DoS-Attack Prevention Configuration Commands

Table of Contents

Chapter 1 DoS Attack Prevention Configuration Commands

1.1 DoS-Attack Prevention Configuration Commands

DoS attack prevention configuration commands are shown below:

- dos enable
- show dos

1.1.1 dos enable

Syntax

dos enable {all | icmp *icmp-value* **| ip | ipv4firstfrag | l4port | mac | tcpflags | tcpfrag** *tcpfrag-value***}**

no dos enable {**all | icmp | ip | ipv4firstfrag | l4port | mac | tcpflags | tcpfrag**}

Parameter

Parameter	Description
all	Enables to prevent all kinds of DoS attacks.
icmp *icmp-value*	Prevents the ICMP DoS attacks. Here, the **icmp-value** parameter means the maximum length of ICMP packet, whose default value is 512.
ip	Prevents those DoS attack packets whose source IP addresses are equal to the destination IP addresses.
ipv4firstfrag	Starts to check the first fragment of IP packet.
l4port	Starts to check the L4 packets whose source port is equal to the destination port.
mac	Starts to check those packets whose source MACs are equal to destination MACs.
tcpflags	Starts to check the TCP packets with illegal flags.
tcpfrag *tcpfrag-value*	Starts to check the DoS attack packet of TCP fragment. Here, the ***tcpfrag-value*** parameter means the minimum TCP header, whose default value is 20.

Default value

DoS attack prevention is disabled by default.

Remarks

DoS attack prevention is configured in global mode.

The DoS IP sub-function can drop those IP packets whose source IPs are equal to the destination IPs.

The DoS ICMP sub-function can drop the following two kinds of packets: 1. ICMPv4/v6 ping packets whose size is larger than icmp-value; 2. ICMP packets.

The DoS l4port sun-function can drop those TCP/UDP packets whose source port is equal to the destination port.

The DoS MAC sub-function can drop those packets whose source MACs are equal to destination MACs.

The DoS tcpflags sub-function can drop the following 4 kinds of TCP packets: 1. TCP SYN flag=1 & source port<1024; 2.TCP control flags = 0 & sequence = 0; 3.TCP FIN URG PSH =1 & sequence = 0; 4.TCP FIN SYN =1.

The DoS tcpfrag sub-function can drop the following two kinds of TCP packets: 1. The TCP header is smaller than the first TCP fragment of **tcpfrag-value**; 2. TCP fragments whose offset values are 1.

Example

The following example shows how to set the global DoS attack prevention function to prevent those IP packets whose source IPs are destination IP addresses.

Switch_config#dos enable ip

The following example shows how to set DoS attack prevention in global mode to prevent those packets whose maximum ICMP length is bigger than 255.

Switch_config#dos enable icmp 255

1.1.2 show dos

Syntax

show dos

It is used to show all DoS attack prevention functions that users have set.

Parameter

N/A

Default value

N/A

Remarks

EXEC mode

Example

The following example shows how to display all DoS attack prevention functions.

```
Switch_config#dos enable all
Switch_config#show dos
dos enable ip
dos enable ipv4firstfrag
dos enable tcpflags
dos enable l4port
dos enable mac
dos enable tcpfrag
```

```
dos enable icmp
Switch_config#
```

The following example shows how to set **dos enable icmp** to display the sub-function that users have set.

```
Switch_config#dos enable icmp
Switch_config#show dos
dos enable icmp
```

The following example shows how to set **dos enable icmp 255** to display the sub-function that users have set.

```
Switch_config#dos enable icmp 255
Switch_config#show dos
dos enable icmp 255
```