DOI:10. 13876/J. cnki. ydnse. 2018. 01. 034

# 基于 Wireshark 的 DHCP 网络故障定位分析

辛伟伟[1],郝继升[1*],张 成[2]

(1. 延安大学 数学与计算机科学学院,陕西 延安 716000;
2. 西安医学院,陕西 西安 710021)

**摘 要**:针对在一个网络中出现多个 DHCP(动态主机配置协议)服务器时,导致 Client(客户端)的网络故障,分析了在 eNSP(企业网络仿真平台)上模拟 DHCP 服务器为客户端动态分配 IP 地址的过程,并利用 Wireshark(网络封包分析软件)工具捕获和分析 DHCP 数据包来定位网络故障。

**关键词**:DHCP 协议;eNSP 模拟器;Wireshark 软件;交换机

**中图分类号**:TP393 **文献标识码**:A **文章编号**:1004 - 602X(2018)01 - 0034 - 03

随着 Internet 的飞速发展,越来越多的设备接入互联网。这些设备在网络中要实现通信,就需要给每个设备配置一个 IP 地址、子网掩码、网关地址和 DNS(域名解析系统)[1]。为方便用户快速地接入和退出网络、提高 IP 地址资源的利用率和管理效率,DHCP 协议应运而生。DHCP(动态主机设置协议)是一个局域网的网络协议,采用客户/服务器(C/S)架构,使用 UDP 协议工作,主要用于动态指派 IP 地址给 DHCP 客户端以及便于网络管理员对所有计算机的管理[2]。eNSP(企业网络仿真平台)是一款由华为提供的免费的、可扩展的、图形化操作的网络仿真工具平台[3],主要针对企业网路由器、交换机等网络设备进行硬件模拟,完美呈现真实设备实景,让用户有机会在没有真实设备的情况下模拟网络环境、学习网络技术和分析网络故障。Wireshark(前身为 Ethereal)是一个免费开源的网络数据包分析软件[4]。它的功能是抓取网络数据包,并尽可能显示出最为详细的网络数据包数据。

本文主要分析了在一个网络中出现多台 DHCP 服务器时,客户端如果获取到伪 DHCP 服务器分配的 IP 地址,将无法正常连接网络资源。本文使用 eNSP 仿真软件模拟网络环境[5],搭建两台 DHCP 服务器的简单网络环境,并利用 Wireshark(网络封包分析工具)软件抓取和分析 DHCP 数据包来定位网络故障。

## 1 模拟实验过程

### 1.1 搭建实验模拟环境

使用 eNSP 网络仿真软件,分别搭建一台主 DHCP 服务器,一台伪 DHCP 服务器,一台交换机和两台 PC 客户端,如下图 1 所示:

