Attack Prevention Configuration

Table of Contents

Chapter 1 Attack Prevention Introduction..... 1
1.1 Overview of Filter..... 1
1.2 The Mode of Filter..... 1
Chapter 2 Attack Prevention Configuration..... 2
2.1 Attack Prevention Configuration Tasks..... 2
2.2 Attack Prevention Configuration..... 2
2.2.1 Configuring the Attack Filter Parameters..... 2
2.2.2 Configuring the Attack Prevention Type..... 2
2.2.3 Enabling the Attack Prevention Function..... 3
2.2.4 Checking the State of Attack Prevention..... 3
Chapter 3 Attack Prevention Configuration Example..... 4
3.1 Using Filter ARP to Protect the LAN..... 4
3.2 Using Filter IP to Protect Layer-3 Network..... 4

Chapter 1 Attack Prevention Introduction

1.1 Overview of Filter

To guarantee the reasonable usage of network bandwidth, this switch series provides the function to prevent vicious traffic from occupying lots of network bandwidth.

Filter can identify the packets received by the interface of the switch and calculate them according to the packet type. In light of current attack modes, Filter can calculate the number of ARP, IGMP or IP message that a host sends in a time. Once the number exceeds the threshold, the OLT will not provide any service to these hosts.

Filter limits the packet from a certain host by blocking the source address. For ARP attack, Filter blocks source MAC address; for IP attacks, such as Ping scan and TCP/UDP scan, Filter blocks source IP address.

1.2 The Mode of Filter

The mode of Filter determines how the switch specifies the attack source. There are two modes of Filter.

Source Address Block Time (Raw)

In Raw mode, the switch will drop packets from the attack source in scheduled block-time since the attack source is determined. After block-time, the restriction on the attack source will be removed and a new calculation will be enabled.

In Raw mode, all the packets from the source address will be blocked. For instance, when the MAC address of the attack source is blocked, all packets whose source MAC address are the same with that of the attack source will be dropped, no matter it is ARP, ICMP, DHCP or other types.

Source Address Block Polling (Hybrid)

After blocking the attack source, the switch will continue calculate the packets from the attack source and detect whether the packet number exceeds the threshold before the end of Polling Interval. If the packet number exceeds the threshold, the blocking state keeps. Otherwise, the blocking will be removed. In Hybrid Mode, the packet number when initially determining the attack source and the threshold of the packet number in Polling can be configured independently.

To realize continually calculate the packet, in the hybrid mode the packet type will be matched while the source address is blocked. For instance, if the MAC address of a host is blocked as it triggers ARP attack, IP packets from the host will be sent by the switch continually, unless the host is also identified with the existence of IP attack.

Please select the mode of Filter according to your application environment. If you want to set a strict limit on the attack source and reduce the burden of switch CPU, please use Raw mode; if you want to control the attack source flexibly and resume communication of the host as soon as possible after the end of the attack, please use Hybrid mode. Note that the Filter number a switch can support in Hybrid mode is limited. In condition of inadequate Filter number, Raw mode will be adopted automatically.

Chapter 2 Attack Prevention Configuration

2.1 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 filter parameters

Configuring the attack prevention type

Enables the attack prevention function.

Checking the State of Attack Prevention

2.2 Attack Prevention Configuration

2.2.1 Configuring the Attack Filter Parameters

In global configuration mode, run the following command to configure the parameters of Filter.

Command	Purpose
Switch# config	Enters the global configuration mode.
Switch_config# **filter period** *time*	Sets the attack filter period to time. Its unit is second.
Switch_config# **filter threshold [arp | bpdu | dhcp | igmp | ip | icmp]** *value*	Sets the attack filter threshold to value.
Switch_config# **filter block-time** *time*	Sets the out-of-service time (block-time) for the attack source when the attack source is detected. Its unit is second.
Switch_config# filter polling period time	Sets the filter polling period in Hybrid mode. Its unit is second.
Switch_config# filter polling threshold [arp | bpdu | dhcp | igmp | ip | icmp] value	Sets the filter polling threshold in Hybrid mode.
Switch_config# filter polling auto-fit	Sets the corresponding parameters of period and threshold of polling filter which adapts to the attack source filter. The command is efficient by default. The polling period equals with the attack filter period and the polling packet threshold equals to 3/4 of the attack filter packet threshold

2.2.2 Configuring the Attack Prevention Type

In global and interface configuration mode, use the following command to configure the type of attack filter.

