Contents

Overview ................................................................................................................................................. 1

Technical background ................................................................................................................................. 1
  Operation of ARP ....................................................................................................................................... 1
  ARP attacks ............................................................................................................................................... 1
  Impacts of ARP attacks ............................................................................................................................. 4

Benefits ..................................................................................................................................................... 4

ARP attack protection implementation ................................................................. 5

  ARP attack protection implementation on the access device ................................................................. 5
  ARP attack detection ................................................................................................................................ 5
  ARP gateway protection ............................................................................................................................ 6
  ARP filtering ................................................................................................................................................ 7
  ARP packet rate limit ................................................................................................................................. 7

ARP attack protection implementation on the gateway .......................................................... 7

  Authorized ARP ......................................................................................................................................... 8
  ARP scanning and fixed ARP ..................................................................................................................... 8
  Static ARP entries ..................................................................................................................................... 8
  ARP active acknowledgement .................................................................................................................. 8
  ARP packet source MAC consistency check ............................................................................................. 9
  Source MAC-based ARP attack detection ............................................................................................... 9
  Dynamic ARP learning limit on an interface ............................................................................................ 10
  ARP defense against IP packet attacks ................................................................................................. 10

Application scenarios ......................................................................................................................... 11

  Monitoring mode ....................................................................................................................................... 11
  Authentication mode ................................................................................................................................. 11
  Cybercafe solution .................................................................................................................................. 12

References ................................................................................................................................................. 13
Overview

Technical background

Operation of ARP

The Address Resolution Protocol (ARP) is used to resolve an IP address into a physical address (Ethernet MAC address, for example).

ARP works as follows:
1. When a device needs to know the MAC address of another device that has a specific IP address on a subnet, it broadcasts an ARP request on the subnet.
2. Each device on the subnet examines the ARP request, and the device that has the specific IP address sends an ARP reply containing its MAC address and adds the sender MAC and IP addresses in the ARP request to its ARP table.
3. Upon receiving the ARP reply, the requesting device adds the sender MAC and IP addresses in the ARP reply to its ARP table.

ARP attacks

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 can be classified into gateway spoofing, user spoofing, and ARP flooding.

Gateway spoofing

As shown in Figure 1, the forged ARP packet sent from Host A deceives Host B into adding a false IP-to-MAC binding of the gateway. After that, normal communications between Host B and the gateway are interrupted.
Gateway spoofing is a frequently used ARP attack method. It can cause serious impacts. If an ARP packet with the forged gateway MAC address is broadcast to the LAN, all communications within the LAN may fail.

**User spoofing**

An attacker may send a forged ARP packet containing a false IP-to-MAC address binding to a gateway or a host.

As shown in Figure 2, the forged ARP packet sent from Host A deceives the gateway into adding a false IP-to-MAC address binding of Host B. After that, normal communications between the gateway and Host B are interrupted.
As shown in Figure 3, the forged ARP packet sent from Host A deceives Host C into adding a false IP-to-MAC address mapping of Host B. After that, normal communications between Host C and Host B are interrupted.

**Figure 3 User spoofing that deceives a host**
ARP flooding

Processing ARP packets consumes system resources. Generally, the size of an ARP table is restricted to guarantee sufficient system memory and searching efficiency. An attacker may send a large number of forged ARP packets with various sender IP addresses to cause an overflow of the ARP table on the victim. Then the victim cannot add valid ARP entries and thus fails to communicate.

An attacker may also send a large number of packets with unresolvable destination IP addresses. When the victim keeps trying to resolve the destination IP addresses to forward packets, its CPU will be exhausted.

Impacts of ARP attacks

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.

Benefits

To prevent the above mentioned ARP attacks, H3C launches a comprehensive ARP attack protection solution.

Figure 4 Device roles in an ARP attack protection solution

Figure 4 shows the device roles in an ARP attack protection solution. The device roles serve as the basis for analyzing possible ARP attacks that Layer 2 and Layer 3 network devices may encounter, and for providing effective attack protection methods. You can use the preceding configuration methods according to the actual network scenarios.

