Content

CHAPTER 1 LAYER 3 MANAGEMENT CONFIGURATION.....1

1.1 LAYER 3 MANAGEMENT INTERFACE.....1

1.1.1 Introduction to Layer 3 Management Interface.....1
1.1.2 Layer 3 Interface Configuration Task List.....1

1.2 IP CONFIGURATION.....2

1.2.1 Introduction to IPv4, IPv6.....2
1.2.2 IP Configuration.....4
1.2.3 IPv6 Troubleshooting.....5

1.3 STATIC ROUTE.....6

1.3.1 Introduction to Static Route.....6
1.3.2 Introduction to Default Route.....6
1.3.3 Static Route Configuration Task List.....6
1.3.4 Static Route Configuration Examples.....7

1.4 ARP.....8

1.4.1 Introduction to ARP.....8
1.4.2 ARP Configuration Task List.....8
1.4.3 ARP Troubleshooting.....8

CHAPTER 2 ARP SCANNING PREVENTION FUNCTION CONFIGURATION.....1

2.1 INTRODUCTION TO ARP SCANNING PREVENTION FUNCTION.....1

2.2 ARP SCANNING PREVENTION CONFIGURATION TASK SEQUENCE.....1

2.3 ARP SCANNING PREVENTION TYPICAL EXAMPLES.....3

2.4 ARP SCANNING PREVENTION TROUBLESHOOTING HELP.....4

CHAPTER 3 PREVENT ARP SPOOFING CONFIGURATION.....1

3.1 OVERVIEW.....1

3.1.1 ARP (Address Resolution Protocol).....1
3.1.2 ARP Spoofing.....1
3.1.3 How to prevent void ARP Spoofing.....1

3.2 PREVENT ARP SPOOFING CONFIGURATION.....2

3.3 PREVENT ARP SPOOFING EXAMPLE.....3

CHAPTER 4 ARP GUARD CONFIGURATION.....1

4.1 INTRODUCTION TO ARP GUARD.....1

4.2 ARP GUARD CONFIGURATION TASK LIST.....2

CHAPTER 5 GRATUITOUS ARP CONFIGURATION.....1

5.1 INTRODUCTION TO GRATUITOUS ARP.....1

5.2 GRATUITOUS ARP CONFIGURATION TASK LIST.....1

5.3 GRATUITOUS ARP CONFIGURATION EXAMPLE.....2

5.4 GRATUITOUS ARP TROUBLESHOOTING.....2

CHAPTER 6 DYNAMIC ARP INSPECTION CONFIGURATION....1

6.1 INTRODUCTION TO DYNAMIC ARP INSPECTION CONFIGURATION.....1

6.2 DYNAMIC ARP INSPECTION CONFIGURATION TASK LIST.....1

6.3 DYNAMIC ARP INSPECTION CONFIGURATION EXAMPLE.....2

Chapter 1 Layer 3 Management Configuration

Switch only support Layer 2 forwarding, but can configure a Layer 3 management port for the communication of all kinds of management protocols based on IP protocol.

1.1 Layer 3 Management Interface

1.1.1 Introduction to Layer 3 Management Interface

Only one layer 3 management interface can be created on switch. The Layer 3 interface is not a physical interface but a virtual interface. Layer 3 interface is built on VLANs. The Layer 3 interface can contain one or more layer 2 ports which belong to the same VLAN, or contain no layer 2 ports. At least one of the Layer 2 ports contained in Layer 3 interface should be in UP state for Layer 3 interface in UP state, otherwise, Layer 3 interface will be in DOWN state. The switch can use the IP addresses set in the layer 3 management interface to communicate with the other devices via IP.

1.1.2 Layer 3 Interface Configuration Task List

Layer 3 Interface Configuration Task List:
1. Create Layer 3 management interface
2. Configure VLAN interface description

1. Create Layer 3 Management Interface

Command	Explanation
Global Mode	
interface vlan <*vlan-id*> **no interface vlan <*vlan-id*>**	Creates a management VLAN interface; the no command deletes the VLAN interface created in the switch.

2. Configure VLAN interface description

Command	Explanation
VLAN Interface Mode	
description <text> ***no* description**	Configure the description information of VLAN interface. The no command will cancel the description information of VLAN interface.

1.2 IP Configuration

1.2.1 Introduction to IPv4, IPv6

IPv4 is the current version of global universal Internet protocol. The practice has proved that IPv4 is simple, flexible, open, stable, strong and easy to implement while collaborating well with various protocols of upper and lower layers. Although IPv4 almost has not been changed since it was established in 1980's, it has kept growing to the current global scale with the promotion of Internet. However, as Internet infrastructure and Internet application services continue boosting, IPv4 has shown its deficiency when facing the present scale and complexity of Internet.

IPv6 refers to the sixth version of Internet protocol which is the next generation Internet protocol designed by IETF to replace the current Internet protocol version 4 (IPv4). IPv6 was specially developed to make up the shortages of IPv4 addresses so that Internet can develop further.

