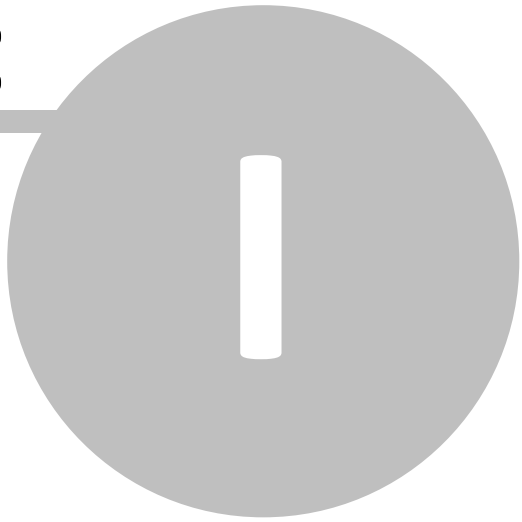
Exinda How to Guide:
ToS and DiffServ

Exinda Firmware Version 6.1

Table of Contents

Part



1 Introduction

ToS and DiffServ

Exinda Firmware Version: 6.1

1.1 Using this Guide

Throughout the manual the following text styles are used to highlight important points:

- Useful features, hints and important issues are called "notes" and they are identified in a light blue background.

Note: This is a note.

- Practical examples are presented throughout the manual for deeper understanding of specific concepts. These are called "examples" and are identified with a light green background.

This is an example.

- Warnings that can cause damage to the device are included when necessary. These are indicated by the word "caution" and are highlighted in yellow.

Caution: This is a caution.

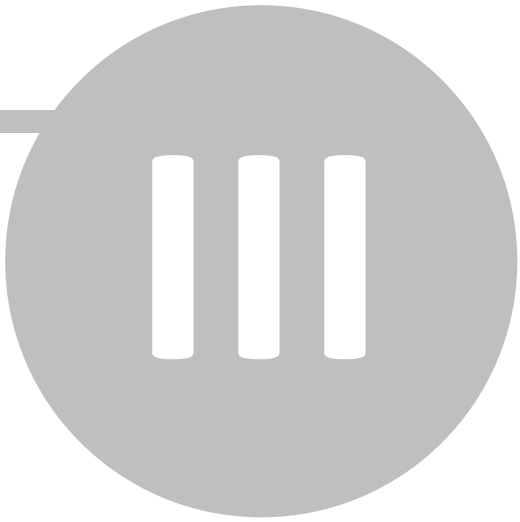
Part

2 Overview

Exinda appliances can read and write ToS/DSCP marks in packets, allowing users fine-grained control and classification of applications that are marked with Tos/DSCP values as well as applying marking policies to ensure traffic is treated appropriately by onward network equipment.

Used in conjunction with Exinda's superior classification techniques, including advanced layer 7 detection, users have complete control over how traffic is marked, and subsequently treated in the WAN cloud.

Part



3 The ToS / DiffServ Field

The ToS (type of service) or DiffServ (differentiated services) field in the IPv4 header, and the Traffic Class field in the IPv6 header are used to classify IP packets so that routers can make QoS (quality of service) decisions about what path packets should traverse across the network. For example, users may want ensure that VoIP utilizes high quality, low latency (and expensive) links, or, they might want to ensure email or recreational traffic uses cheaper (but less reliable) links.

Previously, there were 5 different categories that users could classify their traffic with using the IP ToS field (see RFC 791).

- Normal Service
- Minimize Cost
- Maximize Reliability
- Maximize Throughput
- Minimize Delay

These have since been replaced by a new set of values called DSCP (DiffServ Code Points, see RFC 2474). A DSCP is a 6-bit number; therefore, there are 64 possible DSCP combinations, of which, only a portion have been standardized and are listed below.

IPv6 contains an 8 bit Traffic Class field. The 6 most significant bits are treated the same as IPv4 DSCP. The least 2 significant bits are not modified by the appliance.

DSCP Class Name	Binary Value	Decimal Value
BE (best effort, default)	000000	0
AF11 (assured forwarding, see RFC 2597)	001010	10
AF12	001100	12
AF13	001110	14
AF21	010010	18
AF22	010100	20
AF23	010110	22
AF31	011010	26
AF32	011100	28
AF33	011110	30
AF41	100010	34
AF42	100100	36

DSCP Class Name	Binary Value	Decimal Value
AF43	100110	38
CS1 (class selector)	001000	8
CS2	010000	16
CS3	011000	24
CS4	100000	32
CS5	101000	40
CS6	110000	48
CS7	111000	56
EF (expedited forwarding, see RFC 2598)	101110	46

Table 1: DCSP Class, binary and decimal mappings.

