# DHCP Failover 研究与实验设计①

刘志雄[1], 朱向庆[2]

[1](广州商学院 网络中心, 广州 511363)
[2](嘉应学院 电子信息工程学院, 梅州 514015)

**摘 要**: DHCP 服务广泛应用于大型网络架构中, 为部署安全、可靠的 DHCP 服务器, 通过对 Failover 协议的研究, 设计基于 LINUX 环境下 DHCP Failover 应用服务器实验. 介绍 DHCP Failover 服务器的实验配置, 网络安全配置及实验结果验证等. 实践证明, DHCP 服务器的灾难备份有效地保证用户网络的稳定性, 提高 IP 资源的使用效率.

**关键词**: DHCP 服务器实验; DHCP Failover; 数据包分析

## Research on DHCP Failover and Its Experimental Design

LIU Zhi-Xiong[1], ZHU Xiang-Qing[2]

[1](Guangzhou College of Commerce, Guangzhou 511363, China)
[2](School of Electronic & Information Engineering, Jiaying University, Meizhou 514015, China)

**Abstract**: DHCP services are widely used in large-scale network infrastructure. In order to setup secure, reliable DHCP Server, the authors study the Failover protocol and design experiment on the application of DHCP Failover Server based on the LINUX environment. This paper describes in detail the configuration of DHCP Failover Server in the experiment, network security configuration and the verification of experimental results. The experiment shows that a disaster backup of DHCP Server effectively ensures the stability of users' network and improves the efficient in the use of IP resources.

**Key words**: DHCP server experiment; DHCP Failover; data envelopment analysis

随着网络的扩大以及移动办公的逐步增加, 为了便于管理 IP 地址, DHCP(Dynamic Host Configuration Protocol, 动态主机配置协议)得到了广泛应用[1]. 作为一种核心的网络服务, 要求其具有高稳定性和高灵活性. 如果 DHCP 服务功能出现问题, 将导致用户接入和用户认证无法完成, 严重影响网络的使用. 因此, 为了保证 DHCP 服务的可用性和可靠性. 应该采取相应的冗余策略和负载均衡策略. 传统的简单冗余实现, 往往会带来 IP 地址不一致, 无法实现在线切换等问题. 目前 DHCP Failover(灾难备份)应用技术, 解决了这一难题, 实现了 DHCP 服务器负载均衡, 共享 IP 地址信息数据库, 在实践中得到了很好的应用. 为了让网络专业学生或技术人员, 能够更好的应用 DHCP Failover 协议, 动手构建安全、可靠、高效的 DHCP 服务, 设计了基于 RFC 2131 工作机制的 DHCP 服务器灾难备份实验.

## 1 DHCP工作流程

DHCP 是一种使网络管理员能够集中管理和自动分配 IP 网络地址的通信协议. 当某台计算机移到网络中的其它位置时, 能自动收到新的 IP 地址. DHCP 运行分为四个基本过程, 分别为: 请求 IP 租约、提供 IP 租约、选择 IP 租约和确认 IP 租约, 如图 1 所示. DHCP 统一使用两个分配的端口: 服务器端使用 UDP 协议 67 端口, 客户端使用 UDP 协议 68 端口. 客户在获得了一个 IP 地址以后, 就可以发送一个 ARP 请求来避免由于 DHCP 服务器地址池重叠而引发的 IP 冲突.

为了更好分析 DHCP 分配 IP 的过程, 通过数据包分析软件 Ethereal, 清晰的跟踪客户机从 DHCP 服务器获取 IP 的全过程(如图 1).

