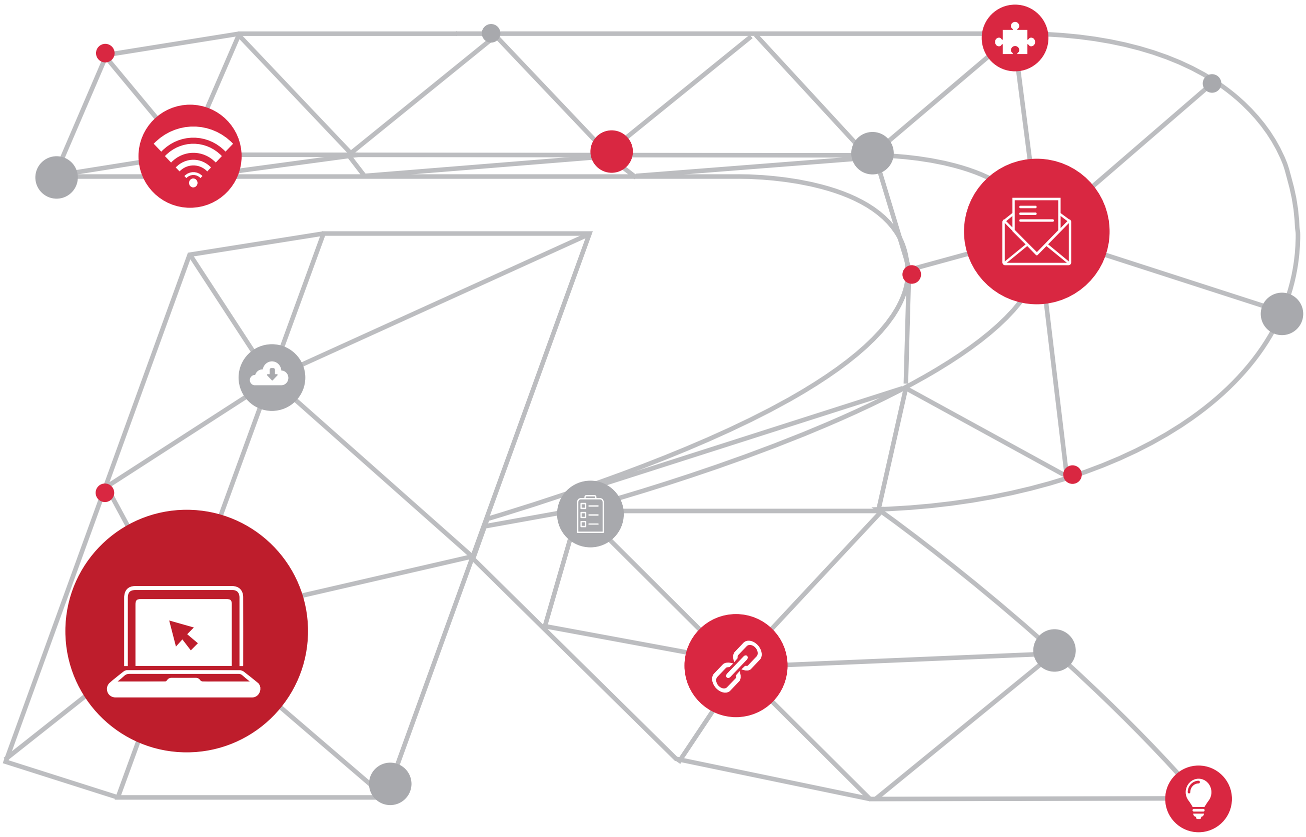
Ruijie Anti-ARP Spoofing

White Paper



Contents

Introduction

As the Address Resolution Protocol (ARP) has inherent vulnerabilities, and attackers often exploit these vulnerabilities to perform ARP spoofing on the Internet. The main principle behind ARP spoofing is to send false IP address-MAC address mappings for the purpose of stealing user information to make profits or endangering network stability. ARP spoofing allows attackers to steal or block packet communication of users. Hazards caused by ARP spoofing cannot be ignored, and countermeasures must be taken to protect against attackers' behaviors.

This document describes the requirement background of anti-ARP spoofing, relevant technologies, and technology principles, and analyzes Ruijie Networks anti-ARP spoofing solutions and typical applications.