The most important problem IPv6 has solved is to add the amount of IP addresses. IPv4 addresses have nearly run out, whereas the amount of Internet users has been increasing in geometric series. With the greatly and continuously boosting of Internet services and application devices (Home and Small Office Network, IP phone and Wireless Service Information Terminal which make use of Internet,) which require IP addresses, the supply of IP addresses turns out to be more and more tense. People have been working on the problem of shortage of IPv4 addresses for a long time by introducing various technologies to prolong the lifespan of existing IPv4 infrastructure, including Network Address Translation(NAT for short), and Classless Inter-Domain Routing(CIDR for short), etc.

Although the combination of CIDR, NAT and private addressing has temporarily mitigated the problem of IPv4 address space shortage, NAT technology has disrupted the end-to-end model which is the original intention of IP design by making it necessary for router devices that serve as network intermediate nodes to maintain every connection status which increases network delay greatly and decreases network performance. Moreover, the translation of network data packet addresses baffles the end-to-end network security check, IPSec authentication header is such an example.

Therefore, in order to solve all kinds of problems existing in IPv4 comprehensively,

the next generation Internet Protocol IPv6 designed by IETF has become the only feasible solution at present.

First of all, the 128 bits addressing scheme of IPv6 Protocol can guarantee to provide enough globally unique IP addresses for global IP network nodes in the range of time and space. Moreover, besides increasing address space, IPv6 also enhanced many other essential designs of IPv4.

Hierarchical addressing scheme facilitates Route Aggregation, effectively reduces route table entries and enhances the efficiency and expansibility of routing and data packet processing.

The header design of IPv6 is more efficient compared with IPv4. It has less data fields and takes out header checksum, thus expedites the processing speed of basic IPv6 header. In IPv6 header, fragment field can be shown as an optional extended field, so that data packets fragmentation process won't be done in router forwarding process, and Path MTU Discovery Mechanism collaborates with data packet source which enhances the processing efficiency of router.

Address automatic configuration and plug-and-play is supported. Large amounts of hosts can find network routers easily by address automatic configuration function of IPv6 while obtaining a globally unique IPv6 address automatically as well which makes the devices using IPv6 Internet plug-and-play. Automatic address configuration function also makes the readdressing of existing network easier and more convenient, and it is more convenient for network operators to manage the transformation from one provider to another.

Support IPSec. IPSec is optional in IPv4, but required in IPv6 Protocol. IPv6 provides security extended header, which provides end-to-end security services such as access control, confidentiality and data integrity, consequently making the implement of encryption, validation and Virtual Private Network easier.

Enhance the support for Mobile IP and mobile calculating devices. The Mobile IP Protocol defined in IETF standard makes mobile devices movable without cutting the existing connection, which is a network function getting more and more important. Unlike IPv4, the mobility of IPv6 is from embedded automatic configuration to get transmission address (Care-Of-Address); therefore it doesn't need Foreign Agent. Furthermore, this kind of binding process enables Correspondent Node communicate with Mobile Node directly, thereby avoids the extra system cost caused by triangle routing choice required in IPv4.

Avoid the use of Network Address Translation. The purpose of the introduction of NAT mechanism is to share and reuse same address space among different network segments. This mechanism mitigates the problem of the shortage of IPv4 address temporally; meanwhile it adds the burden of address translation process for network device and application. Since the address space of IPv6 has increased greatly, address translation becomes unnecessary, thus the problems and system cost caused by NAT deployment are solved naturally.

Support extensively deployed Routing Protocol. IPv6 has kept and extended the supports for existing Internal Gateway Protocols (IGP for short), and Exterior Gateway Protocols (EGP for short). For example, IPv6 Routing Protocol such as RIPng, OSPFv3,

IS-ISv6 and MBGP4+, etc.

Multicast addresses increased and the support for multicast has enhanced. By dealing with IPv4 broadcast functions such as Router Discovery and Router Query, IPv6 multicast has completely replaced IPv4 broadcast in the sense of function. Multicast not only saves network bandwidth, but enhances network efficiency as well.

1.2.2 IP Configuration

Layer 3 interface can be configured as IPv4 interface, IPv6 interface.

1.2.2.1 IPv4 Address Configuration

IPv4 address configuration task list:
1. Configure the IPv4 address of three-layer interface

1．Configure the IPv4 address of three-layer interface

Command	Explanation
VLAN Interface Configuration Mode	
ip address *<ip-address>* *<mask>* [secondary] **no ip address [*<ip-address>* *<mask>*]**	Configure IP address of VLAN interface; the **no ip address [*<ip-address>* *<mask>*]** command cancels IP address of VLAN interface.