① 收稿时间: 2014-12-15;收到修改稿时间:2015-01-26

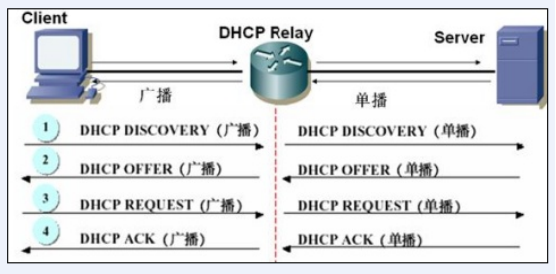


图 1 DHCP 工作流程

## 2 DHCP Failover工作原理

为提高 DHCP 服务器可靠性, 稳定地为客户机分配 IP 地址, ISC (Internet Software Consortium) 提供的开源 DHCP 软件实现了 Failover 功能[2]. RFC 2131 扩展功能是冗余 DHCP 服务器的部署, 它实现主服务器和次服务器同步运行, 以保证冗余度. 它定义了 3 种类型的服务器状态信号: (1)正常(Normal)状态, (2)通信中断 (Communications-Interrupted) 状态, (3)PARTNER-DOWN 状态. 主服务器与次服务器相互监视服务器的状态, 在 Normal 状态下, 二者各自负责客户机的地址分配, 响应所有的 DHCP 消息, 通过相互通信进行地址数据库信息更新, 维护一致的地址池状态, 当某个服务器 Failover 时, 另外一个将自动承担起整个网络的分配管理工作, 而当 failover 服务器重新恢复时, 二者会进行一个地址数据库的同步, 然后继续共同管理. 整个过程都是系统自动切换, 不需任何人工干预, 对用户的网络使用不会造成任何影响.

## 3 DHCP Failover实验设计

### 3.1 实验目的

实验模拟大型企业网络的三层结构设计, 实现 DHCP 主、次服务器负载均衡工作, 共同为不同的子网提供服务, 保持客户端网络配置信息不变.

### 3.2 网络结构的设计

在实验中, DHCP 为不同的子网提供服务, 网络设计采用三层结构[3]: 核心层、汇聚层及接入层, DHCP Failover 服务器组连接在核心交换机上, 在汇聚层交换机上启用 DHCP Relay(中继)功能, 接入层交换机启用非法 DHCP 服务接入安全策略[4], 网络拓朴如图 2 所示.

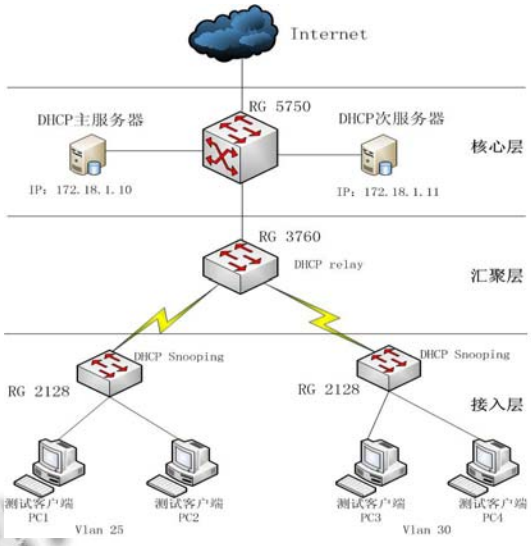


图 2 DHCP Failover 实验网络拓朴

### 3.3 实验环境

1) 软件环境: 使用 Linux redhat as 4 操作系统, 数据包分析软件 Ethereal 0.99.0, DHCP 版本是 dhcp-3.0.1-12_EL.i386.rpm.

2) 硬件环境: 三层交换机锐捷 2 台(核心: RG5750-12SFP, 汇聚: RG3760), 二层接入交换机锐捷(RG2128)1 台, DHCP 服务器 2 台(DELL 4 核至强 CPU, 8G 内存).

### 3.4 实验操作

#### 3.4.1 DHCP Failover 服务器组建立[5]

主服务器和次服务器组成了一对 Failover 工作组, 其地址分别为 172.18.1.10 和 172.18.1.11, 共同管理客户端的网络配置信息. 首先, 主、次服务器上分别接入核心交换机 RG5750, 且安装 DHCP 软件. 其次, 分别对主、次服务器配置, 由于共享地址池信息, 地址池的配置是一致.

(1) 主服务器的主要配置:

```
failover peer "dhcp"   //指定本机所属 failover 域的识别码为 dhcp
{ primary;
address 172.18.1.10;
port 520;
peer address 172.18.1.11;
peer port 519;
max-response-delay 180; //Peer 之间最大无响应时间 180 秒
```

```
max-unacked-updates 20;
mclt 3600; //双机联系中断时所分配的租约时间
split 128; //负载分担比例, 128 为平均分担负载
load balance max seconds 3;
}
# 实验使用子网 IP 分配
subnet 192.168.235.0 netmask 255.255.255.0 {
 option routers 192.168.235.254;
 option subnet-mask 255.255.255.0;
 option nis-domain "scnuzc.cn";
 option domain-name "scnuzc.cn";
 option domain-name-servers 210.39.240.1 , 202.96.128.86;
 option time-offset -18000;
 pool {
 failover peer "dhcp";
 range 192.168.235.1 192.168.235.249;
 deny dynamic bootp clients;
 default-lease-time 259200; //默认租赁时间(秒)
 max-lease-time 432000; //最大租赁时间(秒)
 }
}
……
```

