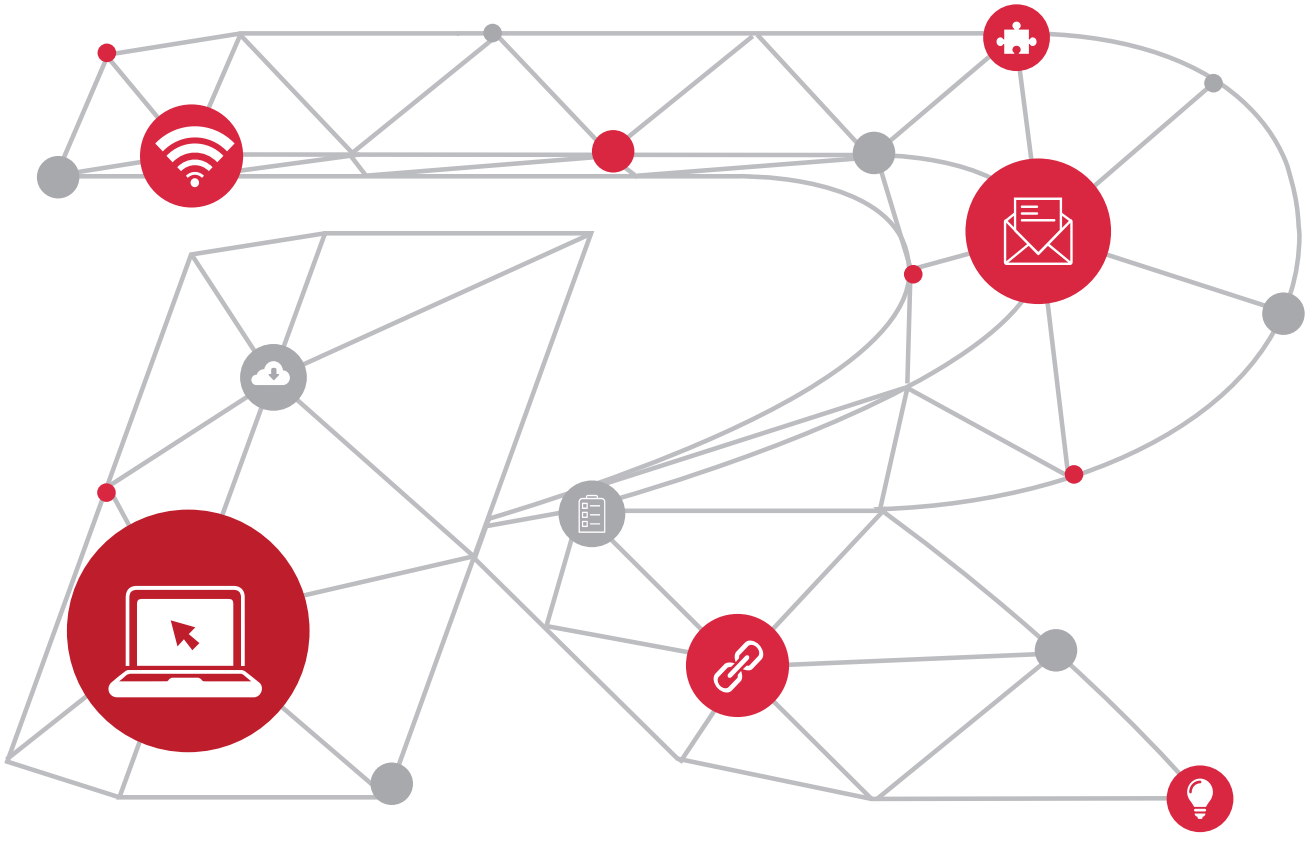
Ruijie DHCP Snooping

White Paper



Contents

Introduction 3

Technical Analysis of DHCP 4

DHCP Overview 4

DHCP Technical Principle 5

Technical Analysis of DAI 7

ARP Overview 7

ARP Spoofing Technical Principle 7

DAI Technical Principle 7

Typical Application 9

Application Topology 9

Application Deployment 9

DHCP Snooping + DAI 10

Conclusion 12

Introduction

This paper introduces DHCP Snooping and relevant technologies, and how to utilize DHCP Snooping technology in conjunction with relevant technologies to implement security control under DCHP environment, including invalid server blocking, preventing user from configuring private IP address, and avoiding ARP spoofing.

