



Differentiated Services Compliant Distributed Weighted Random Early Detection

Feature History

Release	Modification
12.1(5a)E	This feature was introduced.
12.0(15)S	This feature was integrated into Cisco IOS Release 12.0(15)S.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.



Note

This document describes the Differentiated Services Compliant Distributed Weighted Random Early Detection (DiffServ Compliant dWRED) feature that was introduced in Cisco IOS Release 12.1(5a)E and is also available in Cisco IOS Release 12.0(15)S and Cisco IOS Release 12.2(14)S or later on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers and FlexWAN-enabled Catalyst 6000 family switches (in Release 12.1 E only); this is not the document for the DiffServ Compliant Weighted Random Early Detection feature that was originally released in Cisco IOS Release 12.1 T.

If you are running Cisco IOS Release 12.1(5)T or a later release and need information on the DiffServ Compliant Weighted Random Early Detection feature, refer to the [DiffServ Compliant Weighted Random Early Detection](#) document on the Cisco IOS Release 12.1(5)T documentation index.

This document describes the Differentiated Services Compliant Distributed Weighted Random Early Detection (DiffServ Compliant dWRED) feature for Release 12.1(5a)E, 12.0(15)S, and 12.2(14)S and includes the following sections:

- [Feature Overview, page 2](#)
- [Supported Platforms, page 5](#)
- [Supported Standards, MIBs, and RFCs, page 6](#)
- [Configuration Tasks, page 7](#)
- [Configuration Examples, page 9](#)
- [Command Reference, page 10](#)
- [Glossary, page 18](#)

Feature Overview

This feature enables distributed Weighted Random Early Detection (dWRED) to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet. The DSCP value is the first six bits of the IP type of service (ToS) byte.

For a description of how dWRED detects and drops packets, see the [“Functional Description of dWRED” section on page 3](#) of this document.

The **random-detect** command is used to enable DSCP-based dWRED and is introduced on Cisco IOS Release 12.1(5a)E and Release 12.0(15)S as part of this feature (for information on DiffServ Compliant WRED on Release 12.1 T or later release, refer to the note at the beginning of this document).

This feature adds two new arguments, *dscp-based* and *prec-based*, to the existing **random-detect** QoS policy-map class command.

The *dscp-based* argument enables dWRED to use the DSCP value of a packet when it calculates the drop probability for the packet. The *prec-based* argument enables dWRED to use the IP Precedence value of a packet when it calculates the drop probability for the packet.

These arguments are optional (you need not use either of them to use the commands), but they are also mutually exclusive; that is, if you use the *dscp-based* argument, you cannot use the *prec-based* argument with the same command.

The **random-detect dscp** command is then entered to configure the dWRED parameters on a particular DSCP value or code point (the code point explanation begins in the next paragraph). The dWRED parameters include the minimum and maximum threshold values, and the mark probability denominator.

This feature also allows users to enable dWRED using the Assured Forwarding (AF) code points, the Expedited Forwarding (EF) code point, and Class Selector (CS) values within the IP DSCP header. The AF code points provide a means for a domain to offer four different levels (four different AF classes) of forwarding assurances for IP packets received from other (such as customer) domains. Each one of the four AF classes is allocated a certain amount of forwarding services (buffer space and bandwidth).

Within each AF class, IP packets are marked with one of three possible drop precedence values (binary 2{010}, 4{100}, or 6{110}), which exist as the three lowest bits in the DSCP header. In congested network environments, the drop precedence value of the packet determines the importance of the packet within the AF class. Packets with higher drop precedence values are discarded before packets with lower drop precedence values.

The upper three bits of the IP DSCP value determine the AF class; the lower three values determine the drop probability.

The EF code point is usually used to mark high priority, time-sensitive data. The EF code point marking is equal to the highest IP precedence value; therefore, the EF code point is always equal to precedence value 7.

The CS values are equal to IP precedence values (for instance, cs1 is the same as IP precedence 1).

Usage Points to Note

Remember the following points when using the new commands and the new arguments:

- If you use the *dscp-based* argument, dWRED will use the DSCP value to calculate the drop probability.
- If you use the *prec-based* argument, dWRED will use the IP precedence value to calculate the drop probability.
- The *dscp-based* and *prec-based* arguments are mutually exclusive. If you do not specify either argument, dWRED will use the IP precedence value to calculate the drop probability (the default method).
- The **random-detect dscp** command that is used to configure the dWRED parameters in QoS policy-map class configuration mode must be used in conjunction with the **random-detect** (QoS policy-map class) command.
- The **random-detect dscp** command can be used only if you use the *dscp-based* argument with the **random-detect** (QoS policy-map class) command.

