FSOS

Attack Protection Configuration

Contents

1. Attack Protection

1.1 Anti-DDOS Attack Function

Dos is short of Denial of Service. DoS attack caused by the attack is known as DdoS. Its purpose is that let computer or network not provide normal services.

Dos attack is a simple and effective attack method which is very harmful to many network attack technologies. It is through various means to consume network bandwidth and system resources, or attack system defects, so that the normal service of normal system is paralyzed state, and cannot service normal user. It achieves to deny normal user accessing services, so in the internet anti-DOS attack is more important. Configure the anti-TTL attack.

According to the relevant standard, the TTL field in the IP header must be greater than 0. By default, if the message of TTL = 0 is received, the switch discards the message as an attack, but allows the message of ttl = 0 to be discarded.

1.1.1 Anti-TTL Attack

Configure anti-TTL attack

operation	command	remark
Enter the global configuration mode	configure terminal	-
Enable anti-TTL attack	anti-dos ip ttl	Optional. By default, messages with ttl = 0 are discarded
Disable the anti-TTL attack	no anti-dos ip ttl	Optional, After configuration, normal messages are processed
View the configuration information	show anti-dos	optional

1.1.2 Configure Anti-IP Fragment Attack

If the number of an IP message fragment is many, the switch will take up too many system resources and may affect other messages. Therefore, a reasonable limit for the length of the IP message does not allow too many fragments. If the number of fragment exceeds the specified value, the message is discarded as an attack message. By default, an IP message has 800 fragments.

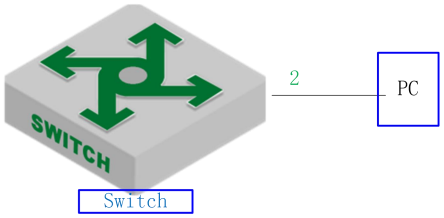
Configure Anti-IP Fragment Attack

operation	command	remark
Enter the global configuration mode	configure terminal	-
Set the maximum number of IP messages allowed	[no]anti-dos ip fragment ***max- numbers***	Optional, no command restores the default value of 800

1.1.3 Configuration Example

1、Network Requirement

The PC directly connects to the switch and communicates. Verify how the DUT handles more than the permitted fragment and the normal fragment, respectively. The switch: ip=10.5.2.134； PC IP=10.5.2.91



Anti-dos attack

2、Configuration steps

Configure an IP message to have up to two fragments

DUT needs two fragments of the IP message, you can communicate properly

Switch(config)#ping -l 2800 10.5.2.91

PING 10.5.2.91: with 2800 bytes of data:

reply from 10.5.2.91: bytes=2800 time<10ms TTL=64

reply from 10.5.2.91: bytes=2800 time<10ms TTL=64

reply from 10.5.2.91: bytes=2800 time<10ms TTL=64

reply from 10.5.2.91: bytes=2800 time<10ms TTL=64

reply from 10.5.2.91: bytes=2800 time<10ms TTL=64

----10.5.2.91 PING Statistics----

5 packets transmitted, 5 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

DUT needs three fragments of the ip message, you cannot communicate

Switch(config)#ping -l 3000 10.5.2.91

PING 10.5.2.91: with 3000 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Request timed out.

no answer from 10.5.2.91

Delete ip fragmentation configuration (restore the default value of 800), and then need to send three pieces of ip messages, communication is normal

Switch(config)#no anti-dos ip fragment

Switch(config)#ping -l 3000 10.5.2.91

PING 10.5.2.91: with 3000 bytes of data:

reply from 10.5.2.91: bytes=3000 time=10ms TTL=64
reply from 10.5.2.91: bytes=3000 time<10ms TTL=64
reply from 10.5.2.91: bytes=3000 time=10ms TTL=64
reply from 10.5.2.91: bytes=3000 time<10ms TTL=64
reply from 10.5.2.91: bytes=3000 time<10ms TTL=64

----10.5.2.91 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/4/10

1.2 CPU-car Function

A large number of messages on the CPU will cause the CPU busy. This function is used to limit the rate of receiving messages by the CPU.