ARP resolves network layer addresses (IP addresses) to data link layer addresses (MAC addresses). It is effective only to IP packets, which are actually transmitted as frames on local area networks (LANs). A frame contains the MAC address of a target host. On the Ethernet, a host must know the MAC address of the target host in order to communicate with the target host, and it obtains the MAC address of the target host through ARP. Address resolution is the process in which a host converts the target IP address into the target MAC address before sending frames. The basic function of ARP is to look up the MAC address of the target device based on its IP address to ensure smooth communication.

A host completes ARP learning according to the sender's protocol address (source IP address) and sender's hardware address (source MAC address in the packet data field) in an ARP packet. This process is crucial to ARP learning. Any host on a network, for example, host A, can broadcast ARP packets to advertise its IP address and MAC address. Each host that receives the ARP packet creates an ARP entry in its ARP table to record host A's IP address and MAC address, regardless of whether the ARP packet is correct.

Address resolution and learning of ARP is a dynamic process. This characteristic may be used for network spoofing. The main principle is to send false IP address-MAC address mappings with the aim of spoofing target hosts or network devices and intercepting or blocking user communications.

Technical Principle

• ARP

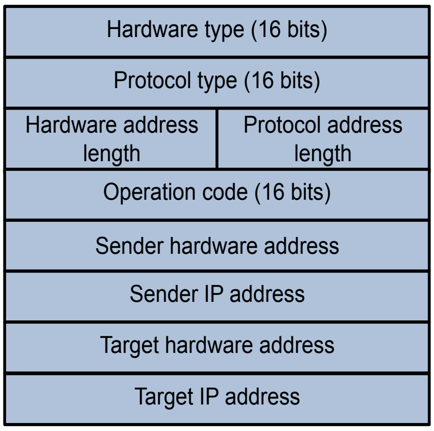
ARP Packet Format

ARP packets include ARP requests and ARP replies. Figure 1 shows the format of ARP request and reply packets.

* **An ARP request uses all fields except the target hardware address (that is, the address requested by the sender).**

* **An ARP reply uses all the fields.**

Figure 1 Format of an ARP Packet



Hardware type (16 bits)

Protocol type (16 bits)

Hardware address length | Protocol address length

Operation code (16 bits)

Sender hardware address

Sender IP address

Target hardware address

Target IP address

Creation of an ARP Table

Before two hosts on the Ethernet communicate with each other, they must know the MAC address of each other. A host does not know the MAC addresses of other hosts or the gateway when it is started. In order to communicate with another host, it needs to send an ARP request over ARP: I need to communicate with XXX (IP address), and what is the MAC address of XXX? After receiving the request, XXX gives an ARP reply: My MAC address is OOOO). The host sending the request records XXX and OOOO (IP address and MAC address) in a mapping table. The host does not need to send an ARP request again when it needs to communicate with XXX later; instead, it directly sends packets to OOOO. This mapping table is an ARP table.

ARP entries are classified into static entries and dynamic entries.

* **Static ARP entry: IP address-to-MAC address mappings manually configured and maintained.**

* **Dynamic ARP entry: IP address-to-MAC address mappings that are dynamically learnt by switches. Dynamic ARP entries age based on the preset time of the dynamic ARP aging timer.**

In general, the ARP table is created in two ways:

* **Proactive resolution: If a host needs to communicate with another host but does not know its MAC address, the host sends an ARP request proactively to learn the MAC address of the target host from the ARP reply.**

* **Reply to requests: If a host receives an ARP request from another host, it locally creates an IP address-MAC address mapping entry for the requesting host.**

The ARP table uses an aging mechanism. If an entry in the ARP table is not used within a certain period of time, the entry will be deleted, thereby greatly saving the space of the ARP table and speeding up the query.