Applying C/S mechanism, DHCP (Dynamic Host Configuration Protocol) is a simplified TCP/IP standard for host IP address configuration and management. This standard allows the DHCP server to provide IP address and other relevant configurations to the client. On the network, enabling DHCP service allows DHCP client to automatically acquire IP address and relevant configurations every time after reboot, thus reducing the burden of configuration and management. On the network with excess computers and multiple subnets, DHCP is especially advantageous as it avoids the error caused by manual configuration of IP address and subnet, as well as the address conflict caused by assigning one IP address to multiple hosts. It can significantly reduce the time spent by network administrator on host address configuration, as well as the configuration burden.

However, with the extensive application of DHCP service, network management is now faced with certain new problems:

* Since there is no authentication mechanism applied during the interaction between client and server. If there is any invalid DHCP server on the network, the administrator won't be able to guarantee that the client can request a valid address from the DHCP server specified by the administrator. The client may acquire IP address and other configurations from the invalid DHCP server, leading to the confusion in address assignment, or even information theft.

* In DHCP-enabled subnet, if a user configures an IP address without authorization, it will cause failure to access the network for other users.

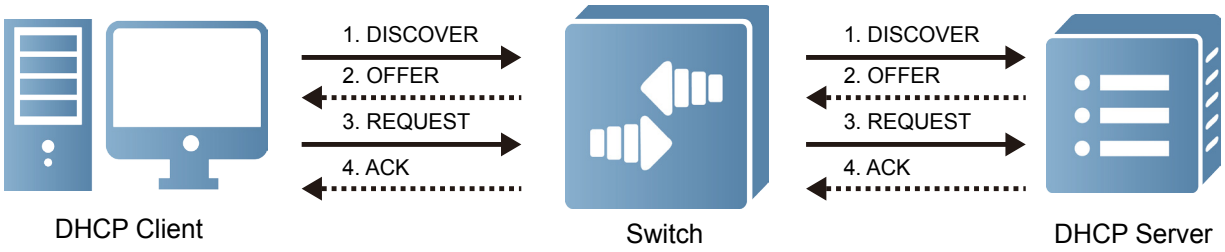
Another major challenge faced by network management is ARP spoofing, which is currently infesting the network. Since ARP protocol cannot verify the authenticity of these packets, hosts and devices on the network are easily spoofed, thus preventing user from using network normally.

Technical Analysis of DHCP

• DHCP Overview

DHCP technology is mainly utilized to dynamically assign reusable IP addresses and parameter configurations to hosts on the network. Applying C/S mechanism, DHCP completes IP address request through DHCP packet interaction between the client and server. The server can assign IP address and other configuration parameters to the client, such as subnet mask, DNS-server, default-router, lease duration and etc. On the same subnet, the typical IP address request procedures are shown below:

Figure 1 DHCP Packet Interaction Procedures



1. DHCP Client sends DHCP DISCOVER broadcast packet to the DHCP Server. If DHCP Client receives no response from the server within the specified time, it will resend DHCP DISCOVER packet.
2. Upon receipt of DHCP DISCOVER packet, the DHCP Server will assign IP address to the DHCP Client according to certain policy, and then send DHCP OFFER packet.
3. Upon receipt of DHCP OFFER packet, DHCP Client will send DHCP REQUEST packet to request parameter configurations from DHCP Server.
4. Upon receipt of DHCP REQUEST packet, the server will verify whether the resources are allocable. If yes, it will send DHCP ACK packet.

The basic DHCP packet interaction procedures during IP address request have been introduced above. There are also other packets during the interaction between DHCP Client and DHCP Server, as shown below:

1. DHCP Client sends DHCP RELEASE packet to notify the DHCP Server to terminate IP address lease.
2. DHCP Server sends DHCP NAK packet to notify the DHCP Client of address request failure.
3. DHCP Client sends DHCP DECLINE packet to notify the DHCP Server that this IP address will lead to conflict and is unusable.