1.2.1 Configure Cpu-car

Cpu-car is enabled by default and does not support the shutdown function

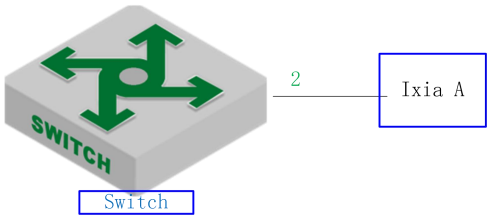
Configure cpu-car

operation	command	remark
Enter the global configuration mode	configure terminal	-
Configure the cpu-car rate	[no]cpu-car ***value***	Optional, The no command restores the default value 400pps
View the configuration information	show cpu-car	optional
View cpu receiving packet port statistics	show cpu-statistics [ethernet ***port-number***]	optional
Clear cpu receiving packet port statistics	clear cpu-statistics	optional
View cpu receiving packet classification statistics	show cpu-classification [interface ethernet ***port-number***]	optional
Clear cpu receiving packet classification statistics	clear cpu-classification [interface ethernet ***port-number***]	optional
View cpu utilization	show cpu-utilization	optional

1.2.2 Configuration Example

1、Network Requirement

Limit the rate of message less than 50 pps on the switch.



cpu-car schematic diagram

2. Configuration steps

Configure the cpu-car speed to 50 pps

Switch(config-if-ethernet-0/0/2)#port-car-rate 50

View Configuration Information

Switch(config)#show cpu-car

Send packet to cpu rate = 50 pps.

3. Validation results

Ixia A sends icmp request messages to the DUT: at a rate of 100 pps for 10 seconds, the total number of messages on the dut is 600, indicating that the cpu-car function takes effect.

Switch(config)#clear cpu-statistics

Switch(config)#clear cpu-classification

Switch(config)#clear interface

Switch(config)#show cpu-statistics ethernet 0/0/2

Show packets sent to cpu statistic information

port	64Byte	128Byte	256Byte	512Byte	1024Byte	2048Byte
e0/0/2	600	0	0	0	0	0

Switch(config)#show cpu-classification

Type	Count	Percent(%)
Total	600	100
BPDU	0	0
ERRP	0	0
ARP	0	0
MLD	0	0
IGMP	0	0
ICMP	600	100
OSPF	0	0
RIP	0	0
DHCP	0	0
SNMP	0	0
Telnet	0	0
PIM	0	0

BGP 0 0
SSH 0 0
Other 0 0
Switch(config)#show statistics interface ethernet 0/0/2

Port number : e0/0/2
last 5 minutes input rate 5248 bits/sec, 10 packets/sec
last 5 minutes output rate 433832 bits/sec, 771 packets/sec
64 byte packets:1048
65-127 byte packets:0
128-255 byte packets:0
256-511 byte packets:0
512-1023 byte packets:0
1024-1518 byte packets:0
1048 packets input, 67072 bytes , 0 discarded packets
1048 unicasts, 0 multicasts, 0 broadcasts
0 input errors, 0 FCS error, 0 symbol error, 0 false carrier
0 runts, 0 giants
19 packets output, 1216 bytes, 0 discarded packets
0 unicasts, 9 multicasts, 10 broadcasts
0 output errors, 0 deferred, 0 collisions
0 late collisions
Total entries: 1.

1.3 Shutdown-Control Overview

When the network appears loop or malicious attack, there will be a lot of messages, these messages waste bandwidth or even make the network equipment in the collapse of the edge, and affect the normal use of other users. The shutdown-control function is used to avoid excessive messages in the network. It monitors the bandwidth of each port on the switch. When the number of unknown messages received by the port exceeds the security set by the administrator threshold, the shutdown-control function automatically shuts down the port to ensure that the other links and devices are protected from the impact in the network.

1.3.1 Enable/disable Shutdown-Control

Enable/disable Shutdown-Control

operation	command	remark
Enter the global configuration mode	configure terminal	-
Enter the port configuration mode	interface ethernet *port-num*	-

Enable and configure the shutdown rate	shutdown-control **{broadcast |multicast |unicast}*rate***	required
Shutdown function	no shutdown-control **{broadcast |multicast |unicast}**	optional ，default close
View the configuration information	show shutdown-control interface [ethernet ***port-numer***]	optional

1.3.2 Configure Recovery Mode

Port is shutdown, need to manually restore by default. Administrators can configure automatic recovery, and set the recovery cycle, the default is 480s.

