Study on Availability and Security of DHCP System In Campus Network

Xiaozhong Chen
School of intelligent equipment and Information Engineering
Changzhou Vocational Institute of Engineering
Changzhou, China
chenxiaozhonghh@163.com

Zhijian Mao
School of intelligent equipment and Information Engineering
Changzhou Vocational Institute of Engineering
Changzhou, China
zjmao@email.czie.net

Abstract *—To improve the availability and the security of DHCP system in campus network, the DHCP protocol and the typical fault cases are analyzed, and the three deploy strategies are developed to help the DHCP deployment. Firstly, planning the network addresses properly to prevent the confliction; Secondly, managing the server uniformly with the relay devices; Lastly, implementing the authentication to shield the illegal server. The experiment results show that the strategies are effective for enhancing the availability and security of the DHCP system.*

Keywords: DHCP service; availability; security strategy; campus network

I. INTRODUCTION

With the fast development of the network, more and more clients needs an IP address to link Internet, it is not possible to assign the addresses by manual method in large scaled networks. DHCP (Dynamic Host Configuration Protocol) [1] can uniformly achieve the management of IP address and TCP/IP (Transmission Control Protocol/Internet Protocol) configuration, solving the lack of IP address, and avoiding the unnecessary conflict. As a part of the TCP/IP architecture, DHCP is built on a C/S model by using UDP (User Datagram Protocol). The various clients, such as PCs and mobile terminations, request TCP/IP configuration information from the server, then the server assign the addresses to hosts in centralization. Therefore, DHCP service is widely deployed to release the administrator workload of address planning, management and maintenance in large scaled networks, and plays an increasingly important role in many campus networks.

In view of the importance of DHCP, the high-availability and security must be improved better to ensure the IP address allocation of clients [2-3]. Network security issues have become increasingly prominent, and the DHCP system is also facing serious security threats. Moreover, the unauthorized server in the DHCP system may provide wrong configuration information to clients, resulting in a DoS (Denial of Service) attack. On the other hand, the unauthorized client may disguise as a legitimate one to access the network configuration information from the DHCP server, and the server must check the validity of the client to prevent the illegal client from the misappropriation of DHCP service. In this study, we describe typical faulty deployments of DHCP service, analyze the corresponding risk, and point out the improving approaches to reinforce the system in the campus network.

II. RELATED BACKGROUND KNOWLEDGE

Based on BOOTP (Bootstrap Protocol), DHCP is added the capability of automatic allocation of reusable network addresses and additional configuration options [4].

DHCP is located in the application layer, and uses UDP as its transport protocol (*Tab. 1*). DHCP messages from a client to a server are sent to the port (67), and DHCP messages from a server to a client are sent to the port (68). A server with multiple network address may use any of its network addresses in outgoing DHCP messages [5].

TABLE I. POSITION OF DHCP IN TCP/IP ARCHITECTURE

Application Layer	DHCP
Transport Layer	UDP
Network Layer	IP
Data-link Layer	N/A
Physical Layer	N/A

A. *DHCP structure*

DHCP server has at least one IP address pool, when any client logins into the network, it can lease one address for communication (*Fig. 1*). While the address is no longer in use, it will be put back into the pool for the later lease [1]. To ensure all hosts with the correct configurations is a quite difficult task, especially for the dynamic networks with roaming user and notebook computer. Therefore, a mechanism to simplify the IP address configuration is needed for the centralized management. The DHCP service has the following two advantages.

Fig. 1. *Structure of DHCP system*

Reduce the errors. By deploying DHCP, the errors of manual configuration can be reduced to a minimum. For example, the conflict caused by assigning the assigned IP address to another host will be greatly reduced.

Simplify the network management. The TCP/IP configuration is centralized and automated. The administrator needs not to manually configure the network, and can focus on

the configuration information of global and special subnets. Using the DHCP option functions can automatically allocate all range of additional configuration values to clients. When a host is moved to a new subnet, it is assigned with a new IP address automatically.

B. Packet format

Based on the packet format of BOOTP, only a 1-bit flag is added to describe the packet format of DHCP. However, to allow different interactions with the server, extra options are added to the option field [6]. The new fields are as follows:

Flag. A 1-bit flag is added to the packet to let the client specify a forced broadcast reply from the server. If the reply is to be unicast to the client, the destination IP address of the IP packet is the address assigned to the client.