1.2.2.2 IPv6 Address Configuration

The configuration Task List of IPv6 is as follows:
1. IPv6 basic configuration
   (1) Configure interface IPv6 address
2. IPv6 Neighbor Discovery Configuration
   (1) Configure DAD neighbor solicitation message number
   (2) Configure send neighbor solicitation message interval
   (3) Configure static IPv6 neighbor entries
   (4) Delete all entries in IPv6 neighbor table

1. IPv6 Basic Configuration

(1) Configure interface IPv6 address

Command	Explanation
Interface Configuration Mode	

ipv6 address <*ipv6-address*/*prefix-length*> [eui-64] **no ipv6 address <*ipv6-address/prefix-length*>**	Configure IPv6 address, including aggregatable global unicast addresses, site-local addresses and link-local addresses. The **no ipv6 address <*ipv6-address/prefix-length*>** command cancels IPv6 address.

2. IPv6 Neighbor Discovery Configuration

(1) Configure DAD Neighbor solicitation Message number

Command	Explanation
Interface Configuration Mode	
ipv6 nd dad attempts <value> **no ipv6 nd dad attempts**	Set the neighbor query message number sent in sequence when the interface makes duplicate address detection. The no command resumes default value (1).

(2) Configure Send Neighbor solicitation Message Interval

Command	Explanation
Interface Configuration Mode	
ipv6 nd ns-interval <*seconds*> **no ipv6 nd ns-interval**	Set the interval of the interface to send neighbor query message. The NO command resumes default value (1 second).

(3) Configure static IPv6 neighbor Entries

Command	Explanation
Interface Configuration Mode	
ipv6 neighbor <ipv6-address> <*hardware-address*> interface <*interface-type interface-name*>	Set static neighbor table entries, including neighbor IPv6 address, MAC address and two-layer port.
no ipv6 neighbor <*ipv6-address*>	Delete neighbor table entries.

(4) Delete all entries in IPv6 neighbor table

Command	Explanation
Admin Mode	
clear ipv6 neighbors	Clear all static neighbor table entries.

1.2.3 IPv6 Troubleshooting

- If the connected PC has not obtained IPv6 address, you should check the RA announcement switch (the default is turned off)

1.3 Static Route

1.3.1 Introduction to Static Route

As mentioned earlier, the static route is the manually specified path to a network or a host. Static route is simple and consistent, and can prevent illegal route modification, and is convenient for load balance and route backup. However, it also has its own defects. Static route, as its name indicates, is static, it won't modify the route automatically on network failure, and manual configuration is required on such occasions, therefore it is not suitable for mid and large-scale networks.

Static route is mainly used in the following two conditions: 1) in stable networks to reduce load of route selection and routing data streams. For example, static route can be used in route to STUB network. 2) For route backup, configure static route in the backup line, with a lower priority than the main line.

Static route and dynamic route can coexist; layer3 switch will choose the route with the highest priority according to the priority of routing protocols. At the same time, static route can be introduced (redistribute) in dynamic route, and change the priority of the static route introduced as required.

1.3.2 Introduction to Default Route

Default route is a kind of static route, which is used only when no matching route is found. In the route table, default route in is indicated by a destination address of 0.0.0.0 and a network mask of 0.0.0.0, too. If the route table does not have the destination of a packet and has no default route configured, the packet will be discarded, and an ICMP packet will be sent to the source address indicate the destination address or network is unreachable.

1.3.3 Static Route Configuration Task List

1. Static route configuration

1. Static route configuration

Command	Explanation
Global mode	
ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>*/*<prefix-length>*} {*<gateway-address>* | *<gateway-interface>*} [*<distance>*] **no ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>*/*<prefix-length>*} [*<gateway-address>* | *<gateway-interface>*] [*<distance>*]**	Set static routing; the **no ip route {*<ip-prefix>* *<mask>* | *<ip-prefix>*/*<prefix-length>*} [*<gateway-address>* | *<gateway-interface>*] [*<distance>*]** command deletes a static route entry

1.3.4 Static Route Configuration Examples

The figure shown below is a simple network consisting of three layer3 switches, the network mask for all switches and PC is 255.255.255.0. PC-A and PC-C are connected via the static route set in SwtichA and SwitchC; PC3 and PC-B are connected via the static route set in SwtichC to SwitchB; PC-B and PC-C is connected via the default route set in SwitchB.

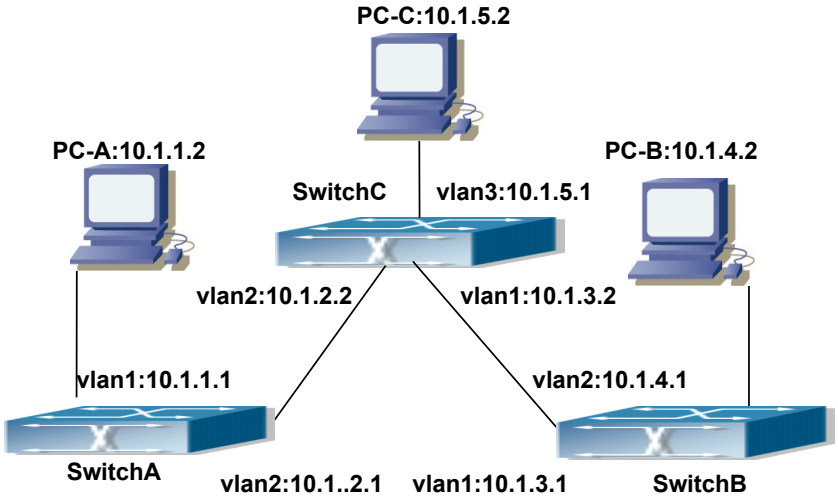


Fig 1-1 Static Route Configurations

Configuration steps:

Configuration of layer3 SwitchA

Switch#config

Switch (config) #ip route 10.1.5.0 255.255.255.0 10.1.2.2

Configuration of layer3 SwitchC

Switch#config

Next hop use the partner IP address

Switch(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.1

Next hop use the partner IP address

Switch(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.1

Configuration of layer3 SwitchB

Switch#config

Switch(config)#ip route 0.0.0.0 0.0.0.0 10.1.3.2

In this way, ping connectivity can be established between PC-A and PC-C, and PC-B and PC-C.

1.4 ARP

1.4.1 Introduction to ARP

ARP (Address Resolution Protocol) is mainly used to resolve IP address to Ethernet MAC address. Switch supports static ARP configuration.

1.4.2 ARP Configuration Task List

ARP Configuration Task List:
1. Configure static ARP

1. Configure static ARP

Command	Explanation
Interface Configuration Mode	
arp <*ip_address*> <*mac_address*> **no arp <ip_address>**	Configures a static ARP entry; the no command deletes a static ARP entry.

1.4.3 ARP Troubleshooting

If ping from the switch to directly connected network devices fails, the following can be used to check the possible cause and create a solution.

- ☞ Check whether the corresponding ARP has been learned by the switch.
- ☞ If ARP has not been learned, then enabled ARP debugging information and view the sending/receiving condition of ARP packets.
- ☞ Defective cable is a common cause of ARP problems and may disable ARP learning.

Chapter 2 ARP Scanning Prevention Function Configuration

2.1 Introduction to ARP Scanning Prevention Function

ARP scanning is a common method of network attack. In order to detect all the active hosts in a network segment, the attack source will broadcast lots of ARP messages in the segment, which will take up a large part of the bandwidth of the network. It might even do large-traffic-attack in the network via fake ARP messages to collapse of the network by exhausting the bandwidth. Usually ARP scanning is just a preface of other more dangerous attack methods, such as automatic virus infection or the ensuing port scanning, vulnerability scanning aiming at stealing information, distorted message attack, and DOS attack, etc.

Since ARP scanning threatens the security and stability of the network with great danger, so it is very significant to prevent it. Switch provides a complete resolution to prevent ARP scanning: if there is any host or port with ARP scanning features is found in the segment, the switch will cut off the attack source to ensure the security of the network.

There are two methods to prevent ARP scanning: port-based and IP-based. The port-based ARP scanning will count the number to ARP messages received from a port in a certain time range, if the number is larger than a preset threshold, this port will be “down”. The IP-based ARP scanning will count the number to ARP messages received from an IP in the segment in a certain time range, if the number is larger than a preset threshold, any traffic from this IP will be blocked, while the port related with this IP will not be “down”. These two methods can be enabled simultaneously. After a port or an IP is disabled, users can recover its state via automatic recovery function.

To improve the effect of the switch, users can configure trusted ports and IP, the ARP messages from which will not be checked by the switch. Thus the load of the switch can be effectively decreased.

2.2 ARP Scanning Prevention Configuration Task Sequence

1．Enable the ARP Scanning Prevention function.
2．Configure the threshold of the port-based and IP-based ARP Scanning Prevention
3．Configure trusted ports
4．Configure trusted IP

5．Configure automatic recovery time

6．Display relative information of debug information and ARP scanning

1. Enable the ARP Scanning Prevention function.

Command	Explanation
Global configuration mode	
anti-arpscan enable **no anti-arpscan enable**	Enable or disable the ARP Scanning Prevention function globally.

2. Configure the threshold of the port-based and IP-based ARP Scanning Prevention

Command	Explanation
Global configuration mode	
anti-arpscan port-based threshold <*threshold-value*> **no anti-arpscan port-based threshold**	Set the threshold of the port-based ARP Scanning Prevention.
anti-arpscan ip-based threshold <*threshold-value*> **no anti-arpscan ip-based threshold**	Set the threshold of the IP-based ARP Scanning Prevention.

3. Configure trusted ports

Command	Explanation
Port configuration mode	
anti-arpscan trust <*port* | *supertrust-port*> **no anti-arpscan trust <*port* | *supertrust-port*>**	Set the trust attributes of the ports.

4. Configure trusted IP

Command	Explanation
Global configuration mode	
anti-arpscan trust ip <*ip-address*> [<*netmask*>] **no anti-arpscan trust ip <*ip-address*> [<*netmask*>]**	Set the trust attributes of IP.