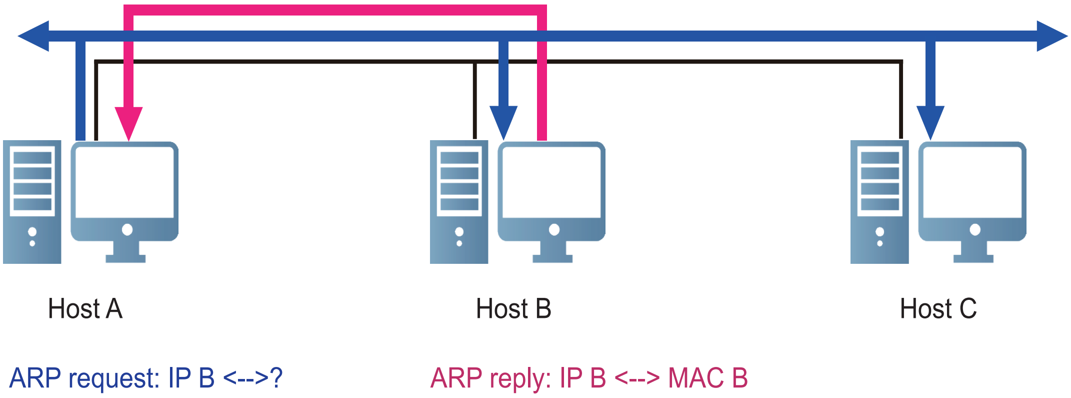
Working Principle of ARP

Each host has an ARP table, in which an IP address is mapped to a MAC address, as shown in the following table.

Host	IP Address	MAC Address
A	192.168.203.4	00-d0-f8-11-33-1a
B	192.168.203.5	00-d0-f8-27-02-2b
C	192.168.203.6	00-d0-f8-06-08-3c

In the following example, host A (with the IP address of 192.168.203.4) needs to send data to host B (with the IP address of 192.168.203.5). In order to send data, host A looks up the target IP address in its APR table. If the target IP address is found, host A directly writes the MAC address mapping to the target IP address into a frame as the target MAC address and sends out the frame. If the ARP table does not have such an IP address, host A broadcasts a packet (the destination MAC address is FF.FF.FF.FF.FF.FF), requesting the MAC address of 192.168.203.5 from all hosts in the same network segment. Other hosts do not respond to the ARP request, and only host B sends a reply (the MAC address of 192.168.203.5 is 00-d0-f8-27-02-2b) to host A, as shown in Figure 2. In this way, host A knows the MAC address of host B and can send messages to host B. In addition, host A updates its ARP table so that it can directly loop up the target MAC address in the ARP table when sending messages to host B next time.

Figure 2 Working Principle of ARP



• ARP Spoofing

According to descriptions above, in order to communicate with XXX, a requester sends an ARP request (I need to communicate with XXX, what is the MAC address of XXX). The requester does not know where XXX is, and the ARP request is broadcasted. All hosts that receive the ARP request can respond to this request. For example, a malicious user may respond to the request by giving a reply (I am XXX and my MAC address is AAAA). Then, the requester believes that the MAC address of XXX is AAAA, and spoofing occurs.

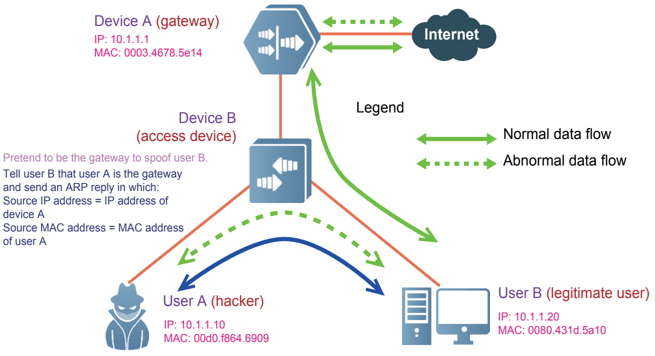
ARP spoofing on an LAN includes gateway spoofing and host spoofing.

Gateway Spoofing

An ARP spoofing attacker on a network advertises a spoofing packet (I am the gateway), other hosts incorrectly believe that the attacker is the gateway, and send packets to the attacker. As a result, the spoofed hosts cannot access the Internet or their information may be stolen.

As shown in Figure 3, in order to communicate with gateway A, user B needs to know the MAC address of gateway A. If user A pretends to be the gateway and sends a reply to user B to inform user B that the MAC address of gateway A is the MAC address of user A. Then, user B is spoofed, and data from user B cannot reach the gateway, causing network disconnection.

Figure 3 Network Topology of Gateway Spoofing



The following table lists changes in the ARP table of user B.