Options. Several options are added into the list of options. One option, with the value 53 for the tag subfield, is used to define the type of interaction between the server and the client, that is, DISCOVER, OFFER, REQUEST, DECLINE,ACK, NAK and RELEASE.

C. Transition states

The client transitions states from one to another according to the messages it receives or sends, *Fig.2* shows the state machine of DHCP [6].

Initializing State. In the initializing state (the client starts), the client broadcasts a DHCPDISCOVER message using port 76.

Selecting State. After broadcasting the DHCPDISCOVER message, the client goes to the selecting state. The servers reply with a DHCPOFFER message in which the servers offer an IP address and lease duration. The client chooses one of the offers and sends a DHCPREQUEST message to the selected server and goes to the requesting state.

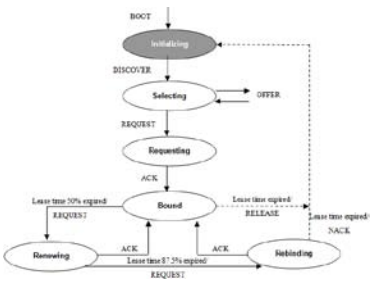

Fig. 2. *DHCP transition diagram*

Requesting state. The client remains in the requesting state until it receives a DHCPACK message from the server which creates the binding between the client MAC address and IP address.

Bound state. After receiving the DHCPACK, the client goes to the bound state in which the client can use the IP address until the lease expires. When 50 percent of the lease period is reached, the client sent another DHCPREQUEST to ask for renewal.

Renewing State. The client remains in this state until it receives a DHCPACK. If the client receives a DHCPACK massage, the client resets the timer and goes back to the bound state. Otherwise, 87.5 percent of the lease time expires, the client goes to the rebounding state.

Rebounding State. The client remains in the rebinding state until one of three events happens. If the client receives a DHCPNACK or the lease expires, it goes back to the initializing state and tries to get another IP address. If the client receives a DHCPACK it goes to the bound state and resets its timer.

III. THE ANALYSIS OF THE TYPICAL FAULT CASES

In this section, the typical faults in the DHCP management are described, and corresponding methods are proposed to troubleshoot the faults in details. In order to understand the current status of the network for the administrator, the packet capture and analysis tools, such as sniffer [7] and wireshark [8], play an important role in the management. In the following parts, typical case are summarized, analyzed, and the each solution is presented.

Case 1. No discovery of server

- Description

All of the clients can not get the IP address.

- Analysis

Capture the packet passing though the adapter of client, and filter the DHCP packets. If there are only DHCPDISCOVERY packets sending from the client, there no DHCPOFFER message, it means that the client can not communicate with the server or there is no DHCP server in the network.

- Solution

Step 1. Check the status of the DHCP service. Login on to the server, check whether the DHCP service is on, and ensure the DHCP pool and its addresses to be right.

Step 2. Check the connectivity between the client and the server. First, check the physical link between the client and the server. Then, check the routing table from the server to the client on the connecting devices (such as routers and Layer 3 switches).

Step 3. Check the DHCP relay [9] configuration. Relay can forward the broadcast from one subnet to another one. If the clients and the server are not in the same subnet, the relay must to be configured at the Layer 3 devices.

Case 2. Partial clients get no address

- Description: Some clients can get IP address and work well, while others can not obtain the address.
- Analysis: Some clients can work properly means that the DHCP server service is work well. There are two reason to cause some clients can not get address. The first one is that because that the pool or the addresses of pools is not enough, when the all the addresses are assigned, the server can not support address to the later

clients. The second reason is that the lease period is unreasonable. If the period is too long, some IP addresses used by offline clients can not recover in time, the server have no more IP addresses to lease, as a result, some client can not link to the network.

- Solution: Preparing more addresses. The number of the addresses must more than the number of clients. Shortening the duration of the lease rather than using the default. DHCP lease time can not be too short.

Case 3. Client get the wrong address

- Description

Some or all clients can get IP address and work well, but the addresses are illegal.

- Analysis

The clients have obtained the IP addresses provided by illegal servers. One of two events happens: another DHCP service is open on another device with wrong operations; the hacker or the computer viruses are attacking the network.

- Solution

Deploy network security policies (such as configuration of the Layer 2 switch port security and DHCP snooping) to quarantine the illegal one.