5. Configure automatic recovery time

Command	Explanation
Global configuration mode	
anti-arpscan recovery enable **no anti-arpscan recovery enable**	Enable or disable the automatic recovery function.

anti-arpscan recovery time *<seconds>* **no anti-arpscan recovery time**	Set automatic recovery time.

6. Display relative information of debug information and ARP scanning

Command	Explanation
Global configuration mode	
anti-arpscan log enable **no anti-arpscan log enable**	Enable or disable the log function of ARP scanning prevention.
anti-arpscan trap enable **no anti-arpscan trap enable**	Enable or disable the SNMP Trap function of ARP scanning prevention.
show anti-arpscan [trust *<ip | port | supertrust-port>* | prohibited *<ip | port>*]	Display the state of operation and configuration of ARP scanning prevention.
Admin Mode	
debug anti-arpscan *<port | ip>* **no debug anti-arpscan *<port | ip>***	Enable or disable the debug switch of ARP scanning prevention.

2.3 ARP Scanning Prevention Typical Examples

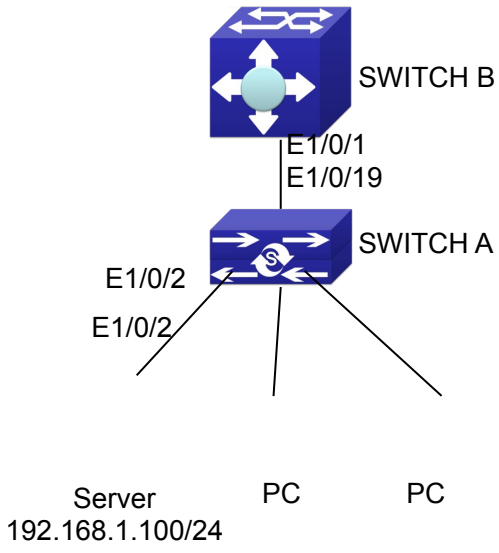


Fig 2-1 ARP scanning prevention typical configuration example

In the network topology above, port E1/0/1 of SWITCH B is connected to port E1/0/19 of SWITCH A, the port E1/0/2 of SWITCH A is connected to file server (IP address is 192.168.1.100/24), and all the other ports of SWITCH A are connected to common PC. The following configuration can prevent ARP scanning effectively without affecting the normal operation of the system.

SWITCH A configuration task sequence:

SwitchA(config)#anti-arpscan enable

SwitchA(config)#anti-arpscan recovery time 3600
SwitchA(config)#anti-arpscan trust ip 192.168.1.100 255.255.255.0
SwitchA(config)#interface ethernet1/0/2
SwitchA (Config-If-Ethernet1/0/2)#anti-arpscan trust port
SwitchA (Config-If-Ethernet1/0/2)#exit
SwitchA(config)#interface ethernet1/0/19
SwitchA (Config-If-Ethernet1/0/19)#anti-arpscan trust supertrust-port
Switch A(Config-If-Ethernet1/0/19)#exit

SWITCHB configuration task sequence:
Switch B(config)# anti-arpscan enable
SwitchB(config)#interface ethernet1/0/1
SwitchB(Config-If-Ethernet1/0/1)#anti-arpscan trust port
SwitchB(Config-If-Ethernet1/0/1)exit

2.4 ARP Scanning Prevention Troubleshooting Help

☞ ARP scanning prevention is disabled by default. After enabling ARP scanning prevention, users can enable the debug switch, "**debug anti-arpscan**", to view debug information.

Chapter 3 Prevent ARP Spoofing Configuration

3.1 Overview

3.1.1 ARP (Address Resolution Protocol)

Generally speaking, ARP (RFC-826) protocol is mainly responsible of mapping IP address to relevant 48-bit physical address, that is MAC address, for instance, IP address is 192.168.0.1, network card Mac address is 00-03-0F-FD-1D-2B. What the whole mapping process is that a host computer send broadcast data packet involving IP address information of destination host computer, ARP request, and then the destination host computer send a data packet involving its IP address and Mac address to the host, so two host computers can exchange data by MAC address.

3.1.2 ARP Spoofing

In terms of ARP Protocol design, to reduce redundant ARP data communication on networks, even though a host computer receives an ARP reply which is not requested by itself, it will also insert an entry to its ARP cache table, so it creates a possibility of “ARP spoofing”. If the hacker wants to snoop the communication between two host computers in the same network (even if are connected by the switches), it sends an ARP reply packet to two hosts separately, and make them misunderstand MAC address of the other side as the hacker host MAC address. In this way, the direct communication is actually communicated indirectly among the hacker host computer. The hackers not only obtain communication information they need, but also only need to modify some information in data packet and forward successfully. In this sniff way, the hacker host computer doesn’t need to configure intermix mode of network card, that is because the data packet between two communication sides are sent to hacker host computer on physical layer, which works as a relay.