ARP table of user B before spoofing	
MAC address	IP address
0003.4678.5e14	10.1.1.1
00d0.f864.6909	10.1.1.10
ARP table of user B after spoofing	
MAC address	IP address
00d0.f864.6909	10.1.1.1

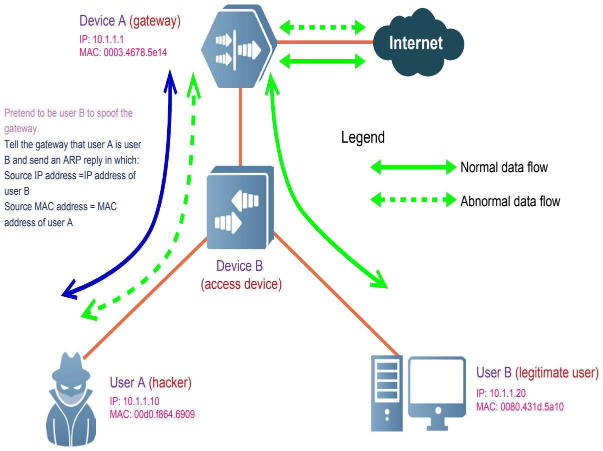
The preceding table shows that the ARP table of user B stores only addresses of user A. Therefore, data streams from user B are all sent to user A instead of the gateway, and user B cannot access the Internet.

Host Spoofing

Host spoofing includes spoofing the gateway and spoofing other hosts. For example, when a gateway sends an ARP request in order to send packets to user B, attacker A sends a reply to the gateway to inform the gateway that attacker A is user B. As a result, the gateway is spoofed, packets that are bound for user B are sent to attacker A, and user B cannot access the Internet or its information is stolen. The principle of spoofing other hosts is the same as the principle of spoofing the gateway.

As shown in Figure 4, network communication is a bidirectional process. That is, user B and gateway A can communicate with each other successfully only when the communications from user B to gateway A and from gateway A to user B are reachable. Assume that user A pretends to be user B and sends a reply to gateway A to inform gateway A that the MAC address of user B is the MAC address of user A. Then, the gateway is spoofed. Though the communication from user B to gateway A is reachable, data streams from gateway A that are originally destined for user B are sent to user A. As a result, user B is disconnected from the network.

Figure 4 Network Topology of Host Spoofing



The following table lists the changes in the ARP table of gateway A.

ARP table of gateway A before spoofing	
MAC address	IP address
0080.431d.5a10	10.1.1.20
00d0.f864.6909	10.1.1.10

ARP table of gateway A after spoofing	
MAC address	IP address
00d0.f864.6909	10.1.1.20

The preceding table shows that the ARP table of the spoofed gateway A stores only addresses of user A. Therefore, data streams from gateway A are all sent to user A instead of user B, and user B cannot access the Internet.

Anti-ARP Spoofing Solutions

• Non-Network Device Solutions

ARP spoofing is a vulnerability of the network protocol, and the protocol cannot be altered to radically fix the vulnerability. Therefore, some "shanzhai" solutions are proposed.

Gratuitous ARP

The gateway repeatedly broadcasts an ARP reply on LANs so that user hosts on the LANs repeatedly update the IP address-MAC address mapping of the gateway. That is, the gateway repeatedly broadcasts a message indicating that it is the gateway, and the packet sent by an attacker who pretends to be the gateway will be "flooded".

This solution can prevent hosts on LANs from pretending to be the gateway and performing ARP spoofing. Nevertheless, the gateway cannot broadcast a packet indicating that it is the gateway all time as it will consume a large number of bandwidth and the ARP tables of user hosts need to be updated continuously. In addition, if an attacker sends a spoofing packet to notify other hosts that it is the gateway at a faster speed, the network bandwidth will be consumed more considerably and hosts are still be spoofed.

Static Binding on Hosts

In this solution, the IP address-MAC address mapping of the gateway is manually and statically bound in hosts, that is, users know the correct IP address and MAC address of the gateway.

This solution seems effective. After careful consideration, it does not work efficiently. How can users know the correct IP address and MAC address of the gateway? Customers with technical background know to run the arp-a command to acquire them but customers without technical background can bind the IP address and MAC address of the gateway only under the guidance of the network center. This solution is inadequate in the presence of numerous users.

