Per-Flow Admission

The Per-Flow Admission feature provides explicit controls to limit packet flow into a WAN edge in order to protect already admitted flows on the routing/WAN edge.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and 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 feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Prerequisites for Per-Flow Admission

A class must have bandwidth or priority defined before configuring the Per-Flow Admission feature.

Restrictions for Per-Flow Admission

Per-flow admission is currently supported only on Ethernet and serial interfaces, and Dynamic Multipoint Virtual Private Network (DMVPN) tunnels.

Information About Per-Flow Admission

Overview of Per-Flow Admission

Application (mainly voice and video) quality drops when they are connected from a branch to head quarters and data centers over a WAN because the WAN interface bandwidth is limited and always comes at a premium cost. There are no well-defined controls to restrict flows through a WAN link and no explicit controls to limit the flows to protect already admitted flows. This limitation leads to quality degradation of already admitted flows.

The Per-Flow Admission feature allows operators to understand the number of flows that can be accommodated into an interface without quality degradation. In most deployments, the N+1st flow affects the quality of all existing valid first N flows. The Per-Flow Admission feature enables nodes to automatically learn about flows and their bandwidth as they get accommodated into the interface where bandwidth is at a premium. The network node accommodates only flows that the interface can handle, and it drops flows thereafter.

Benefits of Per-Flow Admission

The following are benefits of integrating the Per-Flow Admission feature to Quality of Service (QoS):

- Makes QoS networks more predictable and robust.
- Requires no end-to-end coordination because per-flow admission is a per-hop decision and each hop makes decision independently.
- Does not require the source to predict the flow rate.
- Ensures a higher probability of getting a reservation in the network.
- Works well with rate adaption because certain parts of the flow may be elastic.
- Promotes better selection of admitted traffic.
- Works at the IP layer.
- Works transparently with other network technologies such as Network Address Translation (NAT).
- Does not allow the source to hog the network.
- Provides benefits for certain endpoints by selecting only certain parts of the flow as admitted.

How to Configure Per-Flow Admission

Configuring a Class Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **metadata flow**
4. **class-map** [**match-all** | **match-any**] *class-map-name*
5. exit
6. **class-map** [**match-all** | **match-any**] *class-map-name*

7. **match dscp** *dscp-value*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**metadata flow** **Example:** `Device(config)# metadata flow`	Enables metadata on all interfaces.
Step 4	**class-map** [**match-all** | **match-any**] *class-map-name* **Example:** `Device(config)# class-map match-all admitted`	Creates a class map for matching traffic to a specified class, and enters class-map configuration mode. • Enter the class map name.
Step 5	exit **Example:** `Device(config-cmap)# exit`	Exits the class-map configuration mode and returns to global configuration mode.
Step 6	**class-map** [**match-all** | **match-any**] *class-map-name* **Example:** `Device(config-cmap)# class-map match-all af4`	Creates a class map to be used for matching traffic to a specified class. • Enter the class map name.
Step 7	**match dscp** *dscp-value* **Example:** `Device(config-cmap)# match dscp af41 af42 af43`	Identifies a specific IP Differentiated Services Code Point (DSCP) value as a match criterion.
Step 8	**end** **Example:** `Device(config-cmap)#end`	Exits class-map configuration mode and returns to privilged EXEC mode.

Configuring a Child Policy Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **set dscp** *dscp-value*
6. **class** {*class-name* | **class-default**}
7. **set dscp** *dscp-value*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Device(config)# policy-map child`	Creates a policy map using the specified name and enters policy-map configuration mode. • Enter the name of the policy map that you want to create.
Step 4	**class** {*class-name*	**class-default**} **Example:** `Device(config-pmap)# class admitted`	Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. • This class is associated with the class map created earlier.
Step 5	**set dscp** *dscp-value* **Example:** `Device(config-pmap-c)# set dscp af41`	Sets the differentiated services code point (DSCP) value in the type of service (ToS) byte and assigns higher priority to admitted traffic by marking up the admitted flow and marking down the un-admitted flow. • Enter the DSCP value.
Step 6	**class** {*class-name*	**class-default**} **Example:** `Device(config-pmap-c)# class un-admitted`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class default class) before you configure its policy.