- **ARP attack protection on the access device**—An access device is configured to prevent ARP attacks, as ARP attacks generally arise from the host side. To prevent ARP attacks, the access switches must be able to provide the following functions:
  - 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.
With this configuration method, you do not need to deploy ARP attack protection configuration on the gateway. This relieves the burden from the gateway.

- **ARP attack protection on the gateway**—If the access devices do not support ARP attack protection, or the hosts are connected to a gateway directly, you must configure the gateway to prevent ARP attacks to provide the following functions:
  - 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.

This configuration method reduces the dependency on the access devices and properly supports the existing network, thus effectively protecting user investment.

## ARP attack protection implementation

### ARP attack protection implementation on the access device

An access device may encounter gateway spoofing, user spoofing, and ARP flooding. The following sections separately describe the features used to prevent these attacks.

#### Against gateway spoofing

Check the validity of ARP packets. ARP packets that pass the check are forwarded, whereas other ARP packets are discarded. The following protection features are used:

- ARP attack detection
- ARP filtering
- ARP gateway protection

#### Against user spoofing

Check the validity of ARP packets. ARP packets that pass the check are forwarded, whereas other ARP packets are discarded. The following protection features are used:

- ARP attack detection
- ARP gateway protection

#### Against ARP flooding

Use the ARP packet rate limit feature.

## ARP attack detection

ARP attack detection enables access devices to block ARP packets from unauthorized clients to prevent user spoofing and gateway spoofing attacks.

ARP attack detection provides the following features:

- ARP packet validity check.
- User validity check.
- ARP restricted forwarding.

If both ARP packet validity check and user validity check are enabled, the former one applies first, and then the latter applies.

With ARP attack detection enabled for a VLAN, this feature applies to ARP packets received by interfaces in the VLAN.
In a VXLAN network, you can configure a VTEP to perform ARP attack detection in a VSI. ARP attack detection performs user validity check and ARP packet validity check on ARP packets from ARP untrusted ACs.

**ARP packet validity check**

ARP packet validity check does not check ARP packets received by ARP trusted interfaces. To check ARP packets received on untrusted interfaces, you can specify the following objects to be checked:

- **Source MAC-based**—Checks whether the sender MAC address in the message body is identical to the source MAC address in the Ethernet header. If they are identical, the packet is forwarded. Otherwise, the packet is discarded.
- **Destination MAC-based**—Checks the target MAC address of ARP replies. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.
- **IP-based**—Checks the sender and target IP addresses of ARP replies, and the sender IP address of ARP requests. All-one or multicast IP addresses are considered invalid and the corresponding packets are discarded.

**User validity check**

User validity check does not check ARP packets received by ARP trusted interfaces. This feature compares the sender IP and sender MAC in the ARP packet received on an ARP untrusted interface with the matching criteria in the following order:

1. **User validity check rules.**
   - If a match is found, the device processes the ARP packet according to the rule.
   - If no match is found or no user validity check rule is configured, proceeds to step 2.
2. **Static IP source guard bindings, DHCP snooping entries, and 802.1X security entries.**
   - If a match is found, the device forwards the ARP packet.
   - If no match is found, the device discards the ARP packet.

Static IP source guard bindings are created by using the `ip source binding` command. DHCP snooping entries are automatically generated by DHCP snooping. 802.1X security entries record the IP-to-MAC mappings for 802.1X clients. After a client passes 802.1X authentication and uploads its IP address to an ARP attack detection enabled device, the device automatically generates an 802.1X security entry. The 802.1X client must be enabled to upload its IP address to the device.