What is worse is that present ARP viruses are able to delete ARP static binding of the gateway from hosts. That is, users need to repeatedly configure the static binding of IP address and MAC address of the gateway. One binding for each host is a great bottleneck, let alone repeated binding. This solution is basically unfeasible if repeated binding is required.

• Ruijie Anti-ARP Spoofing Solutions

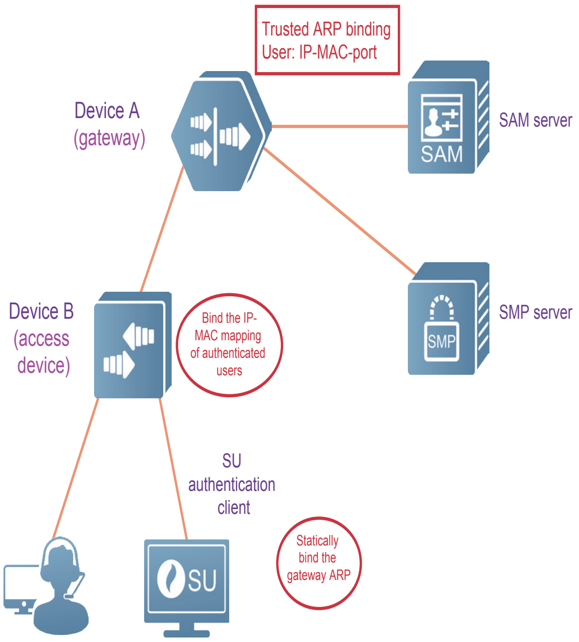
GSN Solution

As shown in Figure 5, this solution uses the GSN technology, in combination with the following modes:

ARP static binding of gateway addresses on hosts: gateway addresses are statically bound on the supplicant (SU) host, which is the same as the solution of static binding on hosts. The difference is that the static binding is performed automatically in this solution, which resolves problems in the solution of static binding on hosts.

When a user goes online, the security management platform (SMP) delivers the gateway IP address and MAC address of the user to the SU. The SU statically binds the IP address and MAC address of the gateway on the user host, and periodically detects whether the ARP static binding is altered. If it is altered, the SU rebinds the IP address and MAC address of the gateway, to prevent some Trojan horse programs from altering the ARP static binding in a legitimate manner and ensure the accuracy of gateway ARP information. When the user goes offline, the SU deletes the ARP static binding of the gateway from the user host.

Figure 5 GSN Solution



Trusted ARP binding on the gateway: When a user goes online, the security accounts manager (SAM) transfers gateway information of the legitimate user, and the SMP statically binds the IP address and MAC address of the user host over ARP on the gateway according to relevant gateway information. This mode is combined with the mode of ARP static binding of gateway addresses on hosts to achieve dual binding. The ARP-check function enables the gateway to discard received spoofing ARP packets. When the user goes offline, the SMP deletes the trusted ARP binding from the gateway.

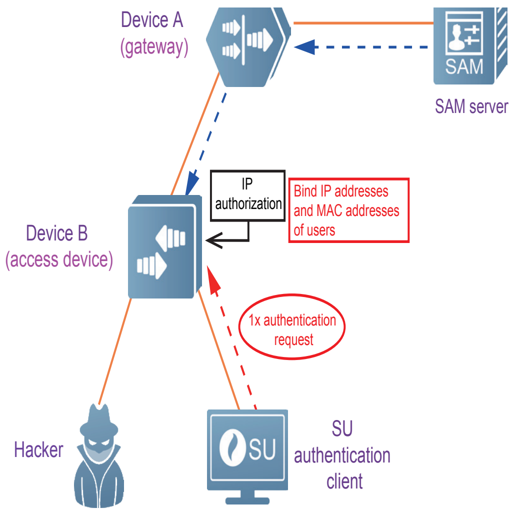
Static ARP binding on the security access switches: A switch detects users' authentication packets. After a user passes the authentication, the switch automatically binds the IP address and MAC address of the user. Then, it checks the security of received ARP packets through the ARP-check function, and discards the ARP packets in which addresses do not match the bound addresses, thereby eliminating ARP spoofing.