	Command or Action	Purpose
		• Enter the name of the class or enter the **class-default** keyword. This class will be matched against the **match metadata cac status un-admitted** command.
Step 7	**set dscp** *dscp-value* **Example:** `Device(config-pmap-c)# set dscp af42`	Sets the DSCP value in the ToS byte. Sets higher priority to admitted traffic by marking up the admitted flow and marking down the un-admitted flow. • Enter the DSCP value.
Step 8	**end** **Example:** `Device(config-pmap-c)# end`	Exits policy-map class configuration mode and returns to privileged EXEC mode.

Configuring Per-Flow Admission for a Class

Before you begin

A class must have bandwidth or priority defined before configuring per-flow admission.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*kilobits* | **percent** *percentage*}
6. **admit cac local**
7. **rate** {*kbps* | **percent** *percentage*}
8. **flow rate fixed** *kbps flow-bit-rate*
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**policy-map** *policy-map-name* **Example:** `Device(config)# policy-map test`	Creates a policy map using the specified name and enters policy-map configuration mode. • Enter the name of the policy map that you want to create.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Device(config-pmap)# class af4` **Note** To divide packets into admitted and un-admitted buckets, you must assign the policy map created earlier, under the **class** command that is defined here as a child policy.	Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. • This class is associated with the class map created earlier.
Step 5	**bandwidth** {*kilobits* | **percent** *percentage*} **Example:** `Device(config-pmap-c)# bandwidth 200`	Specifies the bandwidth for a class of traffic belonging to the policy map. • Enter the bandwidth in kbps.
Step 6	**admit cac local** **Example:** `Device(config-pmap-c)# admit cac local`	Enables per-flow admission for this class and enters per-flow admission configuration mode.
Step 7	**rate** {*kbps* | **percent** *percentage*} **Example:** `Device(config-pmap-admit-cac)# rate percent 80`	Configures the size of the bandwidth pool in kbps or as a percentage of output class bandwidth.
Step 8	**flow rate fixed** *kbps flow-bit-rate* **Example:** `Device(config-pmap-admit-cac)# flow rate fixed 100`	Specifies how much bandwidth to allocate for each flow.
Step 9	**end** **Example:** `Device(config-pmap-admit-cac)# end`	Exits per-flow admission configuration mode and returns to privileged EXEC mode.

Attaching a Per-Flow Admission Policy to an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}

5. **service-policy** *policy-map*
6. **end**
7. **configure terminal**
8. **interface** *type number*
9. **ip address** *ip-address mask*
10. **load-interval** *seconds*
11. **service-policy output** *policy-map-name*
12. **no shutdown**
13. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Device(config)# policy-map test`	Creates a policy map using the specified name and enters policy-map configuration mode. • Enter the name of the policy map that you want to create.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Device(config-pmap)# class af4`	Specifies the name of the class whose policy you want to create and enters policy-map class configuration mode. • This class is associated with the class map created earlier.
Step 5	**service-policy** *policy-map* **Example:** `Device(config-pmap-c)# service-policy child`	Attaches the policy map to a class.
Step 6	**end** **Example:** `Device(config-pmap-c)# end`	Exits policy-map class configuration mode and returns to privileged EXEC mode.
Step 7	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 8	**interface** *type number* **Example:** `Device(config)# interface Serial2/0`	Configures the specified interface and enters interface configuration mode. • Enter the interface type and number.
Step 9	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 10.10.100.1 255.255.255.0`	Sets an IP address for an interface.
Step 10	**load-interval** *seconds* **Example:** `Device(config-if)# load-interval 30`	Specifies the interval for load calculation of an interface.
Step 11	**service-policy output** *policy-map-name* **Example:** `Device(config-if)# service-policy output test`	Attaches a policy map to an interface.
Step 12	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Enables the interface.
Step 13	end **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying Per-flow Admission

SUMMARY STEPS

1. **enable**
2. **show policy-map interface** *interface-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show policy-map interface** *interface-name* **Example:** `Device# show policy-map interface serial2/0`	Displays the configuration of all classes configured for all service policies on the specified interface. • Enter the name of the policy map whose complete configuration is to be displayed.