Functional Description of dWRED

When a packet arrives, the following events occur:

- The average queue size is calculated. See the [“Average Queue Size”](#) section for details.
- If the average queue size is less than the minimum queue threshold, the arriving packet is queued.
- If the average queue size is between the minimum queue threshold and the maximum queue threshold, the packet is either dropped or queued, depending on the packet drop probability. See the [“Packet-Drop Probability”](#) section for details.
- If the average queue size is greater than the maximum queue threshold, the packet is automatically dropped.

Average Queue Size

The average queue size is based on the previous average and the current size of the queue. The formula is:

$$\text{average_queue_size} = (\text{old_average} * (1 - 1/2^n)) + (\text{current_queue_size} * 1/2^n)$$

where n is the exponential weight factor, a user-configurable value.



Note

We recommend using the default value for the exponential weight factor. Change this value from the default value only if you have determined that your situation would benefit from using a different value.

For high values of n , the previous average queue size becomes more important. A large factor smooths out the peaks and lows in queue length. The average queue size is unlikely to change very quickly, avoiding drastic swings in size. The dWRED process is slow to start dropping packets, but it may continue dropping packets for a time after the actual queue size has fallen below the minimum threshold. The slow-moving average accommodates temporary bursts in traffic.

If the value of n becomes too high, dWRED does not react to congestion. Packets are sent or dropped as if dWRED were not in effect.

For low values of n , the average queue size closely tracks the current queue size. The resulting average may fluctuate with changes in the traffic levels. In this case, the dWRED process responds quickly to long queues. Once the queue falls below the minimum threshold, the process stops dropping packets.

If the value of n becomes too low, dWRED overreacts to temporary traffic bursts and drops traffic unnecessarily.

Packet-Drop Probability

The probability that a packet will be dropped is based on the minimum threshold, maximum threshold, and mark probability denominator.

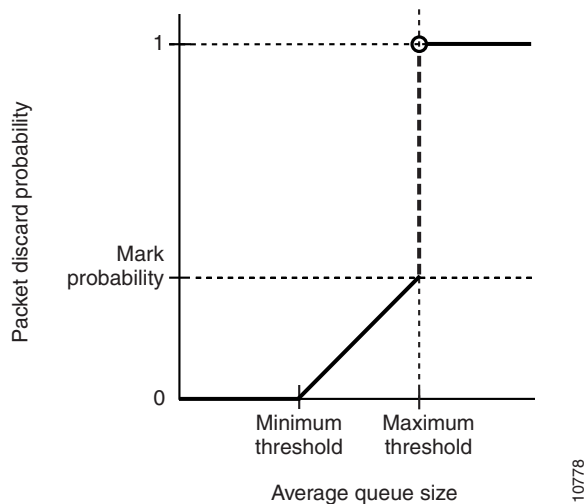
When the average queue size is above the minimum threshold, RED starts dropping packets. The rate of packet drop increases linearly as the average queue size increases, until the average queue size reaches the maximum threshold.

The mark probability denominator is the fraction of packets dropped when the average queue size is at the maximum threshold. For example, if the denominator is 512, one out of every 512 packets is dropped when the average queue size is at the maximum threshold.

When the average queue size is above the maximum threshold, all packets are dropped.

Figure 1 summarizes the packet drop probability.

Figure 1 dWRED Packet Drop Probability



The minimum threshold value should be set high enough to maximize the link utilization. If the minimum threshold is too low, packets may be dropped unnecessarily, and the transmission link will not be fully used.

The difference between the maximum threshold and the minimum threshold should be large enough to avoid global synchronization of TCP hosts (global synchronization of TCP hosts can occur as multiple TCP hosts reduce their transmission rates). If the difference between the maximum and minimum thresholds is too small, many packets may be dropped at once, resulting in global synchronization.

Benefits

This feature extends the functionality of dWRED to enable support for Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB). This feature enables dWRED to be compliant with the DiffServ standard and the AF PHB Internet Engineering Task Force (IETF) standard.

This feature enables customers to implement AF PHB by marking packets according to DSCP values and then assigning preferential drop probabilities to those packets.