**ARP restricted forwarding**

ARP restricted forwarding does not take effect on ARP packets received by ARP trusted interfaces. This feature controls the forwarding of ARP packets that are received by untrusted interfaces and have passed user validity check as follows:

- If the packets are ARP requests, they are forwarded through the trusted interface.
- If the packets are ARP replies, they are forwarded according to their destination MAC address. If no match is found in the MAC address table, they are forwarded through the trusted interface.

**ARP gateway protection**

Configure this feature on interfaces that are not connected with a gateway to prevent gateway spoofing attacks.

When such an interface receives an ARP packet, it checks whether the sender IP address in the packet is consistent with that of any protected gateway.

- If yes, it discards the packet.
- If not, it identifies the packet as legal and continues processing the packet.
ARP filtering

The ARP filtering feature can prevent gateway spoofing and user spoofing attacks. An interface enabled with this feature checks the sender IP and MAC addresses in a received ARP packet against permitted entries.

- If a match is found, it identifies the packet as legal and continues processing the packet.
- If not, the packet is discarded.

ARP packet rate limit

The ARP packet rate limit feature allows you to limit the rate of ARP packets delivered to the CPU. An ARP attack detection-enabled device will send all received ARP packets to the CPU for inspection. Processing excessive ARP packets will make the device malfunction or even crash. To solve this problem, configure ARP packet rate limit. When the receiving rate of ARP packets on the interface exceeds the rate limit, those packets are discarded.

You can enable sending notifications to the SNMP module or enable logging for ARP packet rate limit.

- If notification sending is enabled, the device sends the highest threshold-crossed ARP packet rate within the sending interval in a notification to the SNMP module. You must set the notification type and target host.
- If logging for ARP packet rate limit is enabled, the device sends the highest threshold-crossed ARP packet rate within the sending interval in a log message to the information center. You can configure the information center module to set the log output rules.

ARP attack protection implementation on the gateway

A gateway may encounter user spoofing and ARP flooding. Various features are introduced to prevent these attacks.

Against user spoofing

Establish correct ARP entries through a valid method and prevent the entries from being modified by attackers. The following protection features are used:

- Authorized ARP
- ARP scanning and fixed ARP
- Static ARP entries

Confirm the IP-to-MAC mapping before creating or modifying an ARP entry, so as to ensure that the correct and valid ARP entry is learned. The following protection features are used:

- ARP active acknowledgement
- ARP packet source MAC consistency check

Against ARP flooding

The following protection features are used:

- Source MAC-based ARP attack detection
- Restrict the maximum number of ARP entries that an interface can learn
- ARP defense against IP packet attacks
Authorized ARP

Authorized ARP entries are generated based on the DHCP clients’ address leases on the DHCP server or dynamic bindings on the DHCP relay agent. This feature is applicable to a network where hosts obtain their IP addresses through DHCP.

Static ARP entries can overwrite authorized ARP entries, whereas forged ARP packets cannot modify authorized ARP entries, that is, dynamic ARP entries cannot overwrite authorized ARP entries. This ensures correct ARP entries.

If an attacker sends a forged ARP request by using the IP address of a valid host to the gateway, the gateway with this feature enabled will not send any ARP reply because the MAC address of the attacker is not that in the corresponding authorized ARP entry on the gateway. This prevents the attacker from accessing the Internet by using a valid IP address.

After authorized ARP is enabled on an interface, the interface is disabled from learning dynamic ARP entries. This prevents attacks from unauthorized clients that send packets using other clients’ IP or MAC addresses, and allows only authorized clients to access network resources, thus enhancing network security. Meanwhile, the interface starts authorized ARP entry aging to detect offline anomalies and delete invalid authorized ARP entries in time.

ARP scanning and fixed ARP

ARP scanning is usually used together with the fixed ARP feature.

With ARP scanning enabled on an interface, the device automatically scans neighbors on the interface, sends ARP requests to the neighbors, obtains their MAC addresses, and creates dynamic ARP entries.

Fixed ARP allows the device to change the existing dynamic ARP entries (including those generated through ARP scanning) into static ARP entries. The fixed ARP feature can effectively prevent ARP entries from being modified by attackers.