(2)次服务器的主要配置:

```
failover peer "dhcp" {
secondary;
address 172.18.1.11;
port 520;
peer address 172.18.1.10;
peer port 519;
max-response-delay 180; //Peer 之间最大无响应时间 180 秒
max-unacked-updates 20;
……
```

3.4.2 网络配置

(1)核心交换机配置

实验中采用 RG5750-12SFP 用作核心交换机, 在交换机上启用 dhcp 服务. RG5750(config)#service dhcp

另外, 所有设备都能相互访问, 核心交换机上启用 ospf 路由协议[6], 配置如下:

```
interface Vlan 1
ip address 172.18.1.1 255.255.255.240
router ospf
router-id 10.1.1.1
area 0.0.0.0
network 172.18.1.0 255.255.255.0 area 0.0.0.0
network 192.168.0.0 255.255.0.0 area 0.0.0.0
……
```

(2) 汇聚交换机配置

汇聚交换机 RG3760, 由于 DHCP 客户端设备和 DHCP 服务器不再同一广播域内的时候, 中间设备即二三层交换机必须能够转发这种广播包. 则启用 ip helper—address 命令, 实现中继. 具体配置如下:

```
RG3760(eonfig)# service dhcp
interface VLAN 1
no ip proxy-arp
ip address 172.18.1.2 255.255.255.240 //交换机 IP
interface VLAN 25
 no ip proxy-arp
 ip helper-address 172.18.1.10 //启用 DHCP 中继
 ip helper-address 172.18.1.11 //启用 DHCP 中继
 ip address 192.168.235.254 255.255.255.0
router ospf 1 //启用路由
router-id 10.1.1.8
network 172.18.1.0 0.0.0.255 area 0.0.0.0
network 192.168.0.0 0.0.255.255 area 0.0.0.0
```

(3) 接人层交换机的配置

为了使用户能通过合法的 DHCP 服务器获取 IP 地址. 使用 DHCP Snooping 安全机制过滤非法 IP[7]. 将连接合法 DHCP 服务器的端口或者连接汇聚交换机的上行端口设置为信任端口, 通常为连接终端设备的端口(如 PC, 网络打印机等)设置为非信任端口.

接入层设备 RG2128 配置如下:

```
Swith(config)# ip dhcp snooping
interface GigabitEthernet 0/12 //该设备的上联口
ip dhcp snooping trust //该端口设置成信任端口
 ip arp inspection trust //防止 ARP 攻击
interface GigabitEthernet 0/1
 switchport access vlan 25
 ip arp inspection limit-rate 30
interface GigabitEthernet 0/2
 switchport access vlan 25
 ip arp inspection limit-rate 30
```

……

## 4 实验结果测试

### 4.1 启动 DHCP 服务

主、次服务器依次启动 dhcp 服务, 执行 service dhcpd start 命令, 图 3 是主服务服务器的运行状态, DHCP 已正常运行, 与次服务器 172.18.1.11 建立了 Failover 组.

```
[root@localhost ~]# netstat -anutp | grep dhcpd
tcp        0      0 172.18.1.10:519             0.0.0.0:*                   LISTEN      26245/dhcpd
tcp        0      0 172.18.1.10:32771           172.18.1.11:520             ESTABLISHED 26245/dhcpd
udp        0      0 0.0.0.0:67                  0.0.0.0:*                               26245/dhcpd
```

图 3 DHCP 服务器运行状态

### 4.2 测试服务器 Failover 组正常工作时, DHCP 工作情况及 IP 租约信息是否同步更新.

(1) 在接入交换机(RG2128)端口 1 或 2 可以接入 PC 机, 然后运行 ipconfig/release 命令, 再执行 ipconfig /renew 命令, 可以正常获取到 IP 地址. 如图 4 所示, 通过数据包分析软件可出详细分析客户端 IP 的分配过程[8].