If DHCP Client and DHCP Server are not within the same subnet, IP address request will need a DHCP Relay, which will forward DHCP data packets between DHCP Client and DHCP Server.

• DHCP Technical Principle

DHCP Snooping is capable of blocking invalid DHCP server and invalid DHCP packets, thus addressing the security concern arisen during the interaction between DHCP Client and DHCP Server. As shown in Fig 1, after enabling DHCP Snooping, our switches will be able to snoop the DHCP interaction packets transmitted between DHCP Client and DHCP Server. Through DHCP Snooping, information about valid DHCP users (IP address, MAC address, VLAN, port, lease time and etc) can be recorded to form DHCP Snooping database, which can provide:

* Reference for IP packet filtering;

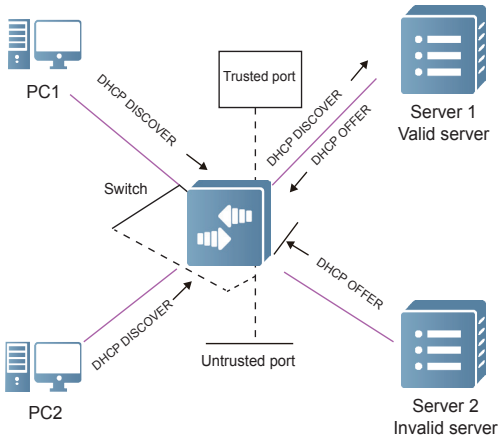
* Reference for ARP packet filtering.

Blocking Invalid DHCP Server

To block invalid DHCP server, the administrator needs to configure ports as trusted ports and untrusted ports. DHCP Snooping will process DHCP packets based on software. As shown in Fig 2, the port connecting with valid server is configured as trusted port, and other ports are by default untrusted ports. For the request packets from DHCP clients, the switch will only forward such packets to the trusted port. For the reply packets from DHCP servers, the device will only forward the reply packets received from trusted port and drop all reply packets received from untrusted port.

As shown in Fig 2, for DHCP DISCOVER packets sent from PC1 and PC2, the switch will only forward them to the trusted port; for DHCP OFFER packets sent from Server1 and Server2, the switch will only forward the reply packets from Server1 and drop the reply packets from Server2.

Figure 2 DHCP Packet Processing on Trusted Port and Untrusted Port



Blocking Invalid Packets

DHCP Snooping will check the validity of DHCP packets passing through the device in order to filter invalid packets. The following types of packets are considered as invalid DHCP packets:

1. The DHCP server reply packets received by untrusted port, including DHCP ACK, DHCP NAK, DHCP OFFER and etc;
2. DHCP client request packets forwarded through DHCP relay;
3. If DHCP Snooping source MAC check is enabled, if the value in the Client MAC field of DHCP packets sent by Client is inconsistent with the source MAC address carried in link-layer header of packets, such packets will be considered as invalid packets;
4. If DHCP RELEASE and DHCP DECLINE packets received are inconsistent with the entries in DHCP Snooping database, such packets will be considered as invalid packets.

Option 82

While implementing IP management of existing users, some network administrators may want to assign IP address according to the network device connected by the user. DHCP Snooping allows the switch to insert certain user-specific device information into the DHCP request packets in the format of DHCP Option during DHCP snooping. According to RFC3046, the DHCP Option number used is 82. The information inserted via Option 82 includes user's MAC address, VLAN ID, port number and etc. Through the Option 82 information carried in DHCP request packets, DHCP server can assign IP addresses in a more accurate manner.

DHCP Snooping Database

After enabling DHCP Snooping on the switch, DHCP Snooping will snoop the DHCP packets exchanged between DHCP Client and DHCP Server. Through DHCP Snooping, such information as the IP address offered, user's MAC address, VLAN, port and lease time can constitute a user record entry which can be added into DHCP Snooping database. Fig 3 shows the user information stored in DHCP Snooping database.

Figure3 DHCP Snooping Database

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
----------	-------	-------	----------	-----	----------
00d0.f866.471c	192.168.10.2	2591469	DHCP Snooping	1	GigabitEthernet 0/5

DHCP Snooping database allows record insertion, update and removal. After the client has successfully requested an IP address, relevant records will be added into the DHCP Snooping database; after the client has successfully renewed the DHCP lease, the lease time in DHCP Snooping database will be updated; when DHCP RELEASE packet is sent by the client or when the lease time expires, the corresponding DHCP Snooping database entry will be removed. DHCP Snooping database also allows manual entry insertion and removal and static user binding.

