ARP Attack Protection

Technical Introduction

ARP Attack Protection

About ARP attack protection

An attacker can exploit ARP vulnerabilities to launch ARP flood attack, ARP user spoofing attack, and ARP gateway spoofing attack. The ARP attack protection feature can be used to detect and prevent ARP attacks to improve network security.

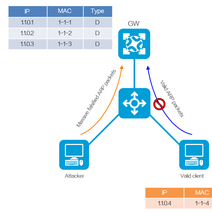
Preventing ARP flood attacks

Attack threats

An attacker sends a large number of unresolvable IP packets to have the receiving device busy resolving IP addresses until its CPU is overloaded.

An attacker sends a large number of ARP packets to exhaust ARP entry resources of the gateway, which causes the gateway fail to learn new valid ARP entries.

Prevention measures



- **ARP source suppression**

This feature allows the device to stop resolving packets from an IP address if the number of unresolvable IP packets from the IP address exceeds the upper limit within 5 seconds. The device continues ARP resolution when the interval elapses. This feature is applicable if the attack packets have the same source addresses.

- **ARP blackhole routing**

This feature enables the device to create a blackhole route destined for an unresolved IP address. The device drops all matching packets until the blackhole route is deleted. A blackhole route is deleted when its aging timer is reached or the route becomes reachable.

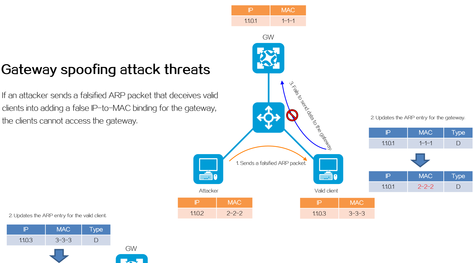
- **Source MAC-based ARP attack detection**

This feature enables the device to check the number of ARP packets delivered to the CPU. The device determines that an attack occurs if the number of packets from the same MAC address exceeds a threshold within 5 seconds. The device can generate log messages or filter out subsequent ARP packets from the MAC address.

- **ARP packet rate limit**

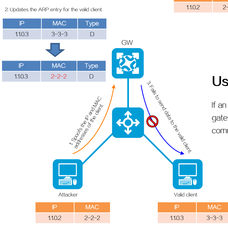
This feature limits the rate of ARP packets delivered to the CPU to avoid CPU overloading.

Preventing user/gateway spoofing attacks



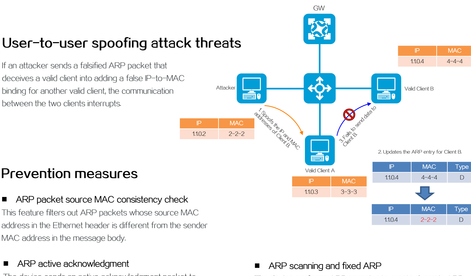
Gateway spoofing attack threats

If an attacker sends a falsified ARP packet that deceives valid clients into adding a false IP-to-MAC binding for the gateway, the clients cannot access the gateway.



User-to-gateway spoofing attack threats

If an attacker sends a falsified ARP packet that deceives the gateway into adding a false IP-to-MAC binding for a valid client, the communication between the gateway and the client interrupts.



User-to-user spoofing attack threats

If an attacker sends a falsified ARP packet that deceives a valid client into adding a false IP-to-MAC binding for another valid client, the communication between the two clients interrupts.

Prevention measures

- **ARP packet source MAC consistency check**

This feature filters out ARP packets whose source MAC address in the Ethernet header is different from the sender MAC address in the message body.

- **ARP active acknowledgment**

The device sends an active acknowledgment packet to the sender IP address of ARP packets before creating or updating ARP entries to prevent itself from leaning incorrect ARP entries.

- **Authorized ARP**

The device generates authorized ARP entries based on the DHCP clients' address leases on the DHCP server or DHCP relay entries on the DHCP relay agent.

- **ARP sender IP address checking**

The device determines that an ARP packet for a VLAN is an attack packet if the sender IP address is out of the allowed IP address range, and discards the packet.

- **ARP attack detection**

The device performs ARP user validity check and ARP packet validity check to filter out inlad ARP packets.

- **ARP scanning and fixed ARP**

The device performs ARP scanning to create dynamic ARP entries for devices in the LAN, and then converts the dynamic ARP entries into static ARP entries through fixed ARP. Typically, these features are used together on small-scaled and stable networks.

- **ARP safe-guard**

The device use this feature to prevent traffic-intensive ARP packet attacks as follows:

- Sends ARP replies to all incoming ARP requests but do not generate corresponding ARP entries.
- Generates ARP entries only for incoming ARP replies that the device requests.
- Drops incoming ARP replies that are not requested by the device.

- **ARP gateway protection**

Configure this feature on interfaces that are not connected with a gateway. The interfaces discards ARP packets of which the sender IP address is the same as the gateway IP address.

- **ARP filtering**

This feature allows only ARP packets of which the sender IP address and sender MAC address are the same as the IP and MAC addresses in a configured entry to pass through on an interface.

Deployment

Configure ARP attack protection features on different network nodes to prevent ARP attacks.

ARP attack protection feature		Deployed on
Prevent ARP flood attacks	ARP source suppression	Gateway
	ARP blackhole routing	Gateway
	Source MAC-based ARP attack detection	Gateway
	ARP packet rate limit	Gateway
Prevent user/gateway spoofing attacks	ARP packet source MAC consistency check	Gateway
	ARP active acknowledgment	Gateway
	Authorized ARP	Gateway
	ARP sender IP address checking	Gateway
	ARP scanning and fixed ARP	Gateway
	ARP safe-guard	Gateway
	ARP gateway protection	NAS
	ARP filtering	NAS
	ARP attack detection	NAS

New H3C Technologies Co., Ltd