SAM Solution

As shown in Figure 6, this solution adopts IP authorization (RADIUS authorization) on a security access switch. When a user performs 802.1X authentication, the switch detects the authentication packets of the user. After the user passes authentication, the switch automatically binds the IP address and MAC address of the user host to generate an IP address + MAC address binding table. Then, it checks he security of received ARP packets through the ARP-check function, and discards the ARP packets in which addresses do not match the binding table, thereby eliminating ARP spoofing.

The principle of this solution is the same as that of static ARP binding on security access switches in the GSN solution. The GSN solution, however, not only eliminates ARP spoofing but also brings other values of the GSN.

Figure 6 Network Topology of the SAM Solution



ARP-Check/DAI Solution

The preceding two solutions are attractive, and why a third solution is required? The reason is that not all projects use the GSN or SAM, and the third solution is a flexible choice for users.

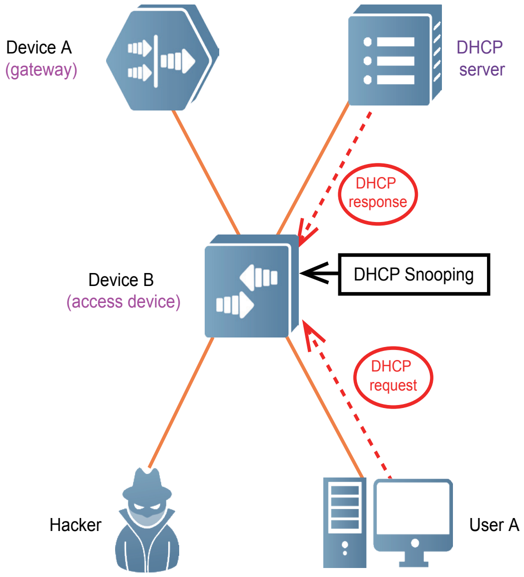
This solution involves two cases:

Dynamic assignment of IP addresses: In this mode, user hosts exchange DHCP packets with the DHCP server to acquire IP addresses. A switch detects DHCP packets of user hosts, and records the IP addresses and MAC addresses of the user hosts in the IP address + MAC address binding table. Then, it checks the security of received ARP packets through the ARP-check function, and discards the ARP packets in which addresses do not match the binding table, thereby eliminating ARP spoofing.

Static assignment of IP addresses: The preceding solutions show that the IP addresses and MAC addresses of users need to be bound first so as to prevent ARP spoofing. In this mode, how can a switch know the correct IP addresses and MAC addresses? The answer is manual binding. Switches do not know the correct IP addresses and MAC addresses, and need to obtain them from a third party, record them in the IP address + MAC address binding table. Then, the switch checks the security of received ARP packets through the ARP-check function, discards the ARP packets in which addresses do not match the binding table, thereby eliminating ARP spoofing.

DAI is short for dynamic ARP inspection. The principle of DAI is the same as that of the ARP-check. The difference is that the ARP-check delivers the IP address + MAC address binding table to hardware and the operation of checking ARP packets is completed by the hardware, whereas the DAI uses software to implement this process. For details, see the DHCP snooping technology white paper.

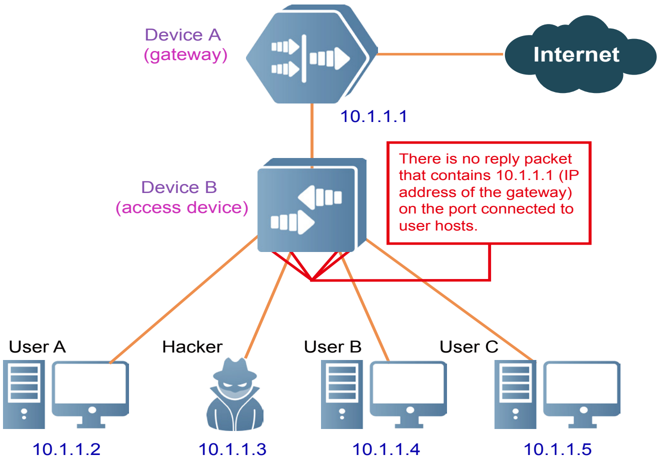
Figure 7 Network Topology of the ARP-Check/DAI Solution



Anti-Gateway Spoofing Solution

As shown in Figure 8, in this solution, the IP address of the gateway is configured on the access device and ARP packets are checked on all ports except the port connected to the gateway. If the ARP packets checked on such ports contain the IP address of the gateway, the ARP packets are considered as spoofing packets and are discarded. The reason is that ARP packets that contain the IP address of the gateway can be detected only on the port connected to the gateway.