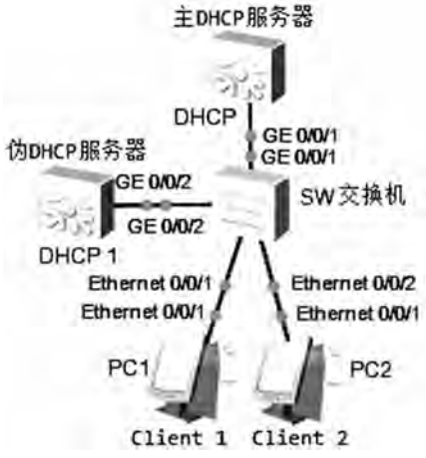


图 1 实验模拟的网络拓扑结构

**收稿日期**:2018 - 01 - 12

**基金项目**:陕西省高水平大学建设专项资金资助项目(2012SXTS06);延安市科技局项目(2014ZC - 6)

**作者简介**:辛伟伟(1984 - ),男,陕西清涧人,延安大学硕士研究生。 * 通讯作者

### 1.2　分别配置两台 DHCP 服务器

在这里使用支持三层网络协议的交换机模拟 DHCP 服务器，并在 vlan1 接口下启用 DHCP 功能，具体配置命令如下：

[DHCP]dhcp enable #启用 DHCP 功能

[DHCP]vlan 1 #默认 vlan1

[DHCP - vlan1]description DHCP Server

#命名为 DHCP Server

[DHCP]interface GigabitEthernet 0/0/1

#接口 1 配置

[DHCP - GigabitEthernet0/0/1]port link - type access #配置接口 1 类型为 access

[DHCP - GigabitEthernet0/0/1]port default vlan 1 #接口 1 加入 vlan1

[DHCP - Vlanif1]ip address 10.0.0.1 24

#配置 IP 地址用作 DHCP 服务器地址

[DHCP - Vlanif1]dhcp select interface

#DHCP 选择接口模式

[DHCP - Vlanif1]dhcp server domain - name DHCP.com

#DHCP 服务器配置域名

[DHCP - Vlanif1]dhcp server dns - list 10.0.0.2

#DHCP 服务器配置主 DNS

[DHCP - Vlanif1]dhcp server nbns - list 10.0.0.3

#DHCP 服务器配置备用 DNS

[DHCP - Vlanif1]dhcp server excluded - ip - address 10.0.0.2 #DHCP 地址池排除该地址

[DHCP - Vlanif1]dhcp server excluded - ip - address 10.0.0.3 #DHCP 地址池排除该地址

[DHCP - Vlanif1]dhcp server netbios - type b - node #NetBios 类型为广播节点

[DHCP - Vlanif1]dhcp server lease day 5

#DHCP 服务器的租约期 5 天

通过上面的配置，模拟的主 DHCP 服务器就架设完成，同理配置伪 DHCP 服务器，伪 DHCP 服务器的 vlan1 接口地址改为 192.168.1.1/24，如下图 2 所示：

```
interface Vlanif1
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
 dhcp server excluded-ip-address 192.168.1.2 192.168.1.3
 dhcp server lease day 10 hour 0 minute 0
 dhcp server dns-list 192.168.1.2
 dhcp server netbios-type b-node
 dhcp server nbns-list 192.168.1.3
 dhcp server domain-name DHCP-1.com
```

图 2　伪 DHCP 服务器配置

### 1.3　配置交换机

这里选用的交换机是支持二层网络协议交换机，它属于数据链路层设备，可以识别数据包中的 MAC 地址信息，根据 MAC 地址进行转发，并将这些 MAC 地址与对应的端口记录在自己内部的一个地址表中[5]。具体配置命令如下：

[Huawei]sysname SW #命名交换机为 SW

[SW]port - group group - member GigabitEthernet 0/0/1 to GigabitEthernet 0/0/2 Ethernet 0/0/1 to Ethernet 0/0/2

#将连接的 4 个接口加入端口组统一配置

[SW - port - group]port link - type access

#将连接的 4 个接口统一配置为 access

[SW - port - group]port default vlan 1

#将连接的 4 个接口统一配置为 vlan1

### 1.4　利用 Wireshark 抓取并分析数据包

配置模拟的两台 Client 为自动获取 IP 地址和 DNS 服务器，分别在两台 Client 上执行 ipconfig/release、ipconfig/renew 命令释放已有的 IP 地址并重新获取新的 IP 地址。如果 client 获取的 IP 地址是 10.0.0.0 网段就可以访问网络资源，获取的 IP 地址是 192.168.1.0 网段就访问不了网络资源。

这里以 Client1 为例，在命令行窗口中，执行以上两条命令，Client1 上释放之后的 IP 地址全为 0，执行两次 ipconfig/renew 命令之后 Client1 获取的两个 IP 地址不在同一网段，第一次获取的 IP 地址是 192.168.1.253，子网掩码是 255.255.255.0，默认网关是 192.168.1.1，主备 DNS 分别为 192.168.1.2 和 192.168.1.3；第二次获取的 IP 地址是 10.0.0.254，子网掩码是 255.255.255.0，默认网关是 10.0.0.1，主备 DNS 分别为 10.0.0.2 和 10.0.0.3。获取地址的同时在交换机 SW 的 Ethernet0/0/1（Client1 连接主交换机的端口）接口处开启数据捕获[6]，并在 Wireshark 里以“BOOTP”为过滤表达式来添加新的过滤规则（BOOTP 协议是 DHCP 协议的前身，在 Wireshark 中，使用 BOOTP 表达式可以过滤出 DHCP 的数据包）[7]。点击 Start Capture 按钮开始抓取数据包，如图 3 所示。

从图 3 中可以看出在抓包的过程中有两个 DHCPoffer 数据包和两个 DHCPACK 数据包[8]，也就是说网络中同时有两个 DHCP 服务器在响应 Client1 的 IP 广播请求，很容易看出源 IP 地址为 192.168.1.1 的 DHCP 服务器就是要找出的伪 DHCP 服务