Configure recovery mode

operation	command	remark
Enter the global configuration mode	configure terminal	-
Configure the recovery mode	[no] shutdown-control-recover mode {**automatic** | **manual**}	Optional, manual and no commands are used to restore the default configuration
Configure the automatic recovery period	[no] shutdown-control-recover automatic-open-time ***value***	optional，Default 480s, only valid for automatic recovery
View configuration information	show shutdown-control interface [ethernet ***port-number***]	optional

1.3.3 Manually Restore Shutdown Port

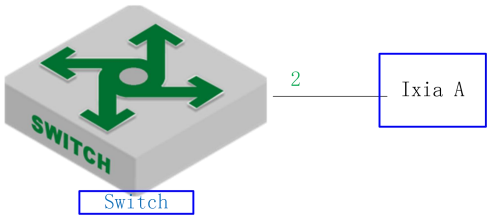
Manually restore shutdown port

operation	command	remark
Enter the shutdown port configuration mode	interface ethernet ***port-number***	required
Command the shutdown port	shutdown	required
Restore the port	no shutdown	required

1.3.4 Configuration Example

1、Network Requirement

Port 2 receiving unknown unicast rate is limited for 1000pps, if it is shutdown, automatic recovery, the default value 480s is used for recovery cycle.



Shutdown-control sketch map

2.configuration steps

Enable the unknow unicast shutdown-control function and set the rate to 1000 pps

Switch(config)#interface ethernet 0/0/2

Switch(config-if-ethernet-0/0/2)#shutdown-control unicast 1000

Switch(config-if-ethernet-0/0/2)#ex

View Configuration Information

Switch(config)#show shutdown-control interface ethernet 0/0/2

port shutdown control recover mode : automatic

Port recover time(second) : 480

port shutdown control information :

PortID	Broadcast status	Broadcast value	Multicast status	Multicast value	Unicast status	Unicast value	RemainTime
e0/0/2	disable	-	disable	-	enable	1000	-

Total entries: 1 .

3. Validation results

Switch(config)#logging monitor 0

The tester sends an unknown message to the DUT 0/0/2 at a rate of 1100 pps.

Switch(config)#05:12:04: Switch: %DEVICE-3-LINKUPDOWN: e0/0/2 LinkDown.

05:12:04: Switch: %OAM-5-SHUTDOWN-CTRL: port e0/0/2 **was shutdown.**

Switch(config)#show shutdown-control interface ethernet 0/0/2

port shutdown control recover mode : automatic

Port recover time(second) : 480

port shutdown control information :

PortID	Broadcast status	Broadcast value	Multicast status	Multicast value	Unicast status	Unicast value	**RemainTime**
e0/0/2	disable	-	disable	-	enable	1000	**07min48sec**

Total entries: 1 .

Switch(config)#show interface brief ethernet 0/0/2

Port	Desc	Link	shutdn	Speed	Pri	PVID	Mode	TagVlan	UtVlan
e0/0/2		down	**ERROR**	auto	0	1	hyb		1

Total entries: 1 .

Switch(config)#05:20:06: Switch: %DEVICE-3-LINKUPDOWN: e0/0/2 LinkUp.

05:20:08: Switch: %OAM-5-PORTRECOVER: port e0/0/2 **recover.**

1.4 Anti-DHCP Attack

Normally, when the dhcp client obtains ip from the dhcp server, the rate of dhcp message sent by the dhcp client is very small. Generally, it doesn't cause the dhcp server disabled. However, a malicious attacker may send large rate dhcp message to the dhcp server, which will cause the dhcp server busy, affect the allocation of ip for other clients, and even cause panic.

The anti-dhcp attack function restricts the dhcp message rate of the dhcp client. Over-rate client will be considered as malicious attackers, according to a good strategy to deal, so as to protect the dhcp server to work normally.

