

Implementing Quality of Service Policies with DSCP

Document ID: 10103

Introduction

Prerequisites

Requirements

Components Used

Background Theory

Conventions

Differentiated Services Code Point

Assured Forwarding

Expedited Forwarding

Using the DSCP Field

Packet Classification

Marking

Using Committed Access Rate or Class-Based Policing

DSCP-Compliant WRED

Known Issues in Cisco IOS Software 12.2 Release Trains

Related Information

Introduction

This document describes how to set the Differentiated Services Code Point (DSCP) values in Quality of Service (QoS) configurations on a Cisco router, and it summarizes the relationship between DSCP and IP precedence.

Prerequisites

Requirements

You should be familiar with the fields in the IP header and Cisco IOS® CLI

Components Used

This document is not restricted to specific software and hardware versions.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Background Theory

Differentiated Services (DiffServ) is a new model in which traffic is treated by intermediate systems with relative priorities based on the type of services (ToS) field. Defined in RFC 2474 and RFC 2475, the DiffServ standard supersedes the original specification for defining packet priority described in RFC 791. DiffServ increases the number of definable priority levels by reallocating bits of an IP packet for priority marking.

The DiffServ architecture defines the DiffServ (DS) field, which supersedes the ToS field in IPv4 to make per-hop behavior (PHB) decisions about packet classification and traffic conditioning functions, such as metering, marking, shaping, and policing.

The RFCs do not dictate the way to implement PHBs; this is the responsibility of the vendor. Cisco implements queuing techniques that can base their PHB on the IP precedence or DSCP value in the IP header of a packet. Based on DSCP or IP precedence, traffic can be put into a particular service class. Packets within a service class are treated the same way.

Conventions

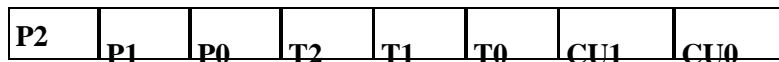
For more information on document conventions, refer to Cisco Technical Tips Conventions.

Differentiated Services Code Point

The six most significant bits of the DiffServ field is called as the DSCP. The last two Currently Unused (CU) bits in the DiffServ field were not defined within the DiffServ field architecture; these are now used as Explicit Congestion Notification (ECN) bits. Routers at the edge of the network classify packets and mark them with either the IP Precedence or DSCP value in a Diffserv network. Other network devices in the core that support Diffserv use the DSCP value in the IP header to select a PHB behavior for the packet and provide the appropriate QoS treatment.

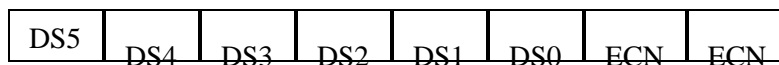
The diagrams in this section show a comparison between the ToS byte defined by RFC 791 and the DiffServ field.

ToS Byte



- IP precedence three bits (P2 to P0)
- Delay, Throughput and Reliability three bits (T2 to T0)
- CU (Currently Unused) two bits(CU1–CU0)

DiffServ Field



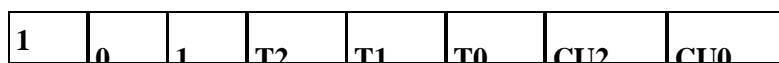
- DSCP six bits (DS5–DS0)
- ECN two bits

The standardized DiffServ field of the packet is marked with a value so that the packet receives a particular forwarding treatment or PHB, at each network node.

The default DSCP is 000 000. Class selector DSCPs are values that are backward compatible with IP precedence. When converting between IP precedence and DSCP, match the three most significant bits. In other words:

IP Prec 5 (101) maps to IP DSCP 101 000

ToS Byte



DiffServ Field

1	0	1	0	0	0	ECN	ECN
---	---	---	---	---	---	-----	-----

The DiffServ standard utilizes the same precedence bits (the most significant bits DS5, DS4 and DS3) for priority setting, but further clarifies the definitions, offering finer granularity through the use of the next three bits in the DSCP. DiffServ reorganizes and renames the precedence levels (still defined by the three most significant bits of the DSCP) into these categories (the levels are explained in greater detail in this document):

Precedence Level	Description
7	Stays the same (link layer and routing protocol keep alive)
6	Stays the same (used for IP routing protocols)
5	Express Forwarding (EF)
4	Class 4
3	Class 3
2	Class 2
1	Class 1
0	Best effort

With this system, a device prioritizes traffic by class first. Then it differentiates and prioritizes same-class traffic, taking the drop probability into account.

