Contents

1 Configuring Gateway-targeted ARP Spoofing Prevention

1.1 Introduction

1.1.1 Overview

Due to defects of Address Resolution Protocol (ARP), ARP cannot check the validity of received ARP packets. Attackers can easily use vulnerabilities of the protocol to launch ARP spoofing. When a malicious user host is disguised as the gateway to send ARP packets, other user hosts in the network will learn false gateway ARP entries, resulting in ARP spoofing.

The gateway-targeted ARP spoofing prevention function is therefore used.

1.1.2 Principles

1. Basic Concepts

- ARP

  ARP is a Transmission Control Protocol (TCP)/IP protocol that obtains physical addresses according to IP addresses. A host broadcasts ARP requests to all hosts in the network and receives the returned packets to determine physical addresses of the target IP addresses, and saves the IP addresses and hardware addresses in the local ARP cache, which can be directly queried in response to future requests. In the same network, all the hosts using ARP are considered as mutually trustful to each other. Each host in the network can independently send ARP response packets, and the other hosts receive the response packets and record them in the local ARP cache without detecting their authenticity. In this way, attackers can send forged ARP response packets to target hosts so that the messages sent from these hosts cannot reach the proper host or reach a wrong host, thereby causing ARP spoofing.

- Gateway-targeted ARP spoofing

  When host A sends an ARP packet requesting the media access control (MAC) address of a gateway, host B on the same VLAN also receives this packet. Host B can send an ARP response packet, passing off the gateway IP address as the source IP address of the packet and host B's MAC address as the source MAC address. This is called gateway-targeted ARP spoofing. After receiving the ARP response, host A regards host B as the gateway. Therefore, all the packets sent from host A to the gateway during communication will be sent to host B. In this way, host A's communications are intercepted, causing ARP spoofing.

2. Gateway-targeted ARP Spoofing Prevention

Gateway-targeted ARP spoofing prevention is used to check whether the source IP address of an ARP packet through an access interface is set to the gateway IP address. If yes, the packet will be discarded to prevent hosts from receiving wrong ARP response packets. If not, the packet will not be handled. In this way, only the uplink devices can send ARP packets, and the ARP response packets sent from other PCs which pass for the gateway are filtered out.

1.1.3 Protocols and Standards

- RFC 826: Ethernet Address Resolution Protocol

1.2 Configuring Gateway-targeted ARP Spoofing Prevention

(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 gateway-targeted ARP spoofing prevention.

anti-arp-spoofing ip *ipv4-address*

Gateway-targeted ARP spoofing prevention is disabled by default.

Gateway-targeted ARP spoofing prevention is supported only on L2 interfaces.

1.3 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 anti-arp-spoofing	Displays all data on gateway-targeted ARP spoofing prevention.

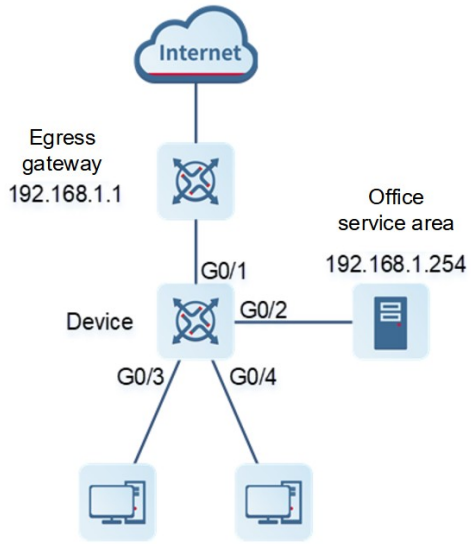
1.4 Configuration Examples

1.4.1 Requirements

User hosts access the office server through the access device, and connect to external networks through the gateway. If any malicious user hosts use forged gateway IP addresses or server IP addresses to perform ARP spoofing, the other user hosts cannot access the Internet or the server. The ARP spoofing packets with forged gateway addresses and intranet server IP addresses must be blocked so that users can access the Internet.

1.4.2 Topology

Figure 1-1 Configuring Gateway-targeted ARP Spoofing Prevention



1.4.3 Notes

Enable gateway-targeted ARP spoofing prevention on the access interface.

1.4.4 Procedure

Configure gateway-targeted ARP spoofing prevention.

```
Device> enable

Device# configure terminal

Device(config)# interface range gigabitEthernet 0/3-4

Device(config-if-range)# anti-arp-spoofing ip 192.168.1.1

Device(config-if-range)# anti-arp-spoofing ip 192.168.1.254
```

1.4.5 Verification

Run the **show anti-arp-spoofing** command to check for data on gateway-targeted ARP spoofing prevention.

```
Device> enable

Device# show anti-arp-spoofing

NO    PORT       IP               STATUS

----- ---------- ---------------- ----------

1     Gi0/3      192.168.1.1      active

2     Gi0/3      192.168.1.254    active
```

```
3     Gi0/4      192.168.1.1      active

4     Gi0/4      192.168.1.254    active
```

1.4.6 Configuration Files

```
hostname Device

!

interface GigabitEthernet 0/3

 anti-arp-spoofing ip 192.168.1.1

 anti-arp-spoofing ip 192.168.1.254

!

interface GigabitEthernet 0/4

 anti-arp-spoofing ip 192.168.1.1

 anti-arp-spoofing ip 192.168.1.254

!

end
```