# Chapter 21: **ARP Spoofing and Flood**

# Table of Contents

# Chapter 21 ARP Spoofing and Flood

## 21.1 ARP Spoofing and Flood Attack Overview

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 withthe 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 mayalso intercept accounts and passwords of services such as games, network banks, and file services.

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.

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, the Switches launches a comprehensive ARPattack protection solution.

An access Switch is a critical point to prevent ARP attacks, as ARP attacks generally arisefrom 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 thevalidity of ARP packets it forwards
- Suppress the burst impact of ARP packets.

After Configure the access Switches properly, you do not need to deploy ARP attackprotection 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 agateway 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 Configure 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.

## 21.2.1 ARP Against ARP Flood

| Configuration Task | Description | Detailed Configuration |
|---|---|---|
| Configure Anti-Spoofing | Required | 21.2.2 |
| Configure ARP Packet Source MAC Address Consistency Check | Required | 21.2.3 |
| Configure Anti-Gateway-Spoofing | Required | 21.2.4 |

## 21.2.2 Configure Anti-spoofing

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **system-view** | |
| Enable ARP anti-spoofing | **arp anti-spoofing** | |
| Configure the method of unknown static ARP packet | **arp anti-spoofing unknown** { *discard* \| *flood* } | |

## 21.2.3 Configure ARP Packet Source MAC Address Consistency Check

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **system-view** | |
| Configure ARP Packet Source MAC Address Consistency Check | **arp anti-spoofing valid-check** | |
| validation operation | **display arp anti-spoofing** | |

## 21.2.4 Configure Anti-Gateway-spoofing

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **system-view** | |
| Enable arp anti-spoofing | **arp anti-spoofing** | |
| Enable anti-gateway-spoofing | **arp anti-spoofing deny-disguiser** | |
| Disable anti-gateway-spoofing | **undo arp anti-spoofing deny-disguiser** | |

# 21.3 Configure against ARP Flood

## 21.3.1 ARP against ARP Flood Configuration List

| Configuration Task | Description | Detailed Configuration |
|---|---|---|
| Configure against ARP Flood | Required | 21.3.2 |
| Display and Maintain against ARP Flood | Required | 21.3.3 |

## 21.3.2 Configure against ARP Flood

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **system-view** | |
| Enable ARP flooding | **arp anti-flood** | |
| Configure safety trigger threshold | **arp anti-flood threshold** *threshold* | |
| Configure approach for the attacker | **arp anti-flood action** { **deny-arp** \| **deny-all** } **threshold** *threshold* | |
| Configure automatically banned user recovery time | **arp anti-flood recover-time** *time* | |
| Banned user manual resume forwarding.. | **arp anti-flood recover** { *H:H:H:H:H:H* \| *all* } | |

## 21.3.3 Display and Maintain Against ARP Flood

| Operation | Command | Remarks |
|---|---|---|
| Display ARP anti-flood configuration and attackers list | **display arp anti-flood** | |