The DiffServ standard does not specify a precise definition of "low," "medium," and "high" drop probability. Not all devices recognize the DiffServ (DS2 and DS1) settings; and even when these settings are recognized, they do not necessarily trigger the same PHB forwarding action at each network node. Each node implements its own response based on how it is configured.

Assured Forwarding

RFC 2597 defines the assured forwarding (AF) PHB and describes it as a means for a provider DS domain to offer different levels of forwarding assurances for IP packets received from a customer DS domain. The Assured Forwarding PHB guarantees a certain amount of bandwidth to an AF class and allows access to extra bandwidth, if available. There are four AF classes, AF1x through AF4x. Within each class, there are three drop probabilities. Depending on a given network's policy, packets can be selected for a PHB based on required throughput, delay, jitter, loss or according to priority of access to network services.

Classes 1 to 4 are referred to as AF classes. The following table illustrates the DSCP coding for specifying the AF class with the probability. Bits DS5, DS4 and DS3 define the class; bits DS2 and DS1 specify the drop probability; bit DS0 is always zero.

Drop	Class 1	Class 2	Class 3	Class 4
Low	001010			
	AF11	010010	011010	100010
	DSCP 10	AF21	AF31	AF41
		DSCP 18	DSCP 26	DSCP 34

Medium	001100			
	AF12	010100	011100	100100
	DSCP 12	AF 22	AF32	AF42
High	001110	DSCP 20	DSCP 28	DSCP 36
	AF13	010110	011110	100110
	DSCP 14	AF23	AF33	AF43

DSCP 22 DSCP 30 DSCP 38

Expedited Forwarding

RFC 2598 defines the Expedited Forwarding (EF) PHB: "The EF PHB can be used to build a low loss, low latency, low jitter, assured bandwidth, end-to-end service through DS (Diffserv) domains. Such a service appears to the endpoints like a point-to-point connection or a "virtual leased line." This service has also been described as Premium service." Codepoint 101110 is recommended for the EF PHB, which corresponds to a DSCP value of 46.

Again, vendor-specific mechanisms need to be configured to implement these PHBs. Refer to RFC 2598 for more information about EF PHB.

Using the DSCP Field

There are three ways you can use the DSCP field:

- Classifier Select a packet based on the contents of some portions of the packet header and apply PHB based on service characteristic defined by the DSCP value.
- Marker Set the DSCP field based on the traffic profile.
- Metering Check compliance to traffic profile using either a shaper or dropper function.

Cisco IOS software considers the precedence bits of the ToS field if there is traffic that is queued in Weighted Fair Queuing (WFQ), Weighted Random Early Detection (WRED), or Weighted Round Robin (WRR). The precedence bits are not considered when Policy Routing, Priority Queuing (PQ), Custom Queuing (CQ), or Class Based Weighted Fair Queuing (CBWFQ) are configured.

Packet Classification

Packet classification involves using a traffic descriptor to categorize a packet within a specific group and making the packet accessible for QoS handling in the network. Using packet classification, you can partition network traffic into multiple priority levels or a class of service (CoS).

You can use either access lists (ACLs) or the **match** command in the modular QoS CLI to match on DSCP values. For more information on how to use ACLs, refer to Quality of Service for the Cisco 7200/7500. Selecting a DSCP value in the match command was introduced in Cisco IOS Software Release 12.1(5)T.

```
Router1(config)# access-list 101 permit ip any any ?
dscp          Match packets with given dscp value
fragments     Check non-initial fragments
log           Log matches against this entry
log-input     Log matches against this entry, including input interface
precedence    Match packets with given precedence value
time-range    Specify a time-range
```

```
tos          Match packets with given TOS value
```

When you specify the *ip dscp* value in the **class map** command, you have these:

```
Router(config)# class-map match-all VOIP
1751-uut1(config-cmap)# match ip dscp ?
<0-63>      Differentiated services codepoint value
af11       Match packets with AF11 dscp (001010)
af12       Match packets with AF12 dscp (001100)
af13       Match packets with AF13 dscp (001110)
af21       Match packets with AF21 dscp (010010)
af22       Match packets with AF22 dscp (010100)
af23       Match packets with AF23 dscp (010110)
af31       Match packets with AF31 dscp (011010)
af32       Match packets with AF32 dscp (011100)
af33       Match packets with AF33 dscp (011110)
af41       Match packets with AF41 dscp (100010)
af42       Match packets with AF42 dscp (100100)
af43       Match packets with AF43 dscp (100110)
cs1        Match packets with CS1(precedence 1) dscp (001000)
cs2        Match packets with CS2(precedence 2) dscp (010000)
cs3        Match packets with CS3(precedence 3) dscp (011000)
cs4        Match packets with CS4(precedence 4) dscp (100000)
cs5        Match packets with CS5(precedence 5) dscp (101000)
cs6        Match packets with CS6(precedence 6) dscp (110000)
cs7        Match packets with CS7(precedence 7) dscp (111000)
default    Match packets with default dscp (000000)
ef         Match packets with EF dscp (101110)
Router1(config-cmap)# match ip dscp af31
```