To avoid the loss of user information in database after device reboot, DHCP Snooping can periodically write such user information into the flash. After device reboot, DHCP Snooping database will be loaded automatically from the flash, so that the former DHCP users can use the network normally.

Providing IP Packet Hardware-Filtering Database

IP packet hardware-filtering feature implements validity check of IP packets based on hardware, so as to permit IP packets sent by valid users and discard IP packets sent by invalid users. IP packet hardware-filtering is based on DHCP Snooping database. Only users having the corresponding entry in DHCP Snooping database are allowed to send IP packets, thus preventing users from configuring IP addresses privately.

After IP packet hardware-filtering feature is enabled, DHCP Snooping will insert DHCP Snooping database information into the hardware-filtering table.

Providing ARP Packet Filtering Database

ARP packet filtering feature will implement validity check of the ARP packets received and directly discard invalid ARP packets, so as to effectively avoid ARP spoofing. DHCP Snooping database maintains such information as IP address, MAC address, VLAN ID and PORT number of valid DHCP users. By comparing the information in ARP packets with the entries in DHCP Snooping database, valid packets are identified and invalid ARP packets are filtered.

Technical Analysis of DAI

To address the problem of ARP spoofing, all ARP packets passing through the switch must be subject to validity check in order to drop ARP-spoofing packets. According to such a need, Ruijie Networks has launched software-based DAI (Dynamic ARP Inspection) technology and hardware-based ARP-Check technology. This paper mainly introduces the software-based DAI technology. For details about ARP-Check technology, please refer to the corresponding white paper.

- ARP Overview

See White Paper for Ruijie Anti-ARP Spoofing Technology for details.

- ARP Spoofing Technical Principle

See White Paper for Ruijie Anti-ARP Spoofing Technology for details.

- DAI Technical Principle

To prevent user or network device from being spoofed by invalid ARP packets, all ARP packets passing through the switch will be sent to the CPU for validity check. This process is called Dynamic ARP Inspection (DAI), which is based on DHCP Snooping database and will only take effect after DHCP Snooping is enabled. After DAI is enabled, the source IP, source MAC, port number and VLAN ID in ARP packets will be compared with the user information contained in DHCP Snooping database. If they are identical, the ARP packet will be considered valid; otherwise, the ARP packet will be considered invalid and discarded.

DAI technology consists of ARP packet rate-limiting, port trust state configuration and ARP packet validity check, while ARP packet validity check is the core component of DAI technology. These three components will be introduced below.

ARP Packet Rate-Limiting

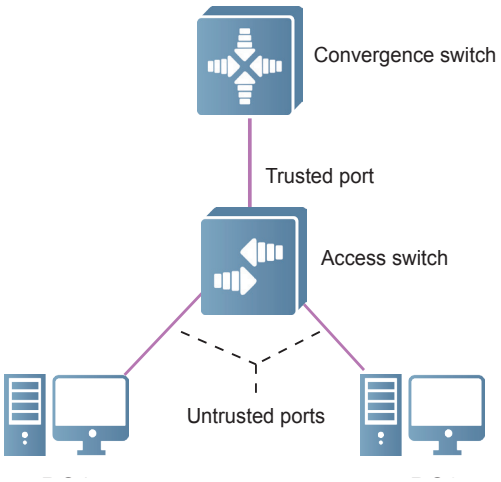
Since DAI validity check will consume certain CPU resources, the data rate of ARP packets must be limited in order to defend against DoS attacks. By default, the maximum number of ARP packets received by an untrusted port is limited to 15, while the trusted ports are not limited. Since ARP packet rate-limiting is based on software, the rate-limiting effect may deviate when the CPU of switch is busy.

Trusted Port & Untrusted Port

In DAI, not all ARP packets received by every port must undergo validity check. To distinguish between ARP packets requiring validity check and those exempted from validity check, the administrator needs to configure ports into trusted ports and untrusted ports. ARP packets received by the trusted port will be exempted from DAI check, while those received by the untrusted port will be sent to validity check.