1.4.1 Enable/disable Anti-DHCP

Enable/disable Anti-DHCP

operation	command	remark
Enter the global configuration mode	configure terminal	-
Enable/disable Anti-DHCP	[no] dhcp anti-attack	required，off by default
View configuration information	show dhcp anti-attack [interface ethernet ***port-numbwer***]	optional

1.4.2 Configure Processing Policy

After the switch detects an attack, it can take two actions: 1) Discard all the messages of the client (based on the source MAC address of messages to distinguish) 2) Discard only the dhcp message of the client (according to the source MAC address of the message to distinguish), that is, the client is not assigned ip.

When the switch detects an attack, it sends the source MAC address of the attack message to the attack entry. If the policy drops all packets, user can manually bind the attack entry to a black hole MAC address.

Configure processing policy

operation	command	remark
Enter the global configuration mode	configure terminal	-
Configure processing policy	dhcp anti-attack action [deny-all | deny-dhcp]	Optional, deny-dhcp by default
Bind black hole mac table	dhcp anti-attack bind blackhole [all |	Optional, It can be

	mac-address]	configured only when deny-all is specified
View configuration information	show dhcp anti-attack [interface ethernet ***port-number***]	optional

1.4.3 Configure Rate Threshold

In the anti-dhcp attack, the rate of dhcp message sent by the same user is determined whether there is attack. If the rate is equal to or higher than 16 pps, the message is considered as an attack. The administrator is allowed to modify the rate threshold.

Configure rate threshold

operation	command	remark
Enter the global configuration mode	configure terminal	-
Configure rate threshold	[no] dhcp anti-attack threshold ***value***	Optional, 16pps by default
View configuration information	show dhcp anti-attack [interface ethernet ***port-number***]	optional
Enter the port configuration mode	interface ethernet ***port-number***	-
Configure rate threshold	[no]dhcp anti-attack threshold ***value***	optional

1.4.4 Configure Recovery Function

When the switch detects an attack, it sends the source MAC address of the attack message to the attack table item. The attack table item maintains an aging time. When the aging time expires, the table item is deleted. The default aging time is 10 minutes. If you do not want to delete a table item, you can configure 0.

Configure recovery function

operation	command	remark
Enter the global configuration mode	configure terminal	-
View Configuration Information	show dhcp anti-attack [interface ethernet ***port-number***]	Optional, and display attack table item
Configure recovery time	dhcp anti-attack recover-time ***value***	optional，10m by default，0 means no aging
Configure manual recovery	dhcp anti-attack recover [all | ***mac-address***]	The table items are restored immediately, and do not need to

		wait for the aging time to expire

1.4.5 Configure Trusted Ports

By default, all ports are considered to be untrustworthy after the global anti-dhcp attack is enabled, and you need to monitor whether the dhcp attack exists or not. If the port does not appear dhcp attack, it can be modified into a trust port, so you do not need to monitor whether there dhcp attack or not.

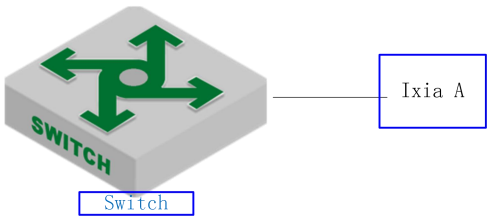
Configure trusted port

operation	command	remark
Enter the port configuration mode	interface ethernet ***port-number***	-
Configure whether the port is a trusted port	[no]dhcp anti-attack trust	optional，un-trusted port by default
View configuration information	show dhcp anti-attack interface ethernet ***port-number***	optional

1.4.6 Configuration Example

I. Network requirement

The switch is regarded as dhcp server, and the anti-dhcp attack function is enabled. Ixia A emulates the PC to send dhcp message. To demonstrate the effect, configure the anti-dhcp attack rate threshold to 1pps, and enable the auto-recovery function.



