, use the **no** form of this command.

class-map [**type** {**stack | access-control | port-filter | queue-threshold | logging**}] [**match-all | match-any**] *class-map-name*

no class-map [**type** {**stack | access-control | port-filter | queue-threshold | logging**}] [**match-all | match-any**] *class-map-name*

Syntax Description

type stack	(Optional) Enables the flexible packet matching (FPM) functionality to determine the correct protocol stack to examine. If the appropriate protocol header description files (PHDFs) have been loaded onto the router (via the **load protocol** command), a stack of protocol headers can be defined so that the filter can determine which headers are present and in what order.
type access-control	(Optional) Determines the exact pattern to look for in the protocol stack of interest. **Note** You must specify a stack class map (via the **type stack** keywords) before you can specify an access-control class map (via the **type access-control** keywords).
type port-filter	(Optional) Creates a port-filter class-map that enables the TCP/UDP port policing of control plane packets. When enabled, it provides filtering of traffic destined to specific ports on the control plane host subinterface.
type queue-threshold	(Optional) Enables queue thresholding that limits the total number of packets for a specified protocol that are allowed in the control plane IP input queue. This feature applies only to the control plane host subinterface.
type logging	(Optional) Enables logging of packet traffic on the control plane.
match-all | match-any	(Optional) Determines how packets are evaluated when multiple match criteria exist. Packets must either meet all of the match criteria (**match-all**) or one of the match criteria (**match-any**) in order to be considered a member of the class.
class-map-name	Name of the class for the class map. The name can be a maximum of 40 alphanumeric characters. The class name is used for both the class map and to configure policy for the class in the policy map.

Command Default

The default is to have no class map configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.4(4)T	The **type stack** and **type access-control** keywords were added to support FPM. The **type port-filter** and **type queue-threshold** keywords were added to support Control Plane Protection.
12.4(6)T	The **type logging** keyword was added to support control plane packet logging.

Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class-map match criteria. The **class-map** command enters class-map configuration mode in which you can enter one of the **match** commands to configure the match criteria for this class. Packets that arrive at either the input or output interface (determined by how the **service-policy** command is configured) are checked against the match criteria configured for a class map to determine if the packet belongs to that class.

When configuring a class map, you can use one or more **match** commands to specify match criteria. For example, you can use the **match access-group** command, the **match protocol** command, or the **match input-interface** command. The **match** commands vary according to the Cisco IOS release. For more information about match criteria and **match** commands, see the "Modular Quality of Service Command-Line Interface (CLI)" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example specifies class101 as the name of a class, and it defines a class map for this class. The class called class101 specifies policy for traffic that matches access control list 101.

```
Router(config)# class-map class101
Router(config-cmap)# match access-group 101
```

The following example shows how to define FPM traffic classes for slammer and UDP packets. The match criteria defined within the class maps are for slammer and UDP packets with an IP length not to exceed 404 bytes, UDP port 1434, and pattern 0x4011010 at 224 bytes from the start of the IP header.

```
Router(config)# load protocol disk2:ip.phdf
Router(config)# load protocol disk2:udp.phdf

Router(config)# class-map type stack match-all ip-udp
Router(config-cmap)# description "match UDP over IP packets"
Router(config-cmap)# match field ip protocol eq 0x11 next udp
Router(config-cmap)# exit

Router(config)# class-map type access-control match-all slammer
Router(config-cmap)# description "match on slammer packets"
Router(config-cmap)# match field udp dest-port eq 0x59A
Router(config-cmap)# match field ip length eq 0x194
Router(config-cmap)# match start 13-start offset 224 size 4 eq 0x4011010
```

The following example shows how to configure a port-filter policy to drop all traffic destined to closed or "nonlistened" ports except SNMP.

```
Router(config)# class-map type port-filter pf-class
Router(config-cmap)# match not port udp 123
```

```
Router(config-cmap)# match closed-ports
Router(config-cmap)# exit
Router(config)# policy-map type port-filter pf-policy
Router(config-pmap)# class pf-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# end
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
class class-default	Specifies the default class for a service policy map.
match (class-map)	Configures the match criteria for a class map on the basis of port filter and/or protocol queue policies.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or virtual circuit (VC) or to an output interface or VC to be used as the service policy for that interface or VC.

debug control-plane

To display debugging output from the control-plane routines, use the **debug control plane** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug control-plane [**all** | **host** | **port-filtering** | **queue-thresholding** | **log** | **management-interface**]

no debug control-plane [**all** | **host** | **port-filtering** | **queue-thresholding** | **log** | **management-interface**]

Syntax Description

all	(Optional) Displays all events on all control-plane interfaces.
host	(Optional) Displays all events on the control-plane host interface.
port-filtering	(Optional) Displays TCP/IP protocol port-filtering events.
queue-thresholding	(Optional) Displays TCP/IP protocol queue-thresholding events.
log	(Optional) Displays control-plane logging events.
management-interface	(Optional) Displays all events on the control-plane management interface.

Command Default

Control-plane debugging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.4(6)T	The **log** and **management-interface** keywords were added to support control-plane logging.

Examples

The following example show a display from the **debug control-plane** command:

```
Router# debug control-plane
Control-plane infrastructure events debugging is on
Router# cp_receive_classify - marking pak host
 ingress pak marked cef-exception
```

The following example shows a display from the **debug control-plane** command using the port-filtering option:

```
Router# debug control-plane port-filtering
TCP/IP Port filtering events debugging is on
Dropped UDP dport 1243 sport 62134 saddr 209.165.200.225
```

Table 1 describes the significant fields shown in the display.

Table 1 debug control plane field descriptions

Field	Description
dport	UPD destination port.
sport	UPD source port.
saddr	Source address of the IP packets.

Related Commands

Command	Description
clear control-plane	Clears packet counters for control-plane interfaces and subinterfaces.
control-plane	Enters control-plane configuration mode, which allows users to associate or modify attributes or parameters that are associated with the control plane of the device.
show control-plane cef-exception counters	Displays the control plane packet counters for the control plane CEF-exception subinterface.
show control-plane cef-exception features	Displays the configured features for the control plane CEF-exception subinterface.
show control-plane counters	Displays the control-plane packet counters for the aggregate control-plane interface.
show control-plane features	Displays the configured features for the aggregate control-plane interface.
show control-plane host counters	Displays the control plane packet counters for the control plane host subinterface.
show control-plane host features	Displays the configured features for the control plane host subinterface.
show control-plane host open-ports	Displays a list of open TCP/UDP ports that are registered with the port-filter database.
show control-plane transit counters	Displays the control plane packet counters for the control plane transit subinterface.

policy-map

To create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map** command in global configuration command. The **policy-map** command enters QoS policy-map configuration mode in which you can configure or modify the class policies for that policy map. To delete a policy map, use the **no** form of this command.

policy-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging**}]
policy-map-name

no policy-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging**}]
policy-map-name

Syntax Description

type stack	(Optional) Determines the exact pattern to look for in the protocol stack of interest.
type access-control	(Optional) Enables the policy map for the flexible packet matching feature.
type port filter	(Optional) Enables the policy map for the port-filter feature.
type queue-threshold	(Optional) Enables the policy map for the queue-threshold feature.
type logging	(Optional) Enables the policy map for the control plane packet logging feature.
policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.

Command Default

There are no default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(4)T	The **type access-control** keyword was added to support flexible packet matching. The **type port-filter** and **type queue-threshold** keywords were added to support control plane protection.
12.4(6)T	The **type logging** keyword was added to support control plane packet logging.

Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added to, or modified before you onfigure policies for classes whose match criteria are defined in a class map. The **policy-map** command enters QoS policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. You use the **class-map** and **match** commands to configure the match criteria for a class. Because you can configure a maximum of 64 class maps, no policy map can contain more than 64 class policies.

A single policy map can be attached to multiple interfaces concurrently. When you attempt to attach a policy map to an interface, the attempt is denied if the available bandwidth on the interface cannot accommodate the total bandwidth requested by class policies comprising the policy map. In this case, if the policy map is already attached to other interfaces, it is removed from them.

Whenever you modify class policy in an attached policy map, class-based weighted fair queueing (CBWFQ) is notified and the new classes are installed as part of the policy map in the CBWFQ system.

Examples

The following example creates a policy map called policy1 and configures two class policies included in that policy map. The class policy called class1 specifies policy for traffic that matches access control list (ACL) 136. The second class is the default class to which packets that do not satisfy configured match criteria are directed.

```
! The following commands create class-map class1 and define its match criteria:
Router(config)# class-map class1
Router(config-cmap)# match access-group 136

! The following commands create the policy map, which is defined to contain policy
! specification for class1 and the default class:
Router(config)# policy-map policy1

Router(config-pmap)# class class1
Router(config-pmap)# bandwidth 2000
Router(config-pmap)# queue-limit 40

Router(config-pmap)# class class-default
Router(config-pmap)# fair-queue 16
Router(config-pmap)# queue-limit 20
```

The following example creates a policy map called policy9 and configures three class policies to belong to that map. Of these classes, two specify policy for classes with class maps that specify match criteria based on either a numbered ACL or an interface name, and one specifies policy for the default class called class-default to which packets that do not satisfy configured match criteria are directed.

```
Router(config)# policy-map policy9

Router(config-pmap)# class acl136
Router(config-pmap)# bandwidth 2000
Router(config-pmap)# queue-limit 40

Router(config-pmap)# class ethernet101
Router(config-pmap)# bandwidth 3000
Router(config-pmap)# random-detect exponential-weighting-constant 10

Router(config-pmap)# class class-default
Router(config-pmap)# fair-queue 10
Router(config-pmap)# queue-limit 20
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.

Command	Description
class class-default	Specifies the default class whose bandwidth is to be configured or modified.
class-map	Creates a class map to be used for matching packets to a specified class.
fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
queue-limit	Specifies or modifies the maximum number of packets that the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.
service-policy	Attaches a policy map to an input interface or VC or to an output interface or VC to be used as the service policy for that interface or VC.

Feature Information for Control Plane Logging

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for Control Plane Logging

Feature Name	Releases	Feature Information
Control Plane Logging	12.4(6)T	Allows the control plane features to log all packets that match the class-map entries.

.