IV. EXPERIMENTS AND DEPLOY STRATEGIES FOR IMPROVING DHCP SYSTEM

In this section, a typical campus network is constructed in CISCO Packet tracer [10] to explain how to improve the availability and security of DHCP system (*Fig.3*). The deployment strategy consists of the design of address pool, DHCP relay and DHCP snooping, which will be expounded in details as follows.

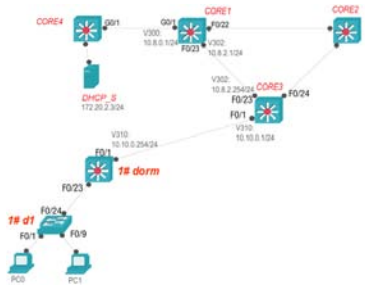

Fig. 3. *DHCP topology*

A. Address pool design

TABLE II. POOLS FOR THE CLIENTS OF DORM SUBNET

Pool Name	Default Gateway	Start IP	Subnet Mask	DNS Server	Max Num
1Pool	172.16.0.254	172.16.0.1	255.255.255.0	172.20.2.2	200
2Pool	172.16.4.254	172.16.4.1	255.255.255.0	172.20.2.2	200

The address pools are designed to assign the addresses to the clients in dorms. Each pool must include the parameters: pool name, start IP, subnet mask, max number, default gateway and DNS server, as shown in *Tab. 2*.

Construct the network basic platform. Configure the routing (such as OSPF) to ensure the connective of the link " DHCP_S-CORE4-CORE1-CORE3-1#dorm" (*Fig. 3*).

Enable the DHCP service the DHCP server (DHCP_S) which IP is 172.20.2.3/24, and configure the pools.

The DISCOVET stage. When the PC0 attempts to get IP address, it broadcasts the DISCOVER message with the destination address FFFF.FFFFF.FFFF in Layer 2 to find the server.

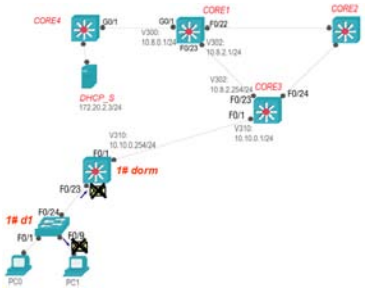

Fig. 4. *Drop the broadcast*

The broadcast is drop at the Layer 3 switch 1#dorm (*Fig. 4*), because of no relay device.

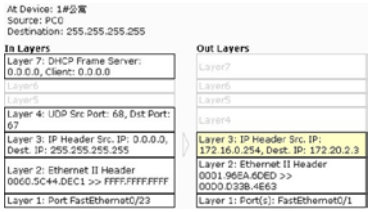

Fig. 5. *Discover with relay address*

B. DHCP relay deployment

To solve the problem that broadcast can not pass through the Layer 3 device, the relay device must be deployed to transform the broadcast into the unicast which destination address is 172.20.2.3. In 1#dorm, the configuration is:

ip help-address 172.20.2.3

After being designed the relay IP address, the DISCOVER message can be sent to the server, as shown in *Fig. 5*, the destination MAC address and IP address are 00D0.D33B.4E63 (the MAC of F0/1 of CORE3) and 172.20.2.3, respectively.

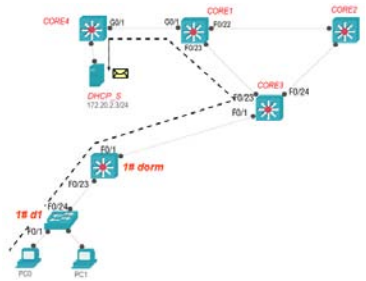

Fig. 6. *Send Discover to the server*

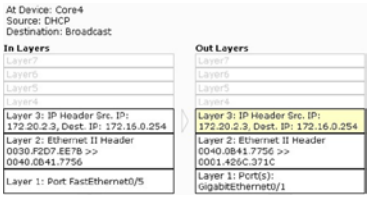

Fig. 7. *Packet structure of OFFER*

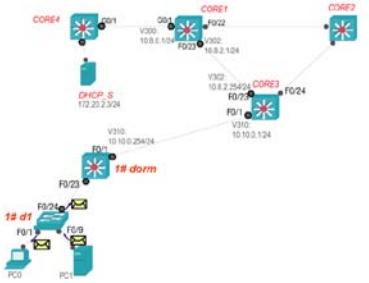

Fig. 8. *Configuration of DHCP pools*

As shown in *Fig.6*, the discovery is sent to the server successfully, and DHCP_S (the server) sends the Offer message to PC0 (*Fig. 7*).