器,对应的 DHCP 服务器的 MAC 地址为 4C:1F:CC:A4:5B:E7[9],得到 MAC 地址后就可以在交换机用 displa ymac – address 命令查出对应的端口号,如下图 4 所示,MAC 地址 4C:1F:CC:A4:5B:E7 对应的交换机端口号是 GE0/0/2,定位到交换机端口后找出并关闭伪 DHCP 服务器或者在交换机上执行 shutdown 命令将 GE0/0/2 接口关闭即可。

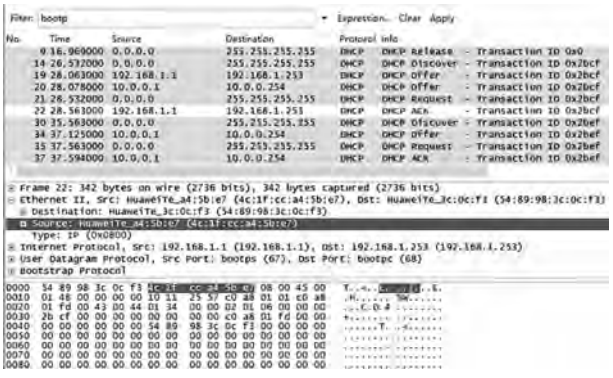


图 3 Wireshark 抓取数据包

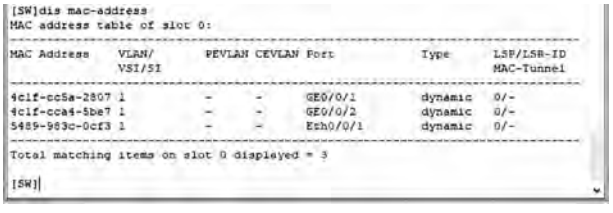


图 4 交换机的 MAC 地址表项

## 2 结论

本文用 eNSP 网络仿真软件模拟 DHCP 网络故障,利用 Wireshark 抓包、分析、定位到 DHCP 服务器,并通过查找线缆标签定位或者关闭交换机端口的方法解决 DHCP 网络故障。DHCP 确实给网络的管理提供了便利,但是当一个网络中出现多个 DHCP 服务器时,会给网络的管理带来很大的不便,可以尝试使用本文的方法来解决故障。

**参考文献:**

[1]张萌雨,胡曦明,马苗. DHCP 及其发展研究[J]. 网络安全技术与应用,2017(7):33 – 35.

[2]高晓红,王超,杨佳. 路由器 DHCP 协议配置在 PacketTracer 环境下的仿真实现[J]. 电脑知识与技术,2014,10(22):5178 – 5179 + 5181.

[3]冯思泉. eNSP 和 WireShark 在防火墙课程教学改革中的应用[J]. 时代教育,2014(12):116.

[4]赵北庚. 基于 Wireshark 的 DHCP 协议工作流程研究[J]. 电脑编程技巧与维护,2015(8):87 + 114.

[5]孟祥成. 基于 eNSP 的二层 VLAN 虚拟仿真实验[J]. 实验室研究与探索,2017,36(9):102 – 106.

[6]郭振勇,沈昌海. H3C 交换机 VLAN 配置实现[J]. 黑龙江科技信息,2013(16):146.

[7]朱煜. 用 Wireshark 解决网络故障[J]. 山西电子技术,2016(4):59 – 60 + 96.

[8]林沛满. Wireshark 网络分析就这么简单[M]. 北京:人民邮电出版社,2014.

[9]罗青林,徐克付,臧文羽,等. Wireshark 环境下的网络协议解析与验证方法[J]. 计算机工程与设计,2011,32(3):770 – 773.

[责任编辑 毕 伟]

# Analysis of DHCP Network Fault Location Based on Wireshark

XIN Wei-wei[1], HAO Ji-sheng[1*], ZHANG CHENG[2]

(1. College of Mathematics and Computer Science, Yan′an University, Yan′an 716000, China;
2. Xi′an Medical College, Xi′an 710021, China)

**Abstract**: In this paper, in order to solve client network failure when more then one DHCP (Dynamic Host Configuration Protocol) servers occur in a network, the process of simulating DHCP server to dynamically assign IP address to client on eNSP (Enterprise Network Simulation Platform) was analyzed, and the Wireshark (Network packet analysis software) tool was used to capture and analyze DHCP packet in order to locate network failure.

**Key words**: DHCP protocol; eNSP simulator; Wireshark software; switch