Part

4 How Exinda uses the ToS / DiffServ Field

All Exinda products can read and write the ToS/DiffServ field, allowing users to:

- Match packets with a ToS/DSCP value and apply optimizer polices to this traffic.
- Mark the packets with a ToS/DSCP value based on source/destination host/subnet, source/destination port, layer 7 application, time of day, vlan id, etc.

4.1 Matching Packets

When defining Optimizer Policies on the Exinda appliance, there is a ToS/DSCP drop down that allows users to match only those packets with the specified ToS/DSCP value.

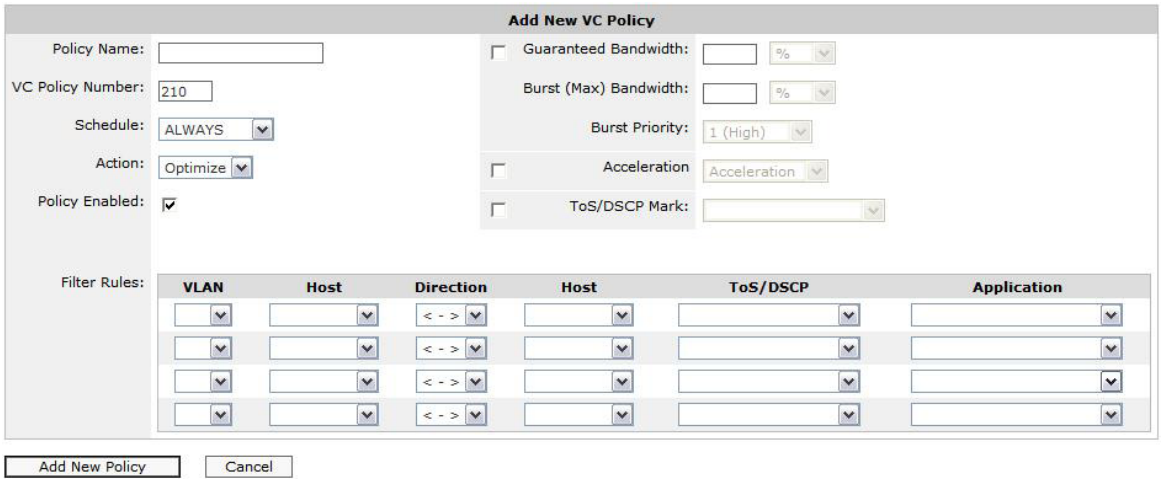


Figure 1: Optimizer Policy configuration page.

Users can select the appropriate DSCP/ToS value from this drop down field and any packets that match this ToS/DSCP value will be applied to this policy.

Example 1: VoIP equipment in a user's network may be configured to mark all outgoing packets as DSCP EF (decimal 46). VoIP is a real-time application and the user wishes to prioritize this with a high priority policy that guarantees VoIP a certain amount of WAN bandwidth. To achieve this, the user selects 'DSCP 46' from the ToS/DSCP drop down and configures the appropriate bandwidth allocation in this policy.

4.2 Marking Packets

Users may want to mark certain packets with a ToS/DSCP value so that external routers can treat the traffic appropriately. The same policy configuration screen above (see Figure 1) allows users to configure such an action.

When the policy action is set to 'Optimize', several options are available on the right-hand side, one of which is the 'ToS/DSCP Mark' checkbox. Users will need to enable this feature by checking the box and selecting the appropriate ToS/DSCP mark from the drop down.

Any traffic that matches the corresponding filter rules will then be marked with the specified value and should be treated appropriately by routing equipment down the line.

Example 2: Service Providers may provide users with a table similar to the one below (example only). Each class has different guaranteed service and pricing levels. This information should be used in conjunction with optimizer policies to implement and ensure quality of service. See Table 1 to convert the DSCP Settings to a decimal value that can be used in the Optimizer Policies.

Traffic Priority Class	IETF DiffServ Traffic Priority Class	DSCP Setting
Real Time (Gold)	Expedited Forwarding	EF
Mission Critical (Silver High)	Assured Forwarding	AF31
Business Critical (Silver Low)	Assured Forwarding	AF32/33
General Business (Bronze)	Best Effort	BE

Table 2: Example service provider DSCP class mapping table.

Index

- I -

- M -

- O -

- T -

- U -