Anti-DHCP attack

2、configuration example

DHCP server configuration omitted, please refer to the relevant manual

#configure anti-DHCP attack

Switch(config)#dhcp anti-attack

Switch(config)#dhcp anti-attack action deny-dhcp

Switch(config)#dhcp anti-attack threshold 1

Switch(config)#dhcp anti-attack recover-time 3

Display the log information (No need to configure the actual use)

Switch(config)#logging monitor 0

Switch(config)#debug dhcp

3. Validation results
Ixia A sends dhcp request message to dut at the rate of 2 pps. The log information is as follows:

```
Switch(config)#
05:26:56: Switch: %DHCP-4-DHCP: 19616:33: Deny user 00:00:00:01:11:23,dhcpRate 2pps
05:26:58: Switch: %DHCP-4-DHCP: 19618:33: Deny user 00:00:00:01:11:23,dhcpRate 2pps

# Send the attack entry
Switch(config)#show dhcp anti-attack
Dhcp anti-attack: enabled
Dhcp rate limit:1pps
User recovery time:3 minutes
Reject type:DenyDHCP
DeniedSrcMAC            Port        Vlan      DenyType    RemainAgingTime(m)
00:00:00:01:11:23       e0/0/1      2         DenyDHCP    3

Total entry: 1.

#After 3 minutes, the attack entry is aged out
Switch(config)#show dhcp anti-attack
Dhcp anti-attack: enabled
Dhcp rate limit:1pps
User recovery time:3 minutes
Reject type:DenyDHCP
DeniedSrcMAC            Port        Vlan    DenyType    RemainAgingTime(m)

Total entry: 0.
```

1.5 ARP Spoofing and Flood Attack

1.5.1 Overview for ARP Spoofing

If two hosts need to communicate, they should know each other's MAC address. ARP protocol makes this procedure transparent to users. However, there is no certification instructions in ARP protocol, it left the door open for attacker as a consequence.

All devices in LAN can receive the ARP request of host A, so if host C is an attacker, he pretends to be host B to send ARP reply to host A "my address is 00:00:00:00:00:03" , host A will unconditionally believe in this reply and then add or cover the intrinsical APR table. However, the IP of this table is 192.168.1.4 while its corresponding MAC is 00:00:00:00:00:03.

So the host C can be able to intercept and capture the message which should be sent to host B. Due to host A is treat by false ARP, this is also called the ARP spoofing attacks.

After enabling this function, all ARP which will go through Switch will be redirected to CPU for a check. The ARP packets will be checked one by one whether they are complete matched with static arp table, ip-source-guard static binding table and dhcp-snooping table. If there exists one cannot be complete matched, it will stop the follow-up inspection and this arp packet can be transmitted. If there exists one incomplete matching (partial matching) table, the arp packet will be discarded. If there is no corresponding static ARP table, static ip-source-guard table and dhcpsnooping will be handled according to configured strategy: discard or flood (send to all ports), the function of anti-ARP spoofing attack will be disabled by default.

1.5.2 Overview for ARP Flooding Attack

Arp flood attack is generally attack the network device (for example: router, Switch, server and so on) with large number of message traffic, exhausting the CPU resource of network device and then leading to the network paralysis.

When facing to such kind of flood attack, the most important thing is to ensure the normal operation of the network device, preventing widespread network paralysis. There are various flood attacks, and the most damage to device is ARP attack. According to the above mentioned ARP mechanism, all network devices will send the ARP request packet to CPU to handle after they receives the ARP request packet. Only in this way can they judge if they are the other equipment who request its MAC address. ARP flood attack takes advantages of this ARP mechanism flaw, randomly sending a lot of ARP request packet to attack the network equipment in the local area network (LAN) .

Main purpose of ARP flood attacker is to impact the network equipment's CPU, and then run out the CPU resources of the core equipment. Switch should judge it ahead of time and forbid the transmission of flood packet so as to defense the attack of this type.

arp anti-flood function can be able to identify each ARP flow and then judge whether it's ARP flood attack according to configured safe ARP rate-value. The Switch will take it as flood attack if the ARP traffic of a certain host exceeds the configured ARP rate-value, and it will put this virus-host into blacklist to forbid the packet transmission from this host.

In order to facilitate the management and maintenance of network administrators, it can be able to perform auto-protect and save relevant warning message. As to those users who have been forbidden, administrator can configure it as manual recovery or automatic recovery.

The whole process on the Switches are as follows:

Enable arp anti-flood function, report the ARP packet to CPU, identify different flow according to the source MAC address of ARP packet.

Configure the safe ARP rate. Switch will take it as ARP attack if the rate exceeds the configured threshold value.

If you select the above deny-all command, when one ARP traffic exceeds configured threshold value, the Switch will put this MAC address into blackhole address list and forbid the this address's packet transmission according to source MAC address.