As shown in Fig 5, PC1 and PC2 may send ARP-spoofing packets, and thus ports connecting PC1 and PC2 must be configured as untrusted ports in order to filter the ARP-spoofing packets received. The convergence switch won't send ARP-spoofing packets, and thus the port connecting convergence switch must be configured as trusted port in order to skip the validity check of ARP packets received.

Figure 5 Port Configuration for DAI



ARP Packet Inspection

DAI handles ARP packets through ARP packet rate-limiting and port state. The following steps are involved:

1. To intercept all ARP packets passing through the switch;
2. If the number of ARP packets received by the port per second exceeds the pre-configured value, the excess ARP packets will be dropped;
3. If DAI is not enabled for the corresponding VLAN, existing procedures will be followed;
4. If the corresponding port is a trusted port, existing procedures will be followed;
5. If DAI has been enabled for the corresponding VLAN and the ingress port is an untrusted port, all ARP packets will be subject to validity check based on DHCP Snooping database.
6. Packets passing validity check will be handled as per the existing procedures; those failed in validity check will be dropped.

Difference Between DAI and ARP Check

DAI filters ARP packets through software. Specifically, DAI sends all ARP packets to CPU for check. The ARP packets not matching IP+MAC address binding are discarded.

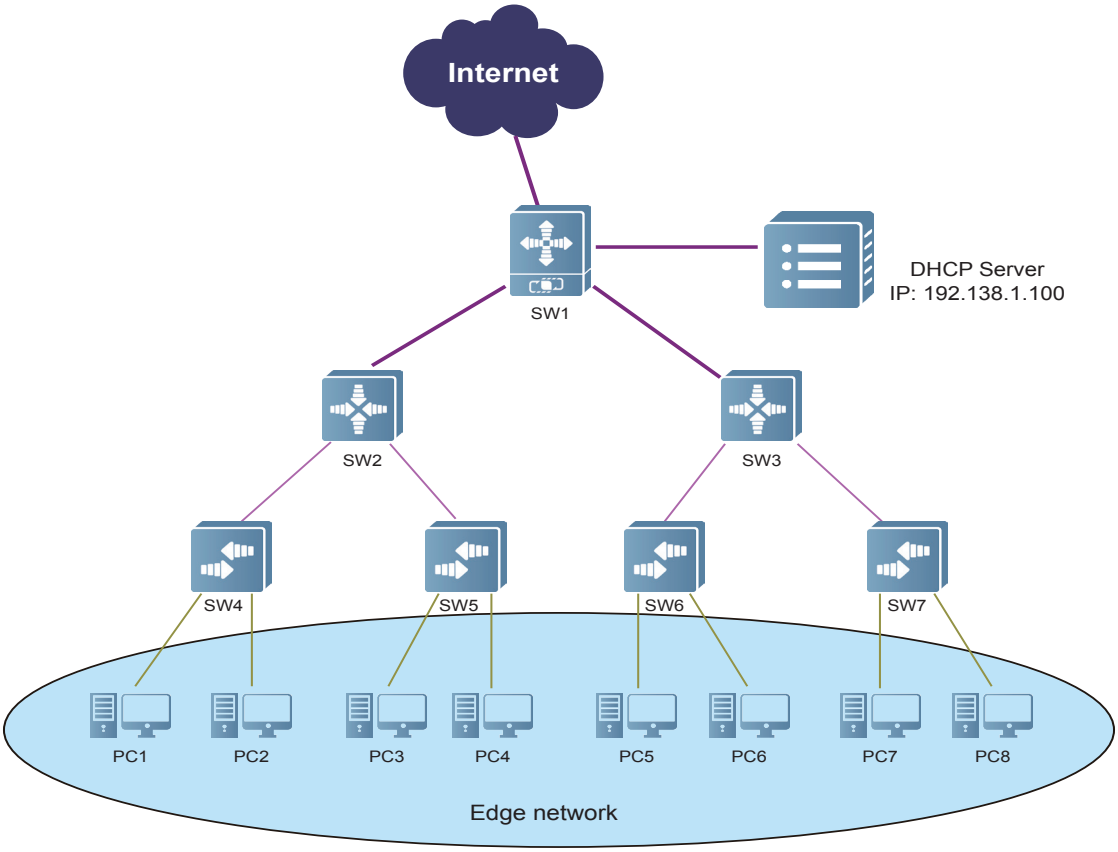
ARP Check filters ARP packets through hardware. When ARP packets are large in number, the approach is effective.