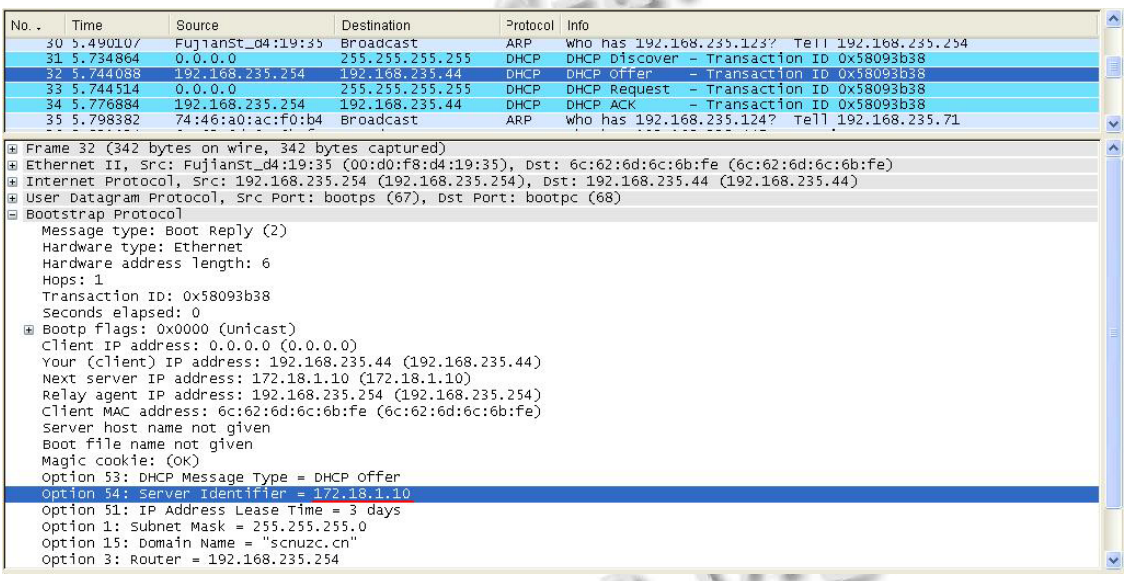


图 4 主服务器分配 IP 的数据包分析

(2) 如图 5 所示, DHCP 服务器分别记录 IP 租约信息, 通过命令 cat /var/lib/dhcp/dhcpd.leases |more 检测到客户端的 IP 租约信息.

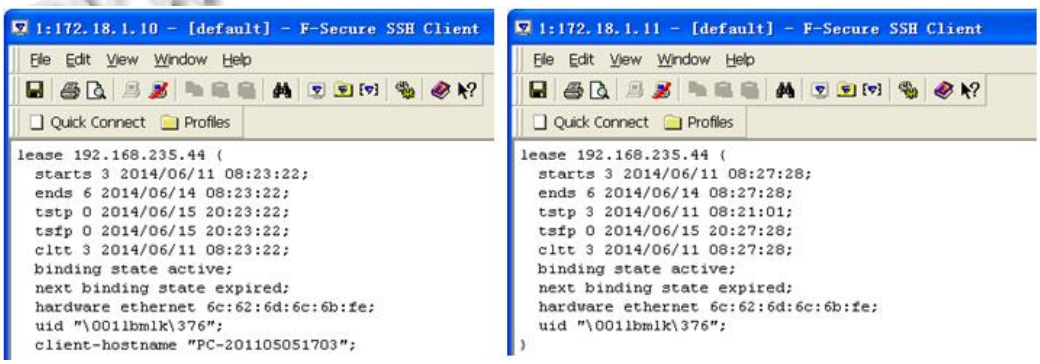


图 5 DHCP Failover 服务器组记录的 IP 租约信息

实验证明, 在主、次服务器正常工作时, Failover 组可以负载均衡的提供 DHCP 服务, 并共管理 IP 地址池等信息, 保持了主、次服务器之间 IP 信息的一致性和同步更新[13].

### 4.3 当主服务器出现故障时, 测试 DHCP Failover 组工作情况.

首先, 主服务器关闭 DHCP 服务, 执行 service dhcpd stop, 模拟主服器故障, 无法提供 DHCP 服务.

其次, 客户端要重新获取 IP 信息. 运行 ipconfig /release 命令, 再执行 ipconfig /renew 命令, 分析客户端获取 IP 信息过程.