If you select the above deny-arp command, the Switch will not deal with the subsequent ARP message based on source mac address when ARP traffic is larger than the configured threshold.

As to the recover for those messages which are forbidden to forward, administrator could configure the recovery time as automatic recovery or handwork recovery.

1.5.3 Anti-Spoofing Configuration

Operation	**Command**	Remarks
Enter global configuration mode	**configure terminal**	
Enable arp anti-spoofing	**arp anti-spoofing**	
Disable arp anti-spoofing	**no arp anti-spoofing**	
Configure the approach for unknown message: discard or flooding	**arp anti-spoofing unknown {diacard | flood}**	unknown arp packet refers to the ip of those arp packets which cannot match with any item of the ip options of arp static table, ip-soure-guard binding table, dhcp-snooping table. In other word, this ip does not exist in the table.

1.5.4 Host Protection Configuration

Configure ip+port binding when configuring to discard the unknown arp packet, and then the arp packet of this ip can flood to other ports only via this valid port. If the arp packet of this ip enters from other ports, it will be discarded.

Operation	**Command**	Remarks
Enter global configuration mode	**configure terminal**	
Enable arp anti-spoofing	**arp anti-spoofing**	
Configure the process mode of unknown ARP message to be discard	**arp anti-spoofing unknown flood**	
Configure host	**host-guard bind ip** *ipaddress* **interface**	

protection	**ethernet** *device/slot/port*	
Delete host protection	**no host-guard bind { ip** *ipaddress* **| interface ethernet** *device/slot/port* **}**	

1.5.5 Configure Source-MAC Consistency Inspection

As to a certain ARP attack packet, their source-MAC in the head of Ethernet data is different from the source-MAC in ARP protocol. After enabling source-MAC consistency inspection, Switch will inspect whether the Ethernet source MAC address in ARP packet is the same as the source MAC in ARP protocol packet. If they are not the same, Switch will discard the packet.

This function is disabled by default.

Operation	**Command**	Remarks
Enter global configuration mode	**configure terminal**	
Enable arp anti-spoofing	**arp anti-spoofing**	
Enable source-mac consistency inspection	**arp anti-spoofing valid-check**	
Disable source-mac consistency inspection	**no arp anti-spoofing valid-check**	

1.5.6 Configure Anti-Gateway-Spoofing for Layer-3 Equipment

When the layer-3 Switch acts as the gateway for some certain LAN equipment, this Switch will list the attacker who wants to simulate the switch into blacklist, and it will send gratuitous ARP to notice the LAN equipment that “It is I who is the correct gateway”.

This function is disabled by default.

Operation	**Command**	Remarks
Enter global configuration mode	**configure terminal**	
Enable arp anti-spoofing	**arp anti-spoofing**	
Enable anti-gateway-spoofi	**arp anti-spoofing deny-disguiser**	

ng		
Disable anti-gateway-spoofing	**no arp anti-spoofing deny-disguiser**	

1.5.7 Configure the Trust Port

The trust port will not perform attack and spoof check when it receives arp message.

Operation	**Command**	Remarks
Enter port configuration mode	**interface ethernet** *device/slot/port*	
Configure the port to be trust port	**arp anti trust**	Untrust by default
Recover the port to be untrust port	**no arp anti trust**	

1.5.8 Anti-Flood Attack Configuration

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Enable anti-ARP flooding attack	**arp anti-flood**	required
Disable anti-ARP flooding attack	**no arp anti-flood**	
Configure safety trigger threshold	**arp anti-flood threshold** *threshold*	optional By default, the safety trigger threshold is 16PPS.
Configure approach for the attacker	**arp anti-flood action {deny-arp|deny-all}**	optional By default, approach for the attacker is deny arp.
Configure automatically banned user recovery time	**arp anti-flood recover-time** *time*	optional Configurable time range to be<0-1440> minutes; if you set the

		value to be 0, it means that you should manually restored. By default, the user automatically banned recovery time is 10 minutes.
Banned user manual resume forwarding	**arp anti-flood recover {***H:H:H:H:H:H* **| all}**	optional
To bind the dynamic blackhole MAC to be static blackhole MAC	**arp anti-flood bind blackhole {***H:H:H:H:H:H* **| all}**	Only when the process mode is deny-all can it generate as the mac of non-stationary black hole
Enter interface configuration mode	**interface ethernet** *device/slot/port*	
Configure threshold limit values for the port	**arp anti-flood threshold** *threshold*	It takes effect only when threshold limit values of the port is smaller than global threshold limit values.