Restrictions

IP Packets

This feature can be used with IP packets only. It is not intended for use with Multiprotocol Label Switching (MPLS)-encapsulated or other packets.

User-Defined Traffic Class Limitations

Either the **bandwidth** or the **shape** command must be used in conjunction with dWRED when dWRED is configured in a traffic policy (also known as a policy map) using a user-defined, nondefault traffic class (which is also known as a class map). Therefore, either the **bandwidth** or the **shape** command must be entered in the same traffic policy as the **random-detect** command if the traffic policy is not using the default traffic class.

If the traffic policy is using the default traffic class, the **bandwidth** and **shape** commands need not be specified in the traffic policy configuration.

Output Policy Limitation

A traffic policy configured using dWRED can be attached only at the output direction of an interface (the **service-policy output** command can be used to attach a traffic policy containing dWRED; the **service-policy input** command cannot be used).

Supported Platforms

This feature is supported on the following platforms:

- Cisco 7500 series routers with a VIP2-40 or later VIP release
- Catalyst 6000 family switches with a FlexWAN module



Note

The Catalyst 6000 family of switches do not run Cisco IOS Release 12.0 S or 12.2(14)S.

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

The Differentiated Services and the Assured Forwarding Per-Hop Behavior standards are supported by this feature.

MIBs

The Class-Based Quality of Service MIB supports this feature. This MIB is actually the following two MIBs:

- CISCO-CLASS-BASED-QOS-MIB
- CISCO-CLASS-BASED-QOS-CAPABILITY-MIB

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

- RFC 2474, *Definition of the Differentiated Services Field in IPv4 and IPv6 Headers*
- RFC 2475, *An Architecture for Differentiated Services Framework*

- RFC 2597, *Assured Forwarding PHB*
- RFC 2598, *An Expedited Forwarding PHB*

Configuration Tasks

See the following sections for configuration tasks for the DiffServ Compliant Distributed Weighted Random Early Detection feature. Each task in the list is identified as optional or required.

- [Configuring dWRED to Use the DSCP Value](#) (required)
- [Verifying the DSCP Value Configuration](#) (optional)

Configuring dWRED to Use the DSCP Value

To configure dWRED to use the DSCP value when it calculates the drop probability, use the following commands beginning in interface configuration mode. These are the commands to use at the class level, within policy maps.



Note


dWRED using DSCP values is enabled using the Modular QoS Command Line Interface (CLI.) For additional information on the Modular QoS CLI, including information on match criteria and QoS feature options, see the [Modular QoS CLI](#) document on Cisco.com.

	Command	Purpose
Step 1	Router(config-if)# class-map [match-all match-any] <i>class-map-name</i>	Creates a traffic class to be used for matching packets to a specified class.
Step 2	Router(config-cmap)# match <i>match-criterion</i>	Configures the match criteria for a traffic class. For additional information on the modular QoS CLI, including information on match criteria in class maps, see the <i>Modular QoS CLI</i> document on Cisco.com. More than one match criterion can be configured in a traffic class. If you want to specify more than one match criterion for a traffic class, simply enter the match command in another command line while in QoS class-map configuration mode.
Step 3	Router(config-cmap)# exit	Exits QoS class-map configuration mode.
Step 4	Router(config-if)# policy-map <i>policy-map</i>	Creates or modifies a traffic policy that can be attached to one or more interfaces to specify a service policy.
Step 5	Router(config-pmap)# class <i>class-map-name</i>	Specifies a traffic class used to classify traffic for the traffic policy. In these instructions, the traffic class was named in Step 1.
	Note If you specify a nondefault traffic class in this step, either the bandwidth or the shape command must be specified in Step 6 or Step 7. If you specified the default traffic class in Step 5, Step 6 and Step 7 can be omitted.	

	Command	Purpose
Step 6	Router(config-pmap-c)# bandwidth { <i>bandwidth-kbps</i> percent <i>percent</i> }	(Optional) Specifies a minimum bandwidth guarantee to a traffic class during periods of network congestion. A minimum bandwidth guarantee can be specified in kilobits per second or by a percentage of the overall available bandwidth.
Step 7	Router(config-pmap-c)# shape { average peak } <i>mean-rate</i> [<i>burst-size</i> [<i>excess-burst-size</i>]]	(Optional) Shapes traffic leaving an interface to an indicated bit rate in order to avoid network congestion.
Step 8	Router(config-pmap-c)# random-detect dscp-based	Indicates that dWRED is to use the DSCP value when it calculates the drop probability for the packet.
Step 9	Router(config-pmap-c)# random-detect dscp <i>dscp-value</i> <i>min-threshold</i> <i>max-threshold</i> [<i>mark-probability-denominator</i>]	Specifies the minimum and maximum packet thresholds and, optionally, the mark probability denominator for the DSCP value.
Step 10	Router(config-pmap-c)# exit	Exits QoS policy-map class configuration mode.
Step 11	Router(config-if)# service-policy output <i>policy-map</i>	Attaches a traffic policy to an interface at the output direction. Therefore, all traffic leaving that interface will be processed according to the configuration of the traffic policy.