You are recommended to use ARP scanning and fixed ARP in a small-scale network such as a cybercafe.

Static ARP entries

You can configure static ARP entries for critical network devices by using their IP-to-MAC mappings. Static ARP entries cannot be overwritten by forged or dynamic ARP packets, and can restrict invalid ARP requests, thus protecting the network devices from attacks.

Configuring static ARP entries is a heavy job. It is not applicable to networks where the host IP addresses are changed frequently. It is recommended that you configure static ARP entries for small-scale networks.

ARP active acknowledgement

Typically, the ARP active acknowledgement feature is configured on gateway devices to identify invalid ARP packets.

Without ARP active acknowledgement enabled, the gateway, upon receiving an ARP packet, searches existing ARP entries for the sender IP address of the ARP packet:

- If no match is found, the gateway creates an ARP entry with the sender IP and MAC addresses of the ARP packet.
- If a match is found, the gateway updates the ARP entry with the sender IP and MAC addresses of the ARP packet.
ARP active acknowledgement works either before creating an ARP entry or before modifying an ARP entry.

**Active acknowledgement before creating an ARP entry**

Before creating an ARP entry according to a received ARP packet, the gateway broadcasts an ARP request in which the target IP address is the sender IP address of the received ARP packet. If no ARP reply is received within three seconds, the gateway does not create the ARP entry. If an ARP reply is received within three seconds, the gateway compares the ARP reply with the formerly received ARP packet, including the sender IP address, sender MAC address, and the receiving interface.

- If the two packets are consistent, the gateway considers the formerly received ARP packet valid and creates the corresponding ARP entry.
- If the two packets are inconsistent, the gateway considers the formerly received ARP packet as an attack and does not create the corresponding ARP entry.

**Active acknowledgement before modifying an ARP entry**

Upon receiving an ARP packet (Packet A), the gateway checks the existing ARP entries for the sender IP address of Packet A. If an ARP entry with a matched IP address but an unmatched MAC address is found, the gateway performs the following actions:

1. Checks whether the ARP entry validity should be examined.
   
   To prevent frequent updating of the ARP entry for the same IP address, the gateway checks whether the ARP entry has been updated within the last minute:
   
   - If yes, the gateway does not update the ARP entry.
   - If not, the gateway checks the validity of the ARP entry.

2. Examines the validity of the ARP entry.
   
   The gateway unicasts an ARP request to the MAC address in the ARP entry. If no ARP reply is received within five seconds, the gateway does not update the ARP entry. If an ARP reply is received within five seconds, the gateway checks whether the sender IP and MAC addresses in the ARP reply are identical with those in the ARP entry:
   
   - If yes, the gateway considers Packet A as an attack and does not update the ARP entry.
   - If not, the gateway checks the validity of Packet A.

3. Checks the validity of Packet A.
   
   The gateway unicasts an ARP request to the sender MAC address in Packet A. If no ARP reply is received within five seconds, the gateway does not update the ARP entry. If an ARP reply is received within five seconds, the gateway checks whether the sender IP and MAC addresses in the ARP reply are identical with those in Packet A:
   
   - If yes, the gateway considers Packet A valid and updates the ARP entry.
   - If not, the gateway considers Packet A an attack and does not update the ARP entry.

**ARP packet source MAC 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. It allows the gateway to learn correct ARP entries.

**Source MAC-based ARP attack detection**

When a gateway device receives a large number of ARP packets from the same source MAC address within a short period of time, the gateway determines that a source MAC address-based ARP attack occurs.
Source MAC-based ARP attack detection allows the device to check the number of ARP packets delivered to the CPU based on their source MAC address. If the number of ARP packets sent from a MAC address within a check interval exceeds the specified threshold, the device generates an ARP attack entry for the MAC address. If the ARP logging feature is enabled, the device handles the attack by using either of the following methods before the ARP attack entry ages out:

- **Monitor**—Only generates log messages.
- **Filter**—Generates log messages and filters out subsequent ARP packets from the MAC address.

