FSOS

ARP Configuration

Contents

1. ARP Configuration

1.1 ARP Overview

1.1.1 ARP Function

Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address.

An IP address is the address of a host at the network layer. To send a network layer packet to a destination host, the device must know the data link layer address (such as the MAC address) of the destination host. To this end, the IP address must be resolved into the corresponding data link layer address.

Unless otherwise stated, the data link layer addresses that appear in this chapter refer to the 48-bit Ethernet MAC addresses.

ARP Address Resolution Process as below:

Suppose that Host A and Host B are on the same subnet and that Host A sends a message to Host B, as show in Figure 1-2. The resolution process is as follows:

1. Host A looks in its ARP mapping table to see whether there is an ARP entry for Host B. If Host A finds it, Host A uses the MAC address in the entry to encapsulate the IP packet into a data link layer frame and sends the frame to Host B.
2. If Host A finds no entry for Host B, Host A buffers the packet and broadcasts an ARP request, in which the source IP address and source MAC address are respectively the IP address and MAC address of Host A and the destination IP address and MAC address are respectively the IP address of Host B and an all-zero MAC address. Because the ARP request is sent in broadcast mode, all hosts on this subnet can receive the request, but only the requested host (namely, Host B) will process the request.
3. Host B compares its own IP address with the destination IP address in the ARP request. If they are the same, Host B saves the source IP address and source MAC address into its ARP mapping table, encapsulates its MAC address into an ARP reply, and unicasts the reply to Host A.
4. After receiving the ARP reply, Host A adds the MAC address of Host B into its ARP mapping table for subsequent packet forwarding. Meanwhile, Host A encapsulates the IP packet and sends it out.

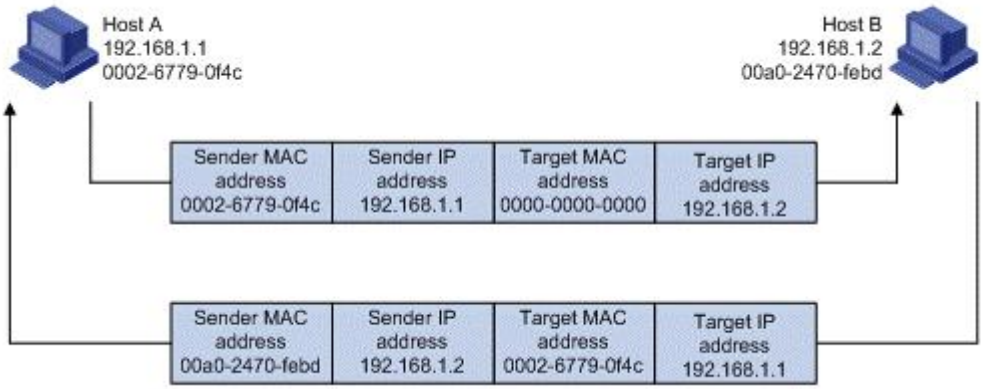

Figure 1-1 ARP address resolution process

When Host A and Host B are not on the same subnet, Host A first sends an ARP request to the gateway. The destination IP address in the ARP request is the IP address of the gateway. After obtaining the MAC address of the gateway from an ARP reply, Host A encapsulates the packet and sends it to the gateway. Subsequently, the gateway broadcasts the ARP request, in which the destination IP address is the one of Host B. After obtaining the MAC address of Host B from another ARP reply, the gateway sends the packet to Host B.

1.1.2 ARP Message Format

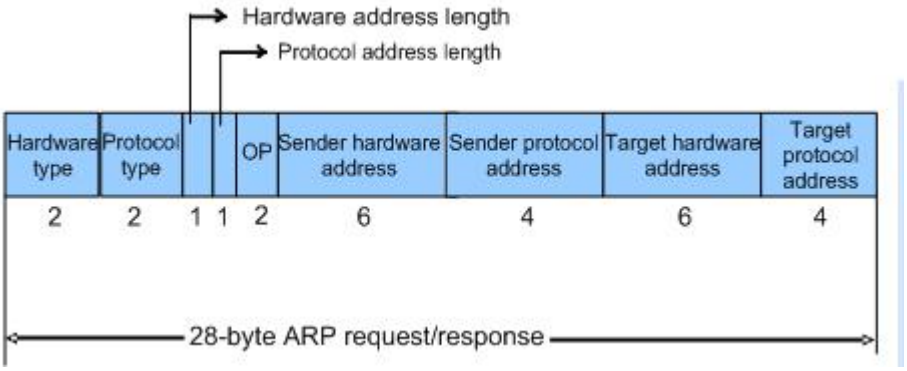

Figure 1-1 ARP Message Format

The following explains the fields in Figure 1-1.