Verifying the DSCP Value Configuration

To verify the DSCP value configuration, use either of the following commands in global configuration mode:

Command	Purpose
Router# show policy-map <i>policy-map-name</i>	Displays the contents of a particular policy map, including information relating to user-configured and active DSCP values.
Router# show policy-map interface	Displays the configuration of classes configured for service policies on the specified interface or permanent virtual circuit (PVC).
	 <p>Note The show policy-map interface command output will display only configuration and statistics for user-defined and active dWRED values.</p>

Configuration Examples

This section provides the following configuration examples:

- [dWRED Configured to Use the DSCP Value Example](#)
- [DSCP Value Configuration Verification Example](#)

dWRED Configured to Use the DSCP Value Example

The following example enables dWRED to use the DSCP value 8 for class c1. The minimum threshold for DSCP value 8 is 24 and the maximum threshold is 40. The last line attaches the traffic policy so the traffic policy applies to all traffic leaving interface pos10/0/0.

```
Router(config-if)# class-map c1
Router(config-cmap)# match access-group 101

Router(config-if)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp 8 24 40

Router# interface pos10/0/0
Router(config-if)# service-policy output p1
```

DSCP Value Configuration Verification Example

In the following example, all traffic marked with the IP DSCP values of 17 and 53 in the default traffic class of the policy map named random-dscp is dWRED-enabled:

```
Router# show policy-map random-dscp

Policy Map random-dscp
Class class-default
  random-detect dscp-based
  random-detect dscp 17 100 200 10
  random-detect dscp 53 200 400 10
```

Assuming policy map random-dscp is attached to interface pos10/0/0, the following output would appear after entering the **show policy-map interface** command. The **show policy-map interface** command displays only output for DSCP values that were user-configured or for active DSCP values. Note that both user-configured DSCP values (17 and 53) appear in the command output, and that DSCP value 0 appears because it is active.

```
Router# show policy-map interface pos10/0/0

POS10/0/0

Service-policy output:random-dscp (1080)

Class-map:class-default (match-any) (1081/0)
  0 packets, 0 bytes
  30 second offered rate 0 bps, drop rate 0 bps
Match:any (1083)
  0 packets, 0 bytes
```

```

30 second rate 0 bps
queue size 0, queue limit 23264
packets output 5, packet drops 0
tail/random drops 0, no buffer drops 0, other drops 0
Random-detect:
  Exp-weight-constant:9 (1/512)
  Mean queue depth:0
  Class Random      Tail      Minimum  Maximum  Mark      Output
                   drop      drop threshold threshold probability packets
  0                 0        0        5816    11632    1/10      5
  17                0        0        100     200     1/10      0
  53                0        0        200     400     1/10      0

```

Command Reference

This section documents the following new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.



Note

The command pages in this section document the entire history of each command, including the introduction of the command on platforms not supported by the DiffServ Compliant dWRED feature. Therefore, the command references might contain information that does not pertain to DiffServ Compliant dWRED but does pertain to the command.

If information in the command reference does not pertain to the DiffServ Compliant dWRED feature, the difference is noted in the command reference for that particular command.