Command	Purpose
Switch# config	Enters the global configuration mode.
Switch_config# filter dhcp	Enables DHCP packet attack filter in the global configuration mode.
Switch_config# filter icmp	Enables ICMP packet attack filter.
Switch_config# **filter igmp**	Enables IGMP packet attack filter.

Switch_config# **filter ip source-ip**	Enables IP attack filter in the global configuration mode.
Switch_config# **interface intf-name**	Enters the interface configuration mode.
Switch_config_intf# **filter arp**	Enables ARP packet attack filter on the interface.
Switch_config_intf# filter bpdu	Enables BPDU packet attack filter on the interface.
Switch_config_intf# filter dhcp	Enables DHCP packet attack filter on the interface.
Switch_config_intf# filter icmp	Enables ICMP packet attack filter on the interface.
Switch_config_intf# filter ip source-ip	Enables IP packet attack filter on the interface.

Note:

ARP attack takes the combination "the host mac address + the source port" as an attack source. That is to say, packets with the same MAC address but coming from different ports, the count will not be accumulated. Both the IGMP attack and IP attack take the host's IP address and source port as the attack source.

Note:

1、 The IGMP attack prevention and the IP attack prevention cannot be started up together.

2. IP, ICMP and DHCP filter take effect only in global and interface configuration mode.

2.2.3 Enabling 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	Purpose
Switch_config# **filter enable**	Enables the attack prevention function.
Switch_config# filter mode [raw | hybrid]	Sets the mode of Filter: Raw or Hybrid.

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

2.2.4 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	Purpose
show filter	After attack prevention is started, you can run the following command to check the state of attack prevention:
show filter summary	Checks the parameter configuration and summary information of Filter.

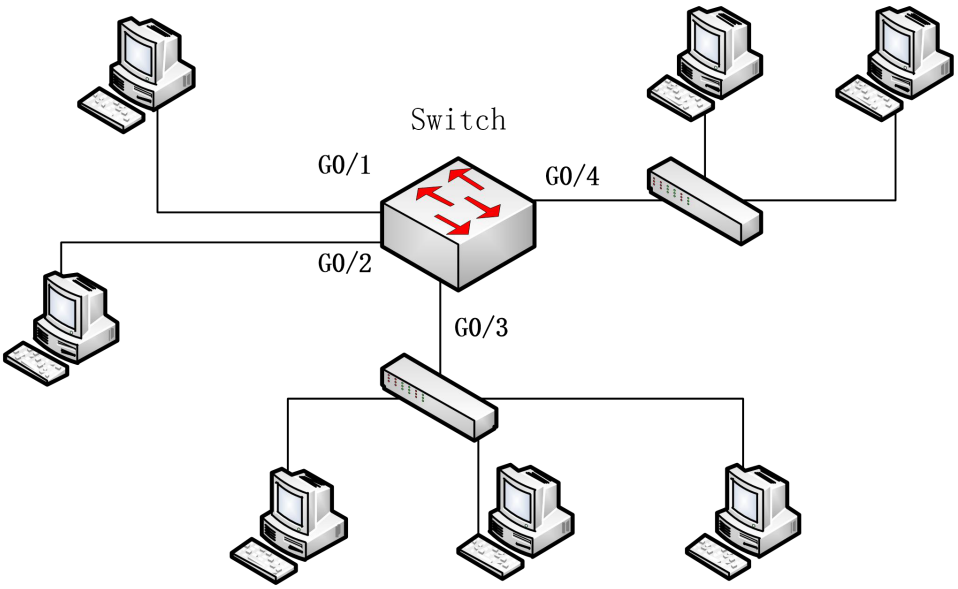
Chapter 3 Attack Prevention Configuration Example

Note:

The examples shown in this chapter is only a reference for Filter configuration. Please configure according to your actual network condition.