3.1.3 How to prevent void ARP Spoofing

There are many sniff, monitor and attack behaviors based on ARP protocol in networks, and most of attack behaviors are based on ARP spoofing, so it is very important to prevent ARP spoofing. ARP spoofing accesses normal network environment by counterfeiting legal IP address firstly, and sends a great deal of counterfeited ARP application packets to switches, after switches learn these packets, they will cover previously corrected IP, mapping of MAC address, and then some corrected IP, MAC

address mapping are modified to correspondence relationship configured by attack packets so that the switch makes mistake on transfer packets, and takes an effect on the whole network. Or the switches are made used of by vicious attackers, and they intercept and capture packets transferred by switches or attack other switches, host computers or network equipment.

What the essential method on preventing attack and spoofing switches based on ARP in networks is to disable switch automatic update function; the cheater can't modify corrected MAC address in order to avoid wrong packets transfer and can't obtain other information. At one time, it doesn't interrupt the automatic learning function of ARP. Thus it prevents ARP spoofing and attack to a great extent.

3.2 Prevent ARP Spoofing configuration

The steps of preventing ARP spoofing configuration as below:

1. Disable ARP automatic update function
2. Disable ARP automatic learning function
3. Changing dynamic ARP to static ARP

1. Disable ARP automatic update function

Command	Explanation
Global Mode and Port Mode	
ip arp-security updateprotect **no ip arp-security updateprotect**	Disable and enable ARP automatic update function.

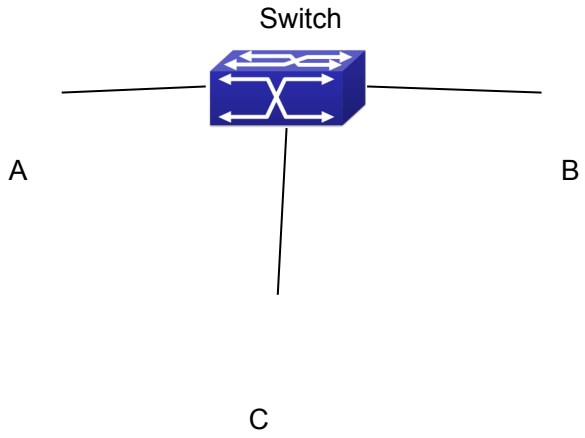
2. Disable ARP automatic learning function

Command	Explanation
Global mode and Interface Mode	
ip arp-security learnprotect **no ip arp-security learnprotect**	Disable and enable ARP automatic learning function.

3. Function on changing dynamic ARP to static ARP

Command	Explanation
Global Mode and Port Mode	
ip arp-security convert	Change dynamic ARP to static ARP.

3.3 Prevent ARP Spoofing Example



Equipment Explanation

Equipment	Configuration	Quality
switch	IP:192.168.2.4; mac: 00-00-00-00-00-04	1
A	IP:192.168.2.1; mac: 00-00-00-00-00-01	1
B	IP:192.168.1.2; mac: 00-00-00-00-00-02	1
C	IP:192.168.2.3; mac: 00-00-00-00-00-03	some

There is a normal communication between B and C on above diagram. A wants switch to forward packets sent by B to itself, so need switch sends the packets transfer from B to A. firstly A sends ARP reply packet to switch, format is: 192.168.2.3, 00-00-00-00-00-01, mapping its MAC address to C's IP, so the switch changes IP address when it updates ARP list., then data packet of 192.168.2.3 is transferred to 00-00-00-00-00-01 address (A MAC address).

In further, a transfers its received packets to C by modifying source address and destination address, the mutual communicated data between B and C are received by A unconsciously. Because the ARP list is update timely, another task for A is to continuously send ARP reply packet, and refreshes switch ARP list.

So it is very important to protect ARP list, configure to forbid ARP learning command in stable environment, and then change all dynamic ARP to static ARP, the learned ARP will not be refreshed, and protect for users.

```
Switch#config
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#arp 192.168.2.1 00-00-00-00-00-01 interface ethernet 1/0/1
Switch(config-if-vlan1)#arp 192.168.2.2 00-00-00-00-00-02 interface ethernet 1/0/2
Switch(config-if-vlan1)#arp 192.168.2.3 00-00-00-00-00-03 interface ethernet 1/0/3
Switch(Config-If-Vlan3)#exit
Switch(Config)#ip arp-security learnprotect
Switch(Config)#
```

Switch(config)#ip arp-security convert

If the environment changing, it enable to forbid ARP refresh, once it learns ARP property, it wont be refreshed by new ARP reply packet, and protect use data from sniffing.