- [random-detect dscp](#)
- [random-detect \(interface and policy map class\)](#)

random-detect dscp

To change the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value, use the **random-detect dscp** command in interface or QoS policy-map class configuration mode. To return the minimum and maximum packet thresholds to the default for the DSCP value, use the **no** form of this command.

```
random-detect dscp dscp-value min-threshold max-threshold [mark-probability-denominator]
```

```
no random-detect dscp dscp-value min-threshold max-threshold [mark-probability-denominator]
```

Syntax Description		
<i>dscp-value</i>		The IP DSCP value. The IP DSCP value can also be specified as one of the following AF code points, CS values or EF code points: af11 , af12 , af13 , af21 , af22 , af23 , af31 , af32 , af33 , af41 , af42 , af43 , cs0 , cs1 , cs2 , cs3 , cs4 , cs5 , cs6 , cs7 or ef .
<i>min-threshold</i>		Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) or distributed WRED randomly drops some packets with the specified DSCP value.
<i>max-threshold</i>		Maximum threshold in number of packets. The value range of this argument is the value of the <i>min-threshold</i> argument to 4096. When the average queue length exceeds the maximum threshold, WRED or dWRED drops all packets with the specified DSCP value.
<i>mark-probability-denominator</i>		(Optional) Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, one out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; one out of every ten packets is dropped at the maximum threshold.

Defaults

The default values for this command are different on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers and Catalyst 6000 family switches with a FlexWAN module (dWRED). All other platforms running WRED have another set of default values.

Both sets of default values are described in the “Usage Guidelines” section.

Command Modes

Interface configuration

Policy map class configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.1(5a)E	This command was integrated into Cisco IOS Release 12.1(5a)E in policy map class configuration mode only. The command was introduced for VIP-enabled Cisco 7500 series routers and Catalyst 6000 family switches with a FlexWAN module.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S in policy map class configuration mode only.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines**VIP-Enabled Cisco 7500 Series Routers and Catalyst 6000 Family Switches with a FlexWAN Module Defaults**

For all IP precedence values, the default *mark-probability-denominator* is 10, and the *max-threshold* value is based on the output buffering capacity and the transmission speed of the interface.

The default *min-threshold* value depends on the IP precedence value. The *min-threshold* value for IP precedence 0 corresponds to half of the *max-threshold* value. The values for the remaining IP precedence values fall between half the *max-threshold* and the *max-threshold* at even interval.

Unless the maximum and minimum threshold values for the IP DSCP values are configured by the user, all DSCP values have the same minimum threshold and maximum threshold values as the value specified for precedence 0.

[Table 1](#) lists the default minimum threshold value for each IP precedence value.

Table 1 Default WRED Minimum Threshold Values for the Distributed platforms

IP Precedence	Class Selector (CS) Value	Minimum Threshold Value (Fraction of Maximum Threshold Value)	Important Notes About the Value
0	cs0	8/16	All DSCP values that are not configured by the user will have the same threshold values as IP precedence 0.
1	cs1	9/16	—
2	cs2	10/16	—
3	cs3	11/16	—
4	cs4	12/16	—
5	cs5	13/16	—
6	cs6	14/16	—
7	cs7	15/16	The EF code point will always be equal to IP Precedence 7.

Non-VIP-Enabled Cisco 7500 Series Routers and Catalyst 6000 Family Switches with a FlexWAN Module Defaults

All platforms except the VIP-enabled Cisco 7500 series router and the Catalyst 6000 have the following default values.

If WRED is using the DSCP value to calculate the drop probability of a packet, all 64 entries of the DSCP table are initialized with the default settings shown in [Table 2](#).

Table 2 *random-detect dscp Default Settings*

DSCP (Precedence)	Minimum Threshold	Maximum Threshold	Mark Probability
0(0)	20	40	1/10
1	22	40	1/10
2	24	40	1/10
3	26	40	1/10
4	28	40	1/10
5	30	40	1/10
6	32	40	1/10
7	34	40	1/10
8(1)	22	40	1/10
9	22	40	1/10
10	24	40	1/10
11	26	40	1/10
12	28	40	1/10
13	30	40	1/10
14	32	40	1/10
15	34	40	1/10
16(2)	24	40	1/10
17	22	40	1/10
18	24	40	1/10
19	26	40	1/10
20	28	40	1/10
21	30	40	1/10
22	32	40	1/10
23	34	40	1/10
24(3)	26	40	1/10
25	22	40	1/10
26	24	40	1/10
27	26	40	1/10
28	28	40	1/10
29	30	40	1/10
30	32	40	1/10
31	34	40	1/10
32(4)	28	40	1/10
33	22	40	1/10
34	24	40	1/10

