

# Attack Prevention Configuration (GTL-2091)



Digital Data Communications GmbH, Germany.

<http://www.level1.com>

# Table of Contents

Chapter 1 Attack Prevention Configuration.....	1
1.1 Overview.....	1
1.2 Attack Prevention Configuration Tasks .....	1
1.3 Attack Prevention Configuration .....	1
1.3.1 Configuraing the Attack Detection Parameters.....	1
1.3.2 Configuring the Attack Prevention Type .....	1
1.3.3 Starting up the Attack Prevention Function .....	2
1.3.4 Checking the State of Attack Prevention .....	2
1.4 Attack Prevention Configuration Example .....	2

# Chapter 1 Attack Prevention Configuration

## 1.1 Overview

To guarantee the reasonable usage of network bandwidth, our 6508 series switches provide the function to prevent vicious traffic from occupying lots of network bandwidth. In light of current attack modes, our 6508 series switches can limit the hosts that send lots of ARP, IGMP or IP message in a period of time and do not provide any service to these hosts. The function can prevent malicious message from occupying lots of network bandwidth. Therefore, the network can not be congested.

## 1.2 Attack Prevention Configuration Tasks

When the number of IGMP, ARP or IP message that is sent by a host in a designated interval exceeds the threshold, we think that the host attack the network.

You can select the type of attack prevention (ARP, IGMP or IP), the attack prevention port and the attack detection parameter. You have the following configuration tasks:

- Configuring the attack prevention type
- Configuring the attack detection parameters

## 1.3 Attack Prevention Configuration

### 1.3.1 Configuring the Attack Detection Parameters

Command	Description
<b>filter period</b> <i>time</i>	Sets the attack detection period to <b>time</b> , whose unit is second.
<b>filter threshold</b> <i>value</i>	Sets the attack detection threshold to <b>value</b> . The parameter <b>value</b> represents the number of message at the threshold.
<b>filter block-time</b> <i>time</i>	Sets the out-of-service time for the attack source when the attack source is detected. Its unit is second.

### 1.3.2 Configuring the Attack Prevention Type

Command	Description
<b>filter igmp</b>	Detects the igmp attack.
<b>filter ip source-ip</b>	Detects the IP attack based on the source IP address.
<b>interface f x/y</b>	Enters interface configuration mode for

	interface y at slot X.
<b>filter arp</b>	Detects the arp attack.

The ARP attack takes the host's MAC address and the source port as the attack source, that is, message from the same MAC address but different ports cannot be calculated together. Both the IGMP attack and IP attack take the host's IP address and source port as the attack source.

Remember that the IGMP attack prevention and the IP attack prevention cannot be started up together.

### 1.3.3 Starting up the Attack Prevention Function

After all parameters for attack prevention are set, you can start up the attack prevention function. Note that small parts of processor source will be occupied when the attack prevention function is started.

Command	Description
<b>filter enable</b>	Starts up the attack prevention function.

Use the **no filter enable** command to disable the attack prevention function and remove the block to all attack sources.

### 1.3.4 Checking the State of Attack Prevention

After attack prevention is started, you can run the following command to check the state of attack prevention:

Command	Description
<b>show filter</b>	Checks the state of attack prevention.

## 1.4 Attack Prevention Configuration Example

To enable the IGMP attack prevention and the ARP attack prevention on port 1/2, consider any host that sends more than 1200 pieces of message within 15 seconds as the attack source and to cut off network service for any attack source.

```
filter period 15
filter threshold 1200
filter block-time 600
interface g0/2
filter arp
exit
filter enable
```