Switch#config

Switch(config)#ip arp-security updateprotect

Chapter 4 ARP GUARD Configuration

4.1 Introduction to ARP GUARD

There is serious security vulnerability in the design of ARP protocol, which is any network device, can send ARP messages to advertise the mapping relationship between IP address and MAC address. This provides a chance for ARP cheating. Attackers can send ARP REQUEST messages or ARP REPLY messages to advertise a wrong mapping relationship between IP address and MAC address, causing problems in network communication. The danger of ARP cheating has two forms: 1. PC4 sends an ARP message to advertise that the IP address of PC2 is mapped to the MAC address of PC4, which will cause all the IP messages to PC2 will be sent to PC4, thus PC4 will be able to monitor and capture the messages to PC2; 2. PC4 sends ARP messages to advertise that the IP address of PC2 is mapped to an illegal MAC address, which will prevent PC2 from receiving the messages to it. Particularly, if the attacker pretends to be the gateway and do ARP cheating, the whole network will be collapsed.

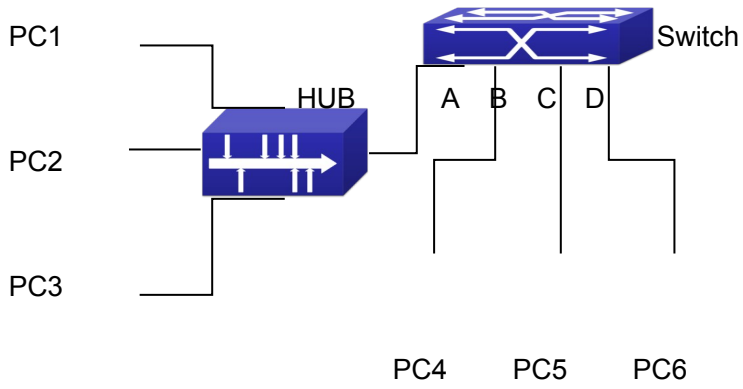


Fig 4-1 ARP GUARD schematic diagram

We utilize the filtering entries of the switch to protect the ARP entries of important network devices from being imitated by other devices. The basic theory of doing this is that utilizing the filtering entries of the switch to check all the ARP messages entering through the port, if the source address of the ARP message is protected, the messages will be directly dropped and will not be forwarded.

ARP GUARD function is usually used to protect the gateway from being attacked. If all the accessed PCs in the network should be protected from ARP cheating, then a large number of ARP GUARD address should be configured on the port, which will take up a big part of FFP entries in the chip, and as a result, might affect other applications. So this will be improper. It is recommended that adopting FREE RESOURCE related accessing scheme. Please refer to relative documents for details.

4.2 ARP GUARD Configuration Task List

1. Configure the protected IP address

Command	Explanation
Port configuration mode	
arp-guard ip <addr> **no arp-guard ip <addr>**	Configure/delete ARP GUARD address

Chapter 5 Gratuitous ARP Configuration

5.1 Introduction to Gratuitous ARP

Gratuitous ARP is a kind of ARP request that is sent by the host with its IP address as the destination of the ARP request.

The basic working mode for the switch is as below: The Layer 3 interfaces of the switch can be configured to advertise gratuitous ARP packets period or the switch can be configured to enable to send gratuitous ARP packets in all the interfaces globally.

The purpose of gratuitous ARP is as below:

1. To reduce the frequency that the host sends ARP request to the switch. The hosts in the network will periodically send ARP requests to the gateway to update the MAC address of the gateway. If the switch advertises gratuitous ARP requests, the host will not have to send these requests. This will reduce the frequency the hosts' sending ARP requests for the gateway's MAC address.
2. Gratuitous ARP is a method to prevent ARP cheating. The switch's advertising gratuitous ARP request will force the hosts to update its ARP table cache. Thus, forged ARP of gateway cannot function.

5.2 Gratuitous ARP Configuration Task List

1．Enable gratuitous ARP and configure the interval to send gratuitous ARP request

2．Display configurations about gratuitous ARP

1. Enable gratuitous ARP and configure the interval to send gratuitous ARP request.

Command	Explanation
Global Configuration Mode and Interface Configuration Mode.	
ip gratuitous-arp <*5-1200*> **no ip gratuitous-arp**	To enable gratuitous ARP and configure the interval to send gratuitous ARP request. The no command cancels the gratuitous ARP.

2. Display configurations about gratuitous ARP

Command	Explanation
Admin Mode and Configuration Mode	

show ip gratuitous-arp [interface vlan *<1-4094>*]	To display configurations about gratuitous ARP.

5.3 Gratuitous ARP Configuration Example

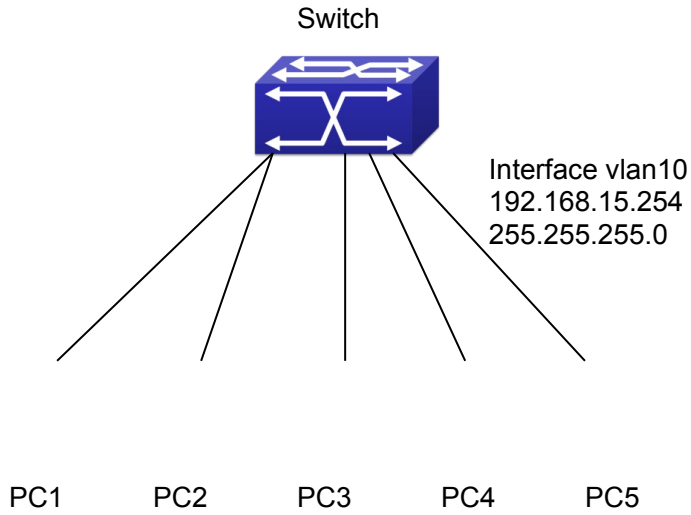


Fig 5-1 Gratuitous ARP Configuration Example

For the network topology shown in the figure above, interface VLAN10 whose IP address is 192.168.15.254 and network address mask is 255.255.255.0 in the switch system. Five PCs – PC1, PC2, PC3, PC4, PC5 are connected to the interface. Gratuitous ARP can be enabled through the following configuration:

1. Configure global gratuitous ARP

```
Switch(config)#ip gratuitous-arp 300
Switch(config)#exit
```

2. Configure interface gratuitous ARP

```
Switch(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip gratuitous-arp 300
Switch(Config-if-Vlan10)#exit
Switch(config) #exit
```

5.4 Gratuitous ARP Troubleshooting

Gratuitous ARP is disabled by default. And when gratuitous ARP is enabled, the debugging information about ARP packets can be retrieved through the command debug ARP send.

If gratuitous ARP is enabled in global configuration mode, it can be disabled only in global configuration mode. If gratuitous ARP is configured in interface configuration

mode, the configuration can only be disabled in interface configuration mode. If gratuitous ARP is enabled in both global and interface configuration mode, and the sending interval of gratuitous ARP is configured in both configuration modes, the switch takes the value which is configured in interface configuration mode.

Chapter 6 Dynamic ARP Inspection Configuration

6.1 Introduction to Dynamic ARP Inspection Configuration

DAI (Dynamic ARP Inspection) is a kind of security property that it can verificate the ARP data packets in the network. Through DAI, the administrator can intercept, record and drop the ARP data packets which have the invalid MAC address/IP address.

The dynamic ARP inspection judges the legality of the ARP data packets according to the lawful IP and MAC addresses in a trusted database. This database can be created by the manual static appointing or the dynamic DHCP monitoring learning. If the ARP data packet is received from the trusted port, the switch will not inspect it and forward it directly. If the ARP data packet is received from the untrusted port, the switch will only forward the lawful data packet. For the illegal data, it will drop the data directly and record this action.

Notice: The trusted/untrusted port above is not the one of DHCP monitoring, it is the rules that the dynamic ARP inspection function needs to configure.

6.2 Dynamic ARP Inspection Configuration Task List

1. Enable the dynamic ARP inspection based on vlan

Command	Explanation
Global Mode	
ip arp inspection vlan <vlan-id> **no ip arp inspection vlan <vlan-id>**	Enable the dynamic ARP inspection function based on vlan. The no command disables it.

2. Configure the trusted port

Command	Explanation
Port Mode	
ip arp inspection trust **no ip arp inspection trust**	Configure the port as the trusted port of the dynamic ARP inspection. The no command

	configures the untrusted port.

3. Configure the rate for the untrusted ARP packet

Command	Explanation
Port Mode	
ip arp inspection limit-rate <rate> **no ip arp inspection limit-rate <rate>**	Limit the ARP packet rate of the untrusted port. The no command cancels the limited cpu rate.

6.3 Dynamic ARP Inspection Configuration Example

Environment: DHCP server and PC client are both en vlan 10.

The MAC of the DHCP server is 00-24-8c-01-05-90, the IP address of 192.168.10.2 needs to be distributed statically, the DHCP server is connected to e 1/0/1. The MAC of the specific server (Other Server) is 00-24-8c-01-05-80, the IP address of 192.168.10.3 needs to be distributed statically, the other server is connected to e 1/0/2. The MAC of the PC client is 00-24-8c-01-05-96, the IP address is gotten dynamically through the DHCP. The PC is connected to e 1/0/3. The layer3 interface of vlan 10 is 192.168.10.1, the MAC is 00-03-0F-01-02-03.

The configuration is as below:

```
ip arp inspection vlan 10
ip dhcp snooping enable
ip dhcp snooping vlan 10
!
Interface Ethernet1/0/1
 description connect DHCP Server
 switchport access vlan 10
 ip dhcp snooping trust
 ip arp inspection limit-rate 50
!
Interface Ethernet1/0/2
```

```
 description connect to Other Server
 switchport access vlan 10
 ip arp inspection limit-rate 50
!
Interface Ethernet1/0/3
 description connect to PC
 switchport access vlan 10
 ip arp inspection limit-rate 50
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
```

Explanation: In this case, there are two method of static and dynamic using of DAI. The ARP packets from the untrusted port will all be transmitted to DHCP monitoring binding table for checking if they are lawful.

After the client gotten the IP address dynamically, it can be modified to be the static IP address, but it must be the same IP address to the dynamic one. If modifies to be other IP address, it cannot be accessed in the network and the switch can send the warning about the illegal ARP.