Marking

The DSCP can be set to a desired value at the edge of the network in order to make it easy for core devices to classify the packet as shown in the Packet Classification section and provide a suitable level of service.

Class-Based Packet Marking can be used to set the DSCP value as shown here:

```
policy-map pack-multimedia-5M

!--- Creates a policy map named pack-multimedia-5M.

class management

!--- Specifies the policy to be created for the
!--- traffic classified by class management.

bandwidth 50
set ip dscp 8

!--- Sets the DSCP value of the packets matching
!--- class management to 8.

class C1
priority 1248
set ip dscp 40
class voice-signalling
bandwidth 120
set ip dscp 24
```

Using Committed Access Rate or Class-Based Policing

Committed Access Rate and Class-Based Policing are traffic regulation mechanisms, used to regulate traffic flow to conform with the agreed upon service parameters. These mechanisms along with DSCP can be used to provide different levels of service to conforming and non-conforming traffic by appropriately modifying the DSCP value, as shown in this section.

Refer to Configuring Traffic Policing and Comparing Class-Based Policing and Committed Access Rate for more information.

```
interface Serial1/0.1 point-to-point

bandwidth 5000
ip address 192.168.126.134 255.255.255.252
rate-limit output access-group 150 8000 1500 2000 conform-action
    set-dscp-transmit 10 exceed-action set-dscp-transmit 20

!--- For traffic matching access list 150, sets the DSCP value of conforming traffic
!-- to 10 and that of non-conforming traffic to 20.

rate-limit output access-group 152 8000 1500 2000 conform-action
    set-dscp-transmit 15 exceed-action set-dscp-transmit 25
rate-limit output access-group 154 8000 1500 2000 conform-action
    set-dscp-transmit 18 exceed-action set-dscp-transmit 28
frame-relay interface-dlci 17
class shaper-multimedia-5M
```

DSCP-Compliant WRED

Weighted Random Early Detection (WRED), selectively discards lower-priority traffic when the interface begins to get congested. WRED can provide differentiated performance characteristics for different CoS. This differentiated service can be on basis of the DSCP, as shown here:

```
class C2
    bandwidth 1750
    random-detect dscp-based

!--- Enable dscp-based WRED as drop policy.

    random-detect exponential-weighting-constant 7

!--- Specifies the exponential weight factor for the
!-- average queue size calculation for the queue.

    random-detect dscp 16 48 145 10

!--- Specifies the minimum and maximum queue thresholds
!-- for each DSCP value.

    random-detect dscp 32 145 435 10
```

Refer to the DiffServ Compliant WRED section of Congestion Avoidance Overview for more information.

Known Issues in Cisco IOS Software 12.2 Release Trains

For more information on the following bugs, You can use the Bug Toolkit (registered customers only) for more information on these bugs:

- CSCdt63295 (registered customers only) If you fail to set the ToS byte with the new DSCP marking commands on the dial peers (set to 0) in Cisco IOS Software Release 12.2.2T, then packets will not be marked and they will remain with a ToS set to 0.
 - CSCdt74738 (registered customers only) Support for the **set ip dscp** command on the Cisco 7200 router and lower-end platforms for the for multicast packets should be available as of Cisco IOS Software Release 12.2(3.6) and later.
-

Related Information

- **Using Content Networking to Provide Quality of Service**
 - **Cisco IOS Software: Quality-of-Service: The Differentiated Services Model (DiffServ)**
 - **Control Plane DSCP Support for RSVP**
 - **Diff-Serv-aware Traffic Engineering (DS-TE)**
 - **Differentiated Services Compliant Distributed Weighted Random Early Detection**
 - **RFC 3168: The Addition of Explicit Congestion Notification (ECN) to IP**
 - **Quality of Service (QoS) Support Pages**
 - **Technical Support – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 15, 2008

Document ID: 10103