Hardware type: This field specifies the hardware address type. The value “1” represents Ethernet.

Protocol type: This field specifies the type of the protocol address to be mapped. The hexadecimal value “0x0800” represents IP.

Hardware address length and protocol address length: They respectively specify the length of a hardware address and a protocol address, in bytes. For an Ethernet address, the value of the hardware address length field is "6”. For an IP(v4) address, the value of the protocol address length field is “4”.

OP: Operation code. This field specifies the type of ARP message. The value "1" represents an ARP request and "2" represents an ARP reply.

Sender hardware address: This field specifies the hardware address of the device sending the message.

Sender protocol address: This field specifies the protocol address of the device sending the message.

Target hardware address: This field specifies the hardware address of the device the message is being sent to.

Target protocol address: This field specifies the protocol address of the device the message is being sent to.

1.2 Configuring ARP Attack Spoofing

1.2.1 Brief Introduction to ARP Spoofing

ARP provides no security mechanism and thus is prone to network attacks. An attacker can construct and send ARP packets, thus threatening network security.

A forged ARP packet has the following characteristics:

- The sender MAC address or target MAC address in the ARP message is inconsistent with the source MAC or destination MAC address in the Ethernet frame.
- The mapping between the sender IP address and the sender MAC address in the forged ARP message is not the true IP-to-MAC address binding of a valid client.

ARP attacks bring many malicious effects. Network communications become unstable, users cannot access the Internet, and serious industrial accidents may even occur. ARP attacks may also intercept accounts and passwords of services such as games, network banks, and file services.

1.2.2 ARP Anti-Spoofing Protection

ARP spoofing attacks to protection, the key is to identify and prohibit forwarding spoofed ARP packets. From the principle of ARP spoofing, we can see, to prevent ARP spoofing attack requires two ways, first to prevent the virus disguised as the gateway host, it will cause the entire segment of the user can not access; followed by preventing the virus from the host masquerade as another host, eavesdropping data or cause the same network segment can't communicate between the individual host.

This series switches provide active defense ARP spoofing function, in practical applications, the network hosts the first communication, the switch will record the ARP table entries, entries in the message of the sender IP, MAC, VID and port correspondence.

To prevent the above mentioned ARP attacks, Switch launch a comprehensive ARP attack protection solution.

An access switch is a critical point to prevent ARP attacks, as ARP attacks generally arise from the host side. To prevent ARP attacks, the access switches must be able to

- Establish correct ARP entries, detect and filter out forged ARP packets, and ensure the validity of ARP packets it forwards
- Suppress the burst impact of ARP packets.

After configuring the access switches properly, you do not need to deploy ARP attack protection configuration on the gateway. This relieves the burden from the gateway.

If the access switches do not support ARP attack protection, or the hosts are connected to a gateway directly, the gateway must be configured to

- Create correct ARP entries and prevent them from being modified.
- Suppress the burst impact of ARP packets or the IP packets that will trigger sending of ARP requests.

The merits of configuring ARP attack protection on the gateway are that this gateway configuration hardly affects the switches and can properly support the existing network, thus effectively protecting user investment

1.2.3 Configuring Anti-Spoofing

Table 1-2 Configure anti-spoofing

Step	Command	Operation
step1	**configure terminal**	Enter global configuration mode
Step2	**arp anti-spoofing**	Enable ARP anti-spoofing
Step3	**arp anti-spoofing unknown** {*diacard* | *flood*}	Configure the method of unknown static ARP packet
Step4	**end**	return to privilege mode
Step5	**copy running-config startup-config**	save modified configuration

1.2.4 Configuring ARP Packet Source MAC Address Consistency Check

This feature enables a gateway device to filter out ARP packets with a source MAC address in the Ethernet header different from the sender MAC address in the message body, so that the gateway device can learn correct ARP entries.