A gateway or critical server may send a large number of ARP packets. To prevent these ARP packets from being discarded, you can specify the MAC address of the gateway or server as a protected MAC address. A protected MAC address is excluded from ARP attack detection.

### Dynamic ARP learning limit on an interface

When the number of dynamic ARP entries learned by an interface reaches the maximum, the interface stops learning new entries. This feature prevents the ARP table of the device from being used up when the device is under an ARP attack.

If the dynamic ARP learning limit on an interface is set to 0, the interface is disabled from learning dynamic ARP entries.

### ARP defense against IP packet attacks

If a device receives large numbers of IP packets from a host to unreachable destinations,

- The device sends large numbers of ARP requests to the destination subnets, which increases the load of the destination subnets.
- The device keeps trying to resolve destination IP addresses, which increases the load of the CPU.

To protect the device from IP packet attacks, you can enable the ARP source suppression function or ARP blackhole routing function.

- **ARP source suppression**—stops 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**—creates 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.

  After a blackhole route is created for an unresolved IP address, the device immediately starts the first ARP blackhole route probe by sending an ARP request. If the resolution fails, the device continues probing according to the probe settings. If the IP address resolution succeeds in a probe, the device converts the blackhole route to a normal route. If an ARP blackhole route ages out before the device finishes all probes, the device deletes the blackhole route and does not perform the remaining probes.

  This feature is applicable regardless of whether the attack packets have the same source addresses.

- **ARP sender IP address checking**—Checks the sender IP address of an ARP packet in a VLAN before ARP learning. If the sender IP address is within the allowed IP address range, the gateway continues ARP learning. If the sender IP address is out of the range, the gateway determines the ARP packet as an attack packet and discards it.
Application scenarios

Monitoring mode

This mode is applicable to a network containing a large number of dynamically configured hosts. As shown in Figure 5, the hosts obtain IP addresses through DHCP. You can configure ARP attack protection on the access devices, and the gateway and the hosts do not need any ARP attack protection configuration.

With ARP attack protection configured, each received ARP packet has its sender IP and MAC addresses checked against the DHCP snooping entries. If no match is found, the ARP packet is considered invalid and discarded. This prevents a false ARP entry from being added to the gateway or a host.

As a best practice, you can also configure ARP packet rate limit to prevent ARP flooding on the access device.

Figure 5 ARP attack protection deployed in monitoring mode

Authentication mode

This mode is applicable to a network where authentication is required for login. As shown in Figure 6, the H3C IMC server, H3C iNode clients, access switches, and the gateway cooperate with each other to prevent ARP attacks. 802.1X authentication or portal authentication on the access devices denies illegal clients. After clients pass authentication, the access devices record the IP-and-MAC bindings of the clients.

To implement ARP attack protection on the access device:

- Configure ARP gateway protection on the user-side interfaces of the access devices to prevent gateway spoofing.
- Configure ARP filtering on the network-side interface of the access devices to prevent user spoofing and gateway spoofing.
Typically, the cybercafe is small-scale and stable, as shown in Figure 7. To implement ARP attack protection on the gateway, perform the following tasks:

1. Use ARP scanning to create dynamic ARP entries for all clients in the LAN.
2. Use the fixed ARP feature to convert the dynamic ARP entries to static.
3. Then, disable the gateway from learning dynamic ARP entries.

With the above configuration, the gateway allows only clients whose IP-to-MAC address bindings match the static ARP entries to access the Internet. In this way, the gateway prevents a client from using another client's IP address to access the Internet, thus keeping a clear online behavior record for the clients.
References

- RFC 826, An Ethernet Address Resolution Protocol
- RFC 2131, Dynamic Host Configuration Protocol (DHCP)
- RFC 3046, DHCP Relay Agent Information Option