Figure 8 Network Topology of the Anti-Gateway Spoofing Solution


Device A
(gateway)
Internet
10.1.1.1
Device B
(access device)
There is no reply packet that contains 10.1.1.1 (IP address of the gateway) on the port connected to user hosts.
User A
Hacker
User B
User C
10.1.1.2
10.1.1.3
10.1.1.4
10.1.1.5

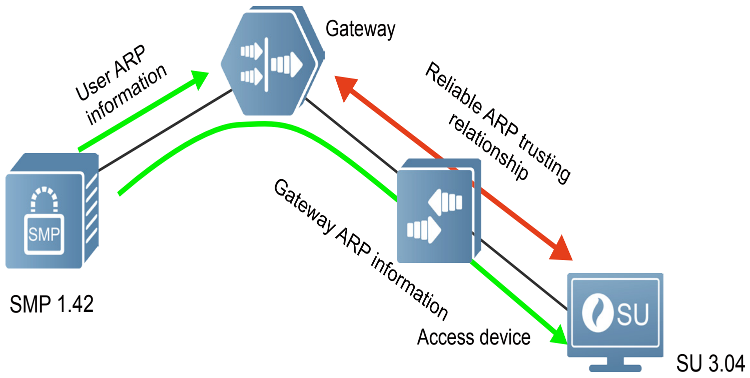
Application Cases of Anti-ARP Spoofing

• GSN Anti-ARP Spoofing in a University

Application Principle

As shown in Figure 9, the SMP server, serving as a reliable third party, provides correct ARP information. It sends correct ARP information about the gateway to the SU for static binding, and sends the correct ARP information about hosts to the gateway to generate trusted ARP entries, implementing bidirectional binding for hosts and the gateway and effectively preventing ARP spoofing.

Figure 9 GSN Anti-ARP Spoofing in a UniversitySpoofing Solution



Applicable Environment

* **There are more than 300 student computers in the central network computer room, and Trojan horses and other viruses are rampant.**

* **Teachers in the computer room report that the network goes offline frequently and considerable ARP attack events occur.**

Application Solution

A test host is connected to the network of the computer room. The ARP firewall software is started, ARP attacks existing on the network are observed, and the actual network conditions are observed before and after the GSN anti-ARP spoofing function is enabled.

1.Connect the test host to the network of the computer room. The following table provides network connection details of the test host.

Network connection details of the test host	
MAC address	0015.f2b5.5b69
IP address	210.34.136.252
Subnet mask	255.255.255.0
Default gateway	210.34.136.1
DNS server	210.34.128.33
WIN server	202.112.

2. It is found that ARP spoofing attacks are rampant on the network.

More than 300 student computers are not managed properly and become a virus and Trojan horse zoo. Mass attack events are detected within one minute after the ARP firewall is enabled.

(1) Actual use condition

The network goes offline once every five minutes on average.

(2) Attack behavior analysis

The gateway entry in the local ARP table is correct. Nevertheless, no response is received after the gateway is pinged. After the packet capture is performed, it can be determined that the gateway encounters ARP spoofing attacks, which results in the disconnection of the PC from the network.

(3) Enabling of the GSN anti-ARP spoofing function

1) View the ARP table of the SU.