DAI and ARP Check shares the same principle but takes effect in different ways. Currently, S23 only supports software-based DAI while the products with the anti-ARP spoofing feature support both ARP Check and DAI.

Typical Application

• Application Topology

Figure 6 Topological Diagram for DHCP Snooping + DAI Application



As shown in Fig 6, SW4-SW7 are access layer devices; SW2-SW3 are convergence layer devices; SW1 is the core layer device. To effectively defend against DHCP and ARP spoofing, DHCP Snooping and DAI (or ARP-Check) must be enabled on SW4-SW7.

• Application Deployment

Through the above description, we can understand that DHCP Snooping + DAI (or ARP-Check) solution will make existing network more stable and secure. This solution is mainly deployed on the access device. If this solution is deployed on devices at the convergence layer or above layer, invalid DHCP and ARP packets from the access layer cannot be controlled effectively, and the advantages of solution won't be given full play to. As shown in Fig 6, if DAI (or ARP-Check) is deployed on SW2, although PC3 and PC4 won't be spoofed by the ARP packets sent from PC1 and PC2, mutual spoofing may take place between PC1 and PC2 and between PC3 and PC4. Given this reason, it is suggested to deploy this solution at the access layer.

• DHCP Snooping + DAI

Here we will take the configurations on SW4 as the example, and the configurations on SW5-SW7 are completely the same. On SW4, assuming that ports connecting with PC1, PC2 and SW2 are Fastethernet0/1, Fastethernet0/2 and Fastethernet0/3 respectively.

Globally enable DHCP Snooping;

```
configure terminal
ip dhcp snooping
end
```

When DHCP server and DHCP client are not on the same subnet, DHCP relay must be enabled and the address of DHCP server must be configured;

```
configure terminal
service dhcp
ip helper-address 192.168.1.100
end
```

Configure the port connecting with valid DHCP server as trusted port and ports connecting with users as untrusted ports;

```
configure terminal
interface fastethernet 0/3
ip dhcp snooping trust
end
```

To prevent user from accessing network with the privately configured IP address, address binding must be enabled on the interface to implement hardware filtering of invalid IP packets;

```
configure terminal
interface range fastethernet 0/1-2
ip dhcp snooping address-bind
end
```

For users intending to use static IP addresses, static bindings can be added (assuming that PC2 needs a static IP address, with MAC address being 00d0.fa88.5687, VLAN ID being 1, IP address being 192.168.11.3, and port number being 2)

```
configure terminal

ip dhcp snooping binding 00d0.fa88.5687 vlan 1 ip 192.168.11.3 interface fastethernet 0/2

end
```

DAI implements control function based on VLAN. When it is needed to filter invalid ARP packets in this VLAN, enable DAI for VLAN 1;

```
configure terminal

ip arp inspection vlan 1

end
```

The uplink port is free from ARP spoofing, and thus should be configured as trusted port (of course, if you are certain that there won't be ARP spoofing on other ports, these port can also be configured as trusted ports, such as the port connecting with a trusted server);

```
configure terminal

interface fastethernet 0/3

ip arp inspection trust

end
```

To avoid high CPU usage caused by submitting excess ARP packets to the CPU, the data rate of ARP packet must be limited on the port connecting with user (such as 20pps);

```
configure terminal

interface range fastethernet 0/1-2

ip arp inspection limit-rate 20

end
```

Currently, although the DHCP Snooping + DAI solution launched by Ruijie Networks can well address the problem of ARP spoofing, the software-based DAI needs to submit all ARP packets to CPU for validity check and may lead to high CPU usage when the device is under ARP attack, thus jeopardizing the normal operation of other protocols.

Conclusion

DHCP Snooping is used to address DHCP security problems and facilitate the implementation of DHCP on the campus network.