By default, system disables gateway spoofing.

Table 1-4 Configure ARP Packet Source MAC Address Consistency Check

Step	Command	Operation
step1	**configure terminal**	Enter global configuration mode
step2	**arp anti-spoofing valid-check**	Configure **ARP Packet Source MAC Address Consistency Check**
step3	**show arp anti-spoofing**	validation operation
step4	**end**	return to privilege mode
step5	**copy running-config startup-config**	save modified configuration

1.2.5 Configuring Default of Anti-Spoofing

Table 1-5 Configure default of anti-spoofing

Function	Default
arp anti-spoofing	disable
Configure ARP Packet Source MAC Address Consistency Check	enable
arp anti-spoofing unknown {*diacard* | *flood***}**	discard

1.2.6 Displaying and Maintain Anti-spoofing

Table 1-6 Configure default of anti-spoofing

Command	Operation
show arp anti-spoofing	Display the status of anti-spoofing
show mac-address-table blackhole	Display users whether add into black hole

1.3 Configuring against ARP Flood

1.3.1 ARP Flood

Flood attacks are based on the principle of the general flow of a large number of attack packets in the network equipment such as routers, switches, and servers, leading to depletion of network equipment, leaving the CPU down the network.

Flood attacks are based on the principle of the general flow of a large number of attack packets in the network equipment such as routers, switches and servers, leading to depletion of network equipment, leaving the CPU down the network.

1.3.2 Configuring against ARP Flood

ARP flood attack is aimed mainly at the impact of network device's CPU, the core CPU resources leading to depletion. To defend this type of attack, the switch must determine in advance and to prohibit flood packet forwarding.

The ARP anti-flood function to identify each ARP traffic, according to the ARP rate setting security thresholds to determine whether the ARP flood attack, when a host's ARP traffic exceeds a set threshold, the switch will be considered a flood attack , immediately pulled into the black host of the virus, banned from the host and all packet forwarding.

In order to facilitate the management of the network administrator to maintain, while the automatic protection will be saved in the system log related to alarms. For disabled users, administrators can set automatic or manual recovery.

In the switch on the entire process is as follows:

1. Enable ARP anti-flood function will be broadcast ARP packets received on the CPU, according to an ARP packet source MAC address to identify the different streams.
2. Set security ARP rate, if the rate exceeds the threshold, the switch that is ARP attack.
3. If you select the above command deny-all, when an ARP traffic exceeds the threshold set, the switch will determine the source MAC address, the MAC address to the black hole list of addresses to ban this address to forward all subsequent messages.
4. If you select the above command deny-arp, ARP traffic when more than a set threshold, the switch will be judged based on the source MAC address, the address against all subsequent handling of ARP packets.
5. For recovery to be disabled in the user's forwarding, administrators can set up automatic or manual recovery recovery time in two ways.

1.3.3 Configuring against ARP Flood

Table 1-7 Configure against ARP flood

Command	Operation	Remark
Enter global configuration mode	**configure terminal**	-
Enable ARP flooding	**arp anti-flood**	required
Configure safety trigger threshold	**arp anti-flood threshold** *threshold*	optional
		By default, the safety trigger threshold 16PPS

Configure approach for the attacker	**arp anti-flood action** {**deny-arp**|**deny-all**} **threshold** *threshold*	optional By default, for the attacker's approach to deny ARP
Configure automatically banned user recovery time	**arp anti-flood recover-time** *time*	optional Configurable time range is <0-1440> minutes, set to 0, said to be manually restored. By default, the user automatically banned recovery time of 10 minutes.
Banned user manual resume forwarding..	**arp anti-flood recover** {*H:H:H:H:H:H* | *all*}	optional

1.3.4 Displaying and Maintain against ARP Flood

Operation	Command	Remark
Display ARP anti-flood configuration and attackers list	**show arp anti-flood**	Perform either of the commands