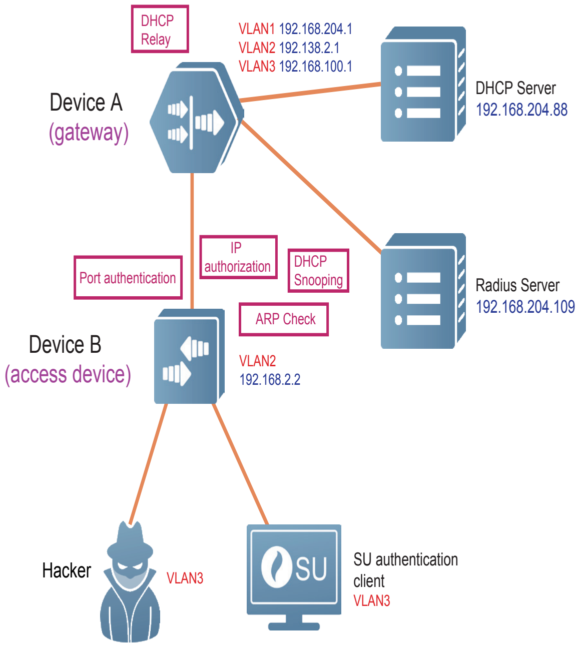
2) View the ARP table of the gateway.

(4) Observation of the trail running of the anti-ARP spoofing function

1) The network is proper and is not affected within the two-hour trial running of the anti-ARP spoofing function.

Application Topology

Figure 10 Topology of Anti-ARP Spoofing in DHCP Relay Authentication



Application Description

As shown in Figure 10, this solution prevents ARP spoofing by using the cross-management VLAN DHCP relay (the DHCP Option82 function is enabled) of L3 devices, IP authorization mode of L2 devices, DHCP snooping, ARP-check, and port authentication.

Before a user host connected to device B passes authentication, it can obtain an address over DHCP but cannot access an external network by using the address. Controlled port does not perform address learning. The ARP-check module does not forward ARP packets from the user host because the addresses of the user host are not bound. Therefore, gateway A will not be spoofed.

After the user host passes authentication, it obtains a correct IP address over DHCP, and the address dynamically obtained in IP authorization mode (from the DHCP server) is bound. The ARP-check module checks received ARP packets and forwards or discards ARP packets according to preset rules, to ensure that forwarded ARP packets are legitimate packets.

If the static IP address of an access client is changed, the ARP-check module matches the IP addresses contained in the received ARP packets with bound addresses in the DHCP snooping database in IP authorization mode, and forwards or discards the packets according to preset rules. The switch does not have the static address of the access client and therefore, it discards the ARP packets sent from the client with the static IP address changed. The ARP packets are not forwarded by device B and the gateway will not be spoofed.

For access devices that do not support the ARP-check function, DAI can be used to check the validity of received ARP packets. DAI mainly performs the following steps:

1. Intercept all ARP request packets and ARP reply packets on untrusted ports in the VLANs where the DAI function is enabled.
2. Check the validity of intercepted ARP packets according to preset rules of the DHCP database.
3. Discard the ARP packets that do not pass the validity check.
4. Send the ARP packets that pass the validity check to the destination.

Precautions

There are multiple anti-ARP spoofing methods. When different functions are used together, pay attention to whether the functions conflict with each other and relevant restrictions.

* **The ARP-check function can be used in combination with the following four modes to prevent ARP spoofing: 1) static binding of secure IP addresses and MAC addresses on ports; 2) dynamic address binding on DHCP ports; 3) IP authorization mode in the case of authentication; 4) binding of GSN access switches.**

* **DAI can be used only in combination with DHCP Snooping.**

* **User hosts that pass authentication and have their addresses bound have the highest priority. When an ACL is re-configured for a port, the ACL is ineffective to the user hosts that have passed authentication.**

* **The security channel function and anti-ARP spoofing function are mutually exclusive.**

The anti-ARP spoofing function uses the ARP-check function, in combination with bound trusted IP addresses and MAC addresses, to detect ARP packets. It forwards valid ARP packets and filters out invalid ARP packets. The security channel function allows untrusted users to access specific websites through specific protocol data before they are authenticated. Therefore, untrusted users are allowed to interact with the gateway through ARP packets. If both the security channel function and ARP-check function are enabled, the ARP packets of the untrusted users will be filtered out.

Conclusion

Ruijie anti-ARP spoofing technologies include the GSN solution, SAM solution, anti-gateway spoofing solution, and intelligent NBR and switch correlation solution. The static ARP binding, trusted ARP binding, and ARP-check in combination with relevant functions are flexibly applied in these solutions, to provide better guarantee for the normal running of networks (especially the normal Internet access service of legitimate users), user security enhancement, and entire network availability.

Ruijie Networks Co.,Ltd

For further information,please visit our website **http://www.ruijienetworks.com**