1.5.9 Display and Maintain

Operation	**Command** 行	Remarks
Display arp anti-spoofing configuration	**show arp anti-spoofing**	
Display ARP anti-flood configuration and attackers list	**show arp anti-flood**	It can be executed under any mode.
Display the state of interface	**show arp anti interface**	

1.5.10 Example for Anti- ARP Spoofing Configuration

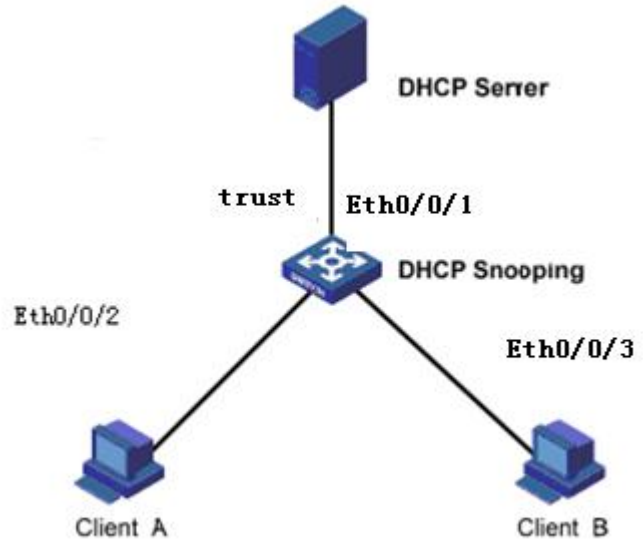
Network requirements

As shown in the figure, Eth0/0/1 port of SwitchA connects to DHCP server, Eth0/0/2 port and Eth0/0/3 port connect to Client A and Client B respectively. Moreover, these three ports are geared to VLAN 1.

Combine dhcp-snooping to use

Enable DHCP Snooping, set port Eth0/0/1 as the trust port of DHCP Snooping to enable anti-arp spoofing.

Network diagram



Configuration steps
Enable DHCP Snooping
Switch(config)#dhcp-snooping
Set port Ethernet 0/0/1 as the trust port of DHCP Snooping
Switch(config-if-ethernet-0/0/1)#dhcp-snooping trust
Config DHCP Snooping mode of port successfully.

Ip-soure-guard binding table
Switch(config)#ip-source-guard bind ip 192.168.5.10 mac 40:16:9f:f2:75:a8 in
terface ethernet 0/0/3 vlan 1
Add ip-source-guard bind entry successfully.

Enable anti-arp spoofing function
Switch(config)#arp anti-spoofing
Switch(config)#arp anti-spoofing unknown discard
Switch(config)#interface ethernet 0/0/1
Switch(config-if-ethernet-0/0/1)#arp anti trust

Client A DHCP obtains ip to form the dhcp-snooping clients table.

```
Switch(config)#show dhcp-snooping clients
DHCP client information:
d - days, h - hours, m - minutes, s - seconds
IPAddress       mac               vlan  port     LeaseTime      ExceedTime
192.168.5.13    00:00:00:00:32:33 1     e0/0/2   10m0s          7m53s

Total entries: 1. Printed entries: 1.
```

Client A forwards arp quest message to dhcpserver, dhcpserver can be able to receive this arp quest message

Client B configure static ip=192.168.5.10 mac=40:16:9f:f2:75:a8， Client B forwards arp quest message to dhcpserver, dhcpserver can be able to receive this arp quest message

If client B enable anti-arp spoofing, source ip of arp message=Client A， the equipment will discard the message if it found this arp message is spoof message.

This instance estimates whether this arp message is spoof message or not according to dhcp-snooping clients table or ip-soure-guard bind table. In addition, ayer-3 equipment can be able to realize this function via static arp table. All of this shares the same principle, no more tautology here.