Table 2 *random-detect dscp Default Settings (continued)*

DSCP (Precedence)	Minimum Threshold	Maximum Threshold	Mark Probability
35	26	40	1/10
36	28	40	1/10
37	30	40	1/10
38	32	40	1/10
39	34	40	1/10
40(5)	30	40	1/10
41	22	40	1/10
42	24	40	1/10
43	26	40	1/10
44	28	40	1/10
45	30	40	1/10
46	36	40	1/10
47	34	40	1/10
48(6)	32	40	1/10
49	22	40	1/10
50	24	40	1/10
51	26	40	1/10
52	28	40	1/10
53	30	40	1/10
54	32	40	1/10
55	34	40	1/10
56(7)	34	40	1/10
57	22	40	1/10
58	24	40	1/10
59	26	40	1/10
60	28	40	1/10
61	30	40	1/10
62	32	40	1/10
63	34	40	1/10
rsvp	36	40	1/10

This command is not available at the interface level for Cisco IOS Release 12.1 E or Release 12.0 S. This command is only available in policy-map class configuration mode in Cisco IOS Release 12.1 E.

The **random-detect dscp** command allows you to specify the DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **ef**.

The Assured Forwarding (AF) code points provide a means for a domain to offer four different levels (four different AF classes) of forwarding assurances for IP packets received from other (such as customer) domains. Each one of the four AF classes is allocated a certain amount of forwarding services (buffer space and bandwidth).

Within each AF class, IP packets are marked with one of three possible drop precedence values (binary 2{010}, 4{100}, or 6{110}), which exist as the three lowest bits in the DSCP header. In congested network environments, the drop precedence value of the packet determines the importance of the packet within the AF class. Packets with higher drop precedence values are discarded before packets with lower drop precedence values.

The upper three bits of the IP DSCP value determine the AF class; the lower three values determine the drop probability.

The Expedited Forwarding (EF) code point is usually used to mark high-priority, time-sensitive data. The EF code point marking is equal to the highest precedence value; therefore, the EF code point is always equal to precedence value 7.

The Class Selector (CS) values are equal to IP precedence values (for instance, cs1 is the same as IP precedence 1).

On a particular traffic class, eight DSCP values can be configured per traffic class. Overall, 29 values can be configured on a traffic class: 8 precedence values, 12 AF code points, 1 EF code point, and 8 user-defined DSCP values.

This command must be used in conjunction with the **random-detect** (interface and policy map class) command.

Additionally, the **random-detect dscp** command is available only if you specified the *dscp-based* argument when using the **random-detect** (interface and policy map class) command.

Examples

The following example enables WRED to use the DSCP value 8. The minimum threshold for the DSCP value 8 is 20, the maximum threshold is 40, and the mark probability is 1/10.

```
random-detect dscp 8 20 40 10
```

Related Commands

Command	Description
random-detect (interface)	Enables WRED or dWRED.
show queueing	Lists all or selected configured queueing strategies.
show queueing interface	Displays the queueing statistics of an interface or VC.

random-detect (interface and policy map class)

To enable Weighted Random Early Detection (WRED) or distributed WRED (dWRED), use the **random-detect** command in interface configuration mode. To configure WRED in a traffic policy, use the **random-detect** command in QoS policy-map class configuration mode. To disable WRED or dWRED, use the **no** form of this command.

random-detect [**dscp-based** | **prec-based**]

no random-detect [**dscp-based** | **prec-based**]

Syntax Description

dscp-based	(Optional) Specifies that WRED is to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet.
prec-based	(Optional) Specifies that WRED is to use the IP precedence value when it calculates the drop probability for a packet.

Defaults

WRED and dWRED are disabled by default.

If you choose not to use either the *dscp-based* or the *prec-based* argument, WRED uses the IP Precedence value (the default method) to calculate drop probability for the packet.

Command Modes

Interface configuration (when used on an interface)

QoS policy-map class (configuration when used to specify class policy in a policy map)

Command History

Release	Modification
11.1 CC	This command was introduced.
12.1(5)T	Arguments were added to support Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB).
12.1(5a)E	This command was integrated into Release 12.1(5a)E in policy map class configuration mode only. This command was implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers and Catalyst 6000 family switches with a FlexWAN module.
12.0(15)S	This command was integrated into Release 12.0(15)S in QoS policy-map class configuration mode only.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

This command is not available at the interface level for Cisco IOS Release 12.1 E or Release 12.0 S. This command is available only in QoS policy-map class configuration mode in Cisco IOS Release 12.1 E.

This command includes two optional arguments, *dscp-based* and *prec-based*, that determine the method WRED uses to calculate the drop probability of a packet.

