

DoS-Attack Prevention Configuration Commands

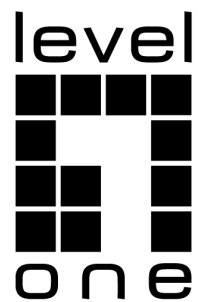


Table of Contents

Chapter 1 DoS Attack Prevention Configuration Commands	3
1.1 DoS-Attack Prevention Configuration Commands	3
1.1.1 dos enable.....	3

Chapter 1 DoS Attack Prevention Configuration Commands

1.1 DoS-Attack Prevention Configuration Commands

DoS attack prevention configuration commands are shown below:

- dos enable

1.1.1 dos enable

Syntax

dos enable {all | ip | l4port | mac | smac | pingflood | tcpflags | tcpsmurf | icmpsmurf | ipsmurf | nullscan}

no dos enable {all | ip | l4port | mac | smac | pingflood | tcpflags | tcpsmurf | icmpsmurf | ipsmurf | nullscan}

Parameter

Parameter	Description
all	Enables to prevent all kinds of DoS attacks.
ip	Enables to prevent the dos attack messages whose source IP address is same as its destination IP address.
l4port	Enables to check the layer-4 messages whose source port is same as its destination port.
mac	Enables to prevent the messages whose source MAC address is same as its destination MAC address.
smac	Enables to prevent multicast and broadcast packets
pingflood	Enables to check pingflood type packets
tcpflags	Starts to check the TCP packets with illegal flags.
tcpsmurf	Enables to prevent tcmsmurf type TCP messages
icmpsmurf	Enables to prevent icmpsmurf type icmp messages
ipsmurf	Enables to prevent ipsmurf type ipsmurf messages
nullscan	Enables to prevent tcp packets with tcp flag 0

Default

DoS attack prevention is disabled by default.

Usage Guidelines

DoS attack prevention is configured in global mode.

The ip sub-function can defend against IP messages whose source address is the same as destination address.

The l4port sub-function can drop TCP packets whose source layer-4 port number is the same as destination layer-4 port number.

The mac sub-function can defend against messages whose source MAC address is the same as destination MAC address.

The smac subfunction of dos discards multicast and broadcast packets.

The pingflood subfunction of dos discards ICMP packets.

The tcpfrags sub-function can drop the following 2 kinds of TCP packets: 1.TCP FIN URG PSH =1 & sequence = 0; 2.TCP FIN SYN =1

The tcpsmurf sub-function can defend against TCP messages whose last 8 bits of the destination IP are 255.

The icmpsmurf sub-function can defend against ICMP messages whose last 8 bits of the source and destination IPs both being 255

The ipsmurf sub-function can defend against IP messages whose last 8 bits of the destination IP are 255.

The nullscan sub-function can defend against TCP messages with tcp flag 0.

Example

The following example shows how to set globally defend against TCP packets whose last 8 digits of the destination IP are 255:

```
Switch(config)#dos enable tcpsmurf
```