Contents

1 Configuring ARP Check

1.1 Introduction

1.1.1 Overview

Address Resolution Protocol (ARP) Check is used to filter all ARP packets through an interface (L2 switching interface, L2 aggregation port, or L2 encapsulation subinterface) and discard all invalid ARP packets to prevent ARP spoofing and improve network stability.

On devices supporting ARP check, invalid ARP packets in networks will be filtered out according to the legitimate user information (detection based on IP address or IP address and MAC address) generated by security application modules such as IP Source Guard, global IP address and MAC address binding, 802.1x authentication, web authentication, and port security.

ARP Check uses the information to detect whether the Sender IP fields or the <Sender IP, Sender MAC> fields in all ARP packets through an interface match those in the legitimate user information table. If not, the ARP packets will be discarded.

1.1.2 Principles

1. Compatible Security Modules

ARP Check supports the following security modules:

- Detection of the IP address field only: port security and static configuration of IP Source Guard.
- Detection of the IP address and MAC address fields: IP Source Guard, global IP address and MAC address binding, 802.1x IP authorization, web authentication, and port security.

2. Filtering out Invalid ARP Packets

Enable ARP Check on specified interfaces to filter out invalid ARP packets.

A device matches the source IP and source MAC addresses of the ARP packets received through its interfaces with the valid user information in the database. With successful matching, packets will be transferred, or otherwise they will be discarded.

1.1.3 Protocols and Standards

- RFC 826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

1.2 Restrictions and Guidelines

- When ARP Check is enabled on an interface but IP Source Guard, global IP address and MAC address binding, 802.1x authentication, web authentication, or port security is not enabled on the interface to provide legitimate user information, all ARP packets through the interface will be discarded.
- ARP Check cannot be configured on mirrored destination ports.
- ARP Check cannot be configured on the trusted interfaces of DHCP Snooping.

- ARP Check cannot be configured on excluded interfaces of global IP address and MAC address binding.
- ARP Check can be configured only on switching interfaces, L2 aggregation ports, and L2 encapsulation subinterfaces.
- When ARP Check is enabled, the number of policies or users of related security applications may decrease.
- When the ARP Check and Virtual Router Redundancy Protocol (VRRP) functions are enabled on an interface and the physical IP address and virtual IP address of the interface can be used as the gateway address, the physical IP address and VRRP IP address need to be permitted to pass. Otherwise, ARP packets sent to the gateway will be filtered out.

1.3 Configuring ARP Check

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable ARP Check.

arp-check

ARP Check is disabled by default.

1.4 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1 Monitoring

Command	Purpose
show interfaces [*interface-type interface-number*] **arp-check list**	Displays the effective ARP Check entries on an interface.