Configuration Examples for Per-Flow Admission

Example: Configuring a Class Map

```
Device> enable
Device# configure terminal
Device(config)# metadata flow
Device(config)# class-map match-all admitted
Device(config-cmap)# match metadata cac status admitted
Device(config-cmap)# class-map match-all af4
Device(config-cmap)# match dscp af41 af42 af43
Device(config-cmap)# end
```

Example: Configuring a Policy Map

```
Device> enable
Device# configure terminal
Device(config)# policy-map child
Device(config-pmap)# class admitted
Device(config-pmap-c)# set dscp af41
Device(config-pmap-c)# class class-default
Device(config-pmap-c)# set dscp af42
Device(config-pmap-c)# end
```

Example: Configuring Per-Flow Admission for a Class

```
Device> enable
Device# configure terminal
Device(config)# policy-map test
Device(config-pmap)# class af4
Device(config-pmap-c)# bandwidth 200
Device(config-pmap-c)# admit cac local
Device(config-pmap-admit-cac)# rate percent 80
Device(config-pmap-admit-cac)# flow rate fixed 100
Device(config-pmap-c)# exit
```

Example: Attaching a Per-Flow Admission Policy to an Interface

```
Device> enable
Device# configure terminal
Device(config-pmap-c)# service-policy child
Device(config-pmap-c)# end
Device# configure terminal
Device(config)# interface Serial2/0
Device(config-if)# bandwidth 384
Device(config-if)# ip address 10.10.100.1 255.255.255.0
Device(config-if)# load-interval 30
Device(config-if)# service-policy output test
Device(config-if)# no shutdown
Device(config-if)# end
```

Example: Verifying Per-Flow Admission

```
Device# show policy-map interface


  Service-policy output: test

    Class-map: af4 (match-all)
      269 packets, 336250 bytes
      30 second offered rate 90000 bps, drop rate 13000 bps
      Match:  dscp af41 (34) af42 (36) af43 (38)
      Queueing
      queue limit 100 ms/ 2500 bytes


      (queue depth/total drops/no-buffer drops) 2500/39/0
      (pkts output/bytes output) 230/287500
      bandwidth 200 kbps

      cac local rate 200 kbps, reserved 200 kbps
      flow rate fixed 100 kbps

      All flows:
        Number of admitted flows: [2]
        Number of non-admitted flows: [1]

      Service-policy : child

        Class-map: admitted (match-all)
          178 packets, 222500 bytes
          30 second offered rate 60000 bps, drop rate 0000 bps
          Match:  metadata cac status admitted
          QoS Set
            dscp af41
              Packets marked 194

        Class-map: unadmitted (match-all)
          88 packets, 110000 bytes
          30 second offered rate 30000 bps, drop rate 0000 bps
          Match:  metadata cac status un-admitted
          QoS Set
            dscp af42
```

```
          Packets marked 96

      Class-map: class-default (match-any)
        3 packets, 3750 bytes
        30 second offered rate 1000 bps, drop rate 0000 bps
        Match: any

Class-map: class-default (match-any)
  181 packets, 115396 bytes
  30 second offered rate 31000 bps, drop rate 0000 bps
  Match: any

  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 181/115396
```

Additional References for Per-Flow Admission

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	Cisco IOS Quality of Service Solutions Command Reference

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Per-Flow Admission

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Per-Flow Admission