Note the following points when deciding which method to instruct WRED to use:

- With the *dscp-based* argument, WRED uses the DSCP value (that is, the first six bits of the IP type of service [ToS] byte) to calculate the drop probability.
- With the *prec-based* argument, WRED uses the IP precedence value to calculate the drop probability.
- The *dscp-based* and *prec-based* arguments are mutually exclusive.
- If neither argument is specified, WRED uses the IP precedence value to calculate the drop probability (the default method).

Examples

The following example enables WRED to use the DSCP value 8. The minimum threshold for DSCP value 8 is 24 and the maximum threshold is 40. This configuration was performed at the interface level and is therefore unavailable in Cisco IOS Release 12.1 E.

```
Router(config-if)# interface seo/0
Router(config-if)# random-detect dscp-based
Router(config-if)# random-detect dscp 8 24 40
```

The following example enables WRED to use the DSCP value 8 for class c1. The minimum threshold for DSCP value 8 is 24 and the maximum threshold is 40. The last line attaches the service policy to the output interface or virtual circuit (VC) p1.

```
Router(config-if)# class-map c1
Router(config-cmap)# match access-group 101
Router(config-if)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp 8 24 40
Router(config-if)# service-policy output p1
```

Related Commands

Command	Description
random-detect dscp	Configures the minimum and maximum packet thresholds, and optionally, the mark probability denominator for the DSCP value.
random-detect exponential-weighting-constant	Configures the WRED and dWRED exponential weight factor for the average queue size calculation.
random-detect flow	Enables flow-based WRED.
random-detect precedence	Configures WRED and dWRED parameters for a particular IP precedence.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show queueing	Lists all or selected configured queueing strategies.
show tech-support rsvp	Generates a report of all RSVP-related information.

Glossary

AF code points—Assured Forwarding code points. The AF code points provide a means for a domain to offer four different levels (four different AF classes) of forwarding assurances for IP packets received from other (such as customer) domains. Each one of the four AF classes is allocated a certain amount of forwarding services (buffer space and bandwidth).

Within each AF class, IP packets are marked with one of three possible drop precedence values (binary 2{010}, 4{100}, or 6{110}), which exist as the three lowest bits in the DSCP header. In congested network environments, the drop precedence value of the packet determines the importance of the packet within the AF class. Packets with higher drop precedence values are discarded before packets with lower drop precedence values.

The upper three bits of the IP DSCP value determine the AF class; the lower three values determine the drop probability.

Assured Forwarding code points—see AF code points.

average queue size—The average queue depth is used in WRED congestion management and is determined by using the following formula:

$$\text{average} = (\text{old_average} * (1 - 1/2^n)) + (\text{current_queue_size} * 1/2^n)$$

where n is the user-defined exponential weighted constant number (although we suggest using the default value in most scenarios; the default value is 9). The average queue depth is used to determine if congestion is present on the interface. If the incoming traffic rate is larger than the queue depth, WRED begins systematically dropping packets to smooth the link.

current queue size—The current queue depth is the current size of the queue. The current queue depth is used as part of the average queue depth calculation when using WRED for congestion avoidance purposes.

EF code point—Expedited Forwarding code point. The EF code point is usually used to mark high-priority, time-sensitive data. The EF code point marking is equal to the highest precedence value; therefore, the EF code point is always equal to precedence value 7.

Expedited Forwarding code point—see EF code point.

exponential weighting constant number—The exponential weighting constant number is used to calculate the average queue depth in WRED congestion management. The average queue depth is used in WRED congestion management and is determined by using the following formula:

$$\text{average} = (\text{old_average} * (1 - 1/2^n)) + (\text{current_queue_size} * 1/2^n)$$

where n is the exponential weighting constant number (although we suggest using the default value in most scenarios; the default value is 9).

mark probability denominator—The mark probability denominator is the fraction of packets dropped when the average queue size is at the maximum threshold. For example, if the denominator is 512, one out of every 512 packets is dropped when the average queue is at the maximum threshold.

maximum threshold parameter—The maximum threshold parameter is specified as part of the WRED and dWRED congestion management features. When the average queue depth exceeds the minimum threshold, WRED or dWRED senses congestion and begins dropping packets. The rate of packet drops until the maximum threshold parameter is met.

minimum threshold parameter—The minimum threshold parameter is specified as part of the WRED and dWRED congestion management features. When the average queue depth exceeds the minimum threshold, WRED or dWRED senses congestion and begins dropping packets. The rate of packet drops until the maximum threshold parameter is met.