

Anti-Attack Configuration Commands



Table of Contents

Chapter 1 Anti-Attack Configuration Commands.....	1
1.1 Anti-Attack Configuration Commands.....	1
1.1.1 filter period <i>time</i>	1
1.1.2 filter threshold <i>value</i>	1
1.1.3 filter block-time <i>value</i>	2
1.1.4 filter igmp.....	3
1.1.5 file ip source-ip.....	3
1.1.6 filter arp.....	3
1.1.7 filter enable.....	4
1.1.8 show filter.....	4

Chapter 1 Anti-Attack Configuration Commands

1.1 Anti-Attack Configuration Commands

1.1.1 filter period *time*

To configure filter period for attack, use the filter period command.

parameter

parameter	Description
<i>time</i>	The filter period for attack in seconds. It is considered as attack when the attack source sends packets above the specified number in any filter period time.

default

10 seconds

Command mode

Global configuration mode

example

Switch_config#filter period 15

Related commands

filter threshold value

1.1.2 filter threshold *value*

To configure the filter threshold value, use the filter threshold value command.

parameter

parameter	Description
<i>value</i>	It is considered as attack when the receiving packets exceeds the filter threshold value.

default

1000

command mode

global configuration mode

example

Switch_config#filter threshold 1500

Related commands**filter period time****1.1.3 filter block-time *value***

To configure the time to block attack resource, use the filter block-time value command.

parameter

parameter	description
<i>Value</i>	Time to block attack source in seconds.

default

300 seconds

command mode

global configuration mode

example

Switch_config#filter block-time 600

Related commands**filter period time****filter threshold value**

1.1.4 filter igmp

To filter IGMP attack, use the filter igmp command.

parameter

none

Command mode

Global configuration mode

example

Switch_config#filter igmp

Related commands

filter enable

1.1.5 file ip source-ip

To filter IP attack, use the file ip source-ip command.

parameter

none

Command mode

global configuration mode

example

switch_config#filter ip source-ip

related commands

filter enable

1.1.6 filter arp

To filter ARP attack, use the filter arp command.

parameter

none

Command mode

physical interface configuration mode

example

Switch_config_f0/1#filter arp

Related commands

filter enable

1.1.7 filter enable

To enable filter feature, use the filter enable command.

parameter

none

Command mode

Global configuration mode

example

Switch_config#filter enable

Related commands

filter igmp

filter arp

1.1.8 show filter

To display working state of the anti-attack feature of the current switch, use the show filter command.

parameter

none

command mode

non-user mode

Switch#show fil

Filter threshold: 1000 packet in any 10 seconds

Filters blocked:

Address	seconds	source interface
00a0.0c13.647d	27.0	FastEthernet1/2

Filters counting:

Address	seconds	count	source interface
00a0.0c43.647d	1.84	371	FastEthernet1/2

Filters blocked: indicates MAC address of the blocked attack source, blocked time and source interface.

Filters counting: indicates MAC address of the attack source, counting time, the number of the receiving packets and the source interface.