3.1 Using Filter ARP to Protect the LAN

As shown in the following figure, configure ARP attack Filter on Switch.



Sets the parameter of Filter. A host sending more than 100 ARP messages in 10s will be taken as an attack source.

Switch# config

Switch_config# filter period 10

Switch_config# filter threshold arp 100

Sets APR attack filter with 4 ports:

Switch_config# interface range g0/1 – 4

Switch_config_intf# filter arp

Sets Raw mode and enable Filter:

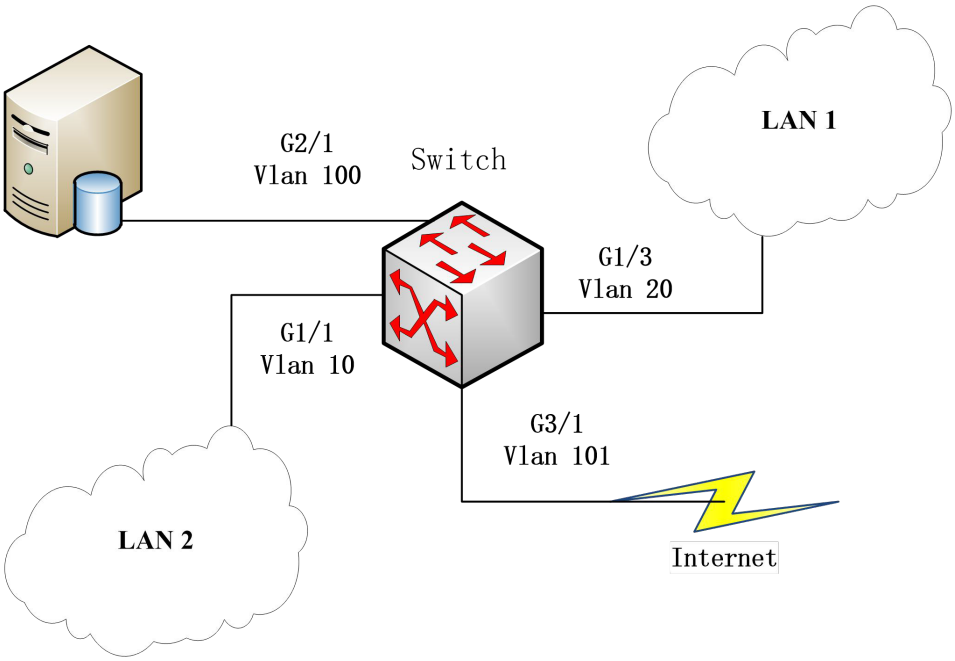
Switch_config_intf# exit

Switch_config# filter mode raw

Switch_config# filter enable

3.2 Using Filter IP to Protect Layer-3 Network

As shown in the following figure, Switch is connected to multiple LANs, servers and the internet. IP packet attack prevention can block IP scan of cross-subnet and large network connections triggered by BitTorrent in a short time.



Sets the parameter of Filter. A host sending more than 300 ARP messages in 1 minute will be taken as an attack source.

Switch# config

Switch_config# filter period 60

Switch_config# filter threshold ip 300

Enable IP packet filter in the global configuration mode and the interface mode. Note that the interface connecting the server and the external network is no need to configure:

Switch_config# filter ip source-ip

Switch_config# interface g1/1

Switch_config_g1/1# filter ip source-ip

Switch_config_g1/1# interface g1/3

Switch_config_g1/3# filter ip source-ip

Switch_config_g1/3# exit

Switch_config#

Enables Filter:

Switch_config# filter enable