C. Authentication of DHCP server

Authentication can shield the illegal server to assign address to the clients [11]. As shown in *Fig. 8*, PC1 enable the DHCP service with wrong operation, and have a default IP pool including the 192.168.0.0/24 network. It sends OFFER message to the PC0, then PC0 get the IP address which prefix is 192, not 172, that is, the client gets the illegal IP address.

Snooping is an effective method to solve the above problem to improve the security. By establishing and maintaining the binding table, the switch can filters the un-trusted DHCP information. After the DHCP Snooping service is opened, the switch can monitor the messages, and extracts and records the IP address and MAC address information from the received Request or the ACK messages. In addition, the snooping allows a physical port set as a trust port which normally receives and retransmits the OFFER message, while the un-trusted port will discard the message.

In this way, the switch can achieve the shielding of fake DHCP server to ensure that the client gets the address from the legal server.

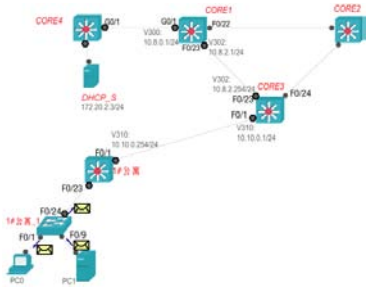

Fig. 9. *Configuration of trust ports*

In *Fig.9*, the circular port and the hexagonal port are the un-trusted and trusted ports, respectively. The snooping is configured in the devices (1#d1, 1#dorm, CORE_1, CORE_3 and CORE_4) as follows:

1#d1 (config)# ip dhcp snooping

1#d1 (config)#ip dhcp snooping vlan 100

1#d1 (config)#interface fastethernet 0/24

1#d1 (config-if)#ip dhcp snooping trust

1#d1 (config-if)#ip dhcp snooping limitrate 100

1#dorm (config)# ip dhcp snooping

1#dorm (config)# ip dhcp snooping vlan 100

1#dorm (config)#interface fastethernet 0/1, fastethernet 0/23

1#dorm (config-if)#ip dhcp snooping trust

1#dorm (config-if)#iip dhcp snooping limitrate 100

CORE_4 (config)# ip dhcp snooping

CORE_4 (config)#ip dhcp snooping vlan 100

CORE_4 (config)#interface gigabitEthernet 0/5, fastethernet 0/23

CORE_4 (config-if)#ip dhcp snooping trust

The configuration of CORE_1 and CORE_3 is similar to CORE_4.

V. CONCLUSION

Base on the analysis of security problems and typical faults of DHCP, the strategy of design and deployment of DHCP system in campus network is proposed to improve the availability and security of DHCP system , including address planning, safety protection. The summarized conclusions are as follows:

1. The three typical fault cases of the DHCP system were summarized and analyzed the each reason, and the corresponding solutions were proposed.

2. The availability and security strategies were suggested, and their effectiveness were verified through the experiments. Those strategies may be used as the theory and practice guidance of DHCP system in campus network deployment.

VI. REFERENCES

[1] R. Droms, Dynamic Host Configuration Protocol, RFC 2131, 1997.

[2] JH. Wang and TL .Lee, “Enhanced intranet management in a DHCP-enabled environment”, Computer Software and Applications Conference Vol.12, 2002, pp. 893-897.

[3] CJ. Park, SJ Ahn, JW. Chung, CH. Lee and CS. Park, “The improvement for integrity between DHCP and DNS”, High Performance Computing on the Information Superhighway, Vol.8, 2002, pp. 511-512.

[4] Bootstrap Protocol (BOOTP), RFC 951, 985.

[5] S.Andrew and Tanenbaum, Computer Networks, Fourth Edition, ISBN 7302089779.

[6] Forouzan, A.Behrouz and Forouzan, “TCP/IP Protocol Suite (Third Edition)”, McGraw-Hill Higher Education , 2009.

[7] Sniffer, http://www.sniffer.net/.

[8] Wireshark, https://www.wireshark.org/.

[9] Link Selection sub-option for the Relay Agent Information Option for DHCPv4, RFC3527, 2003.

[10] CISCO Packet tracer, http://cisco.netacad.net/

[11] J. Demerjian, A.Serhrouehni, “DHCP authentieation using certificates”, 19th IFIP International Information Security Conference, France, 2004.