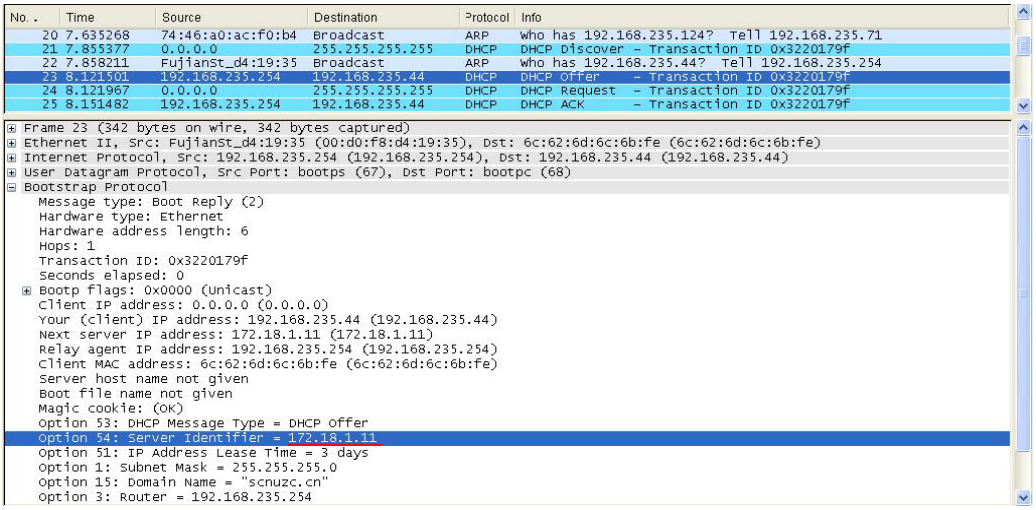


图 6　备份服务器提供 IP 分配

从面的实验测试可以得出, 在主服务器故障时, 由次服务器提供整个网络的 DHCP 服务, 客户端网络配置信息保持不变.

### 4．4 当主服务器恢复正常工作时, 测试 DHCP Failover 组工作情况.

首先, 在主服务器启动 DHCP 服务, 运行命令: service dhcpd restart; 然后, 在客户端运行 ipconfig /release 命令; 再执行 ipconfig /renew 命令, 得到图 7 所示的 IP 信息. 可以看出, 在 Failover 组恢复正常工作并协商后, 恢复各自的 DHCP 服务.

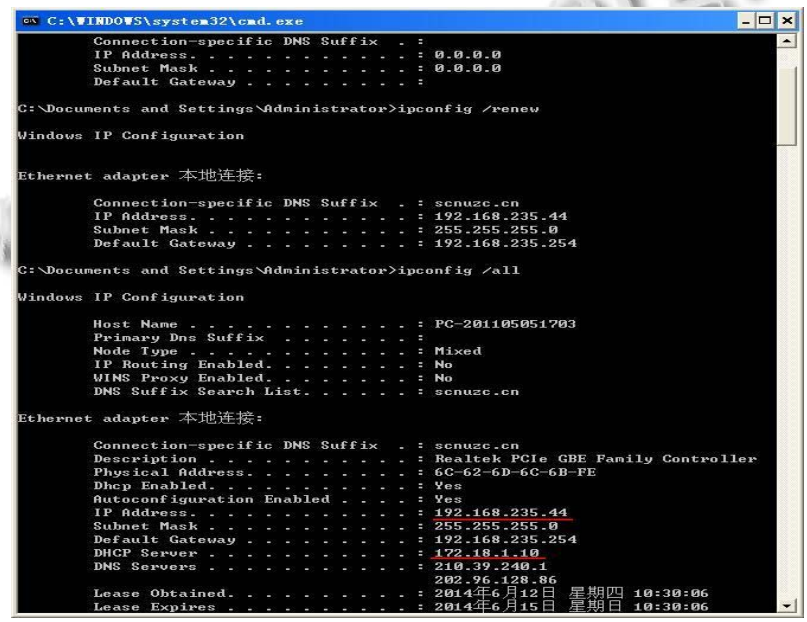


图 7　主服务器恢复 IP 分配

### 4.5 实验结果

实验证明, DHCP Failover 组工作模式下, 实现负载均衡[9]工作, 服务器之间保持通讯, 出现故障时在线切换, 且能共同更新客户端 IP 租约信息, 对用户的使用不造成任何的影响.

## 5 结语

DHCP 技术应用简化了客户端网络配置, 在网络中广泛应用. 因此, 构建高可靠性, 高安全性的 DHCP 服务器具有重要的现实意义. 通过实验的方法, 可以更加清晰分析 DHCP Failover 的技术实现过程, 实验证明, 它能有效地保证了用户网络的稳定性, 减少了网络的人工干预. 为了提高 DHCP 服务器的运行效率, 还需要不断研究和优化, 使 DHCP 服务器能更高效地提供服务[10].

## 参考文献

1 王创社,周树杰,王玮,等.DHCP 在校园网中应用的局限性及解决方案.北京石油化工学院学报,2006,14(2):22–25.

2 林常胜.负载均衡的高可用 DHCP 服务的探索及实践[学位论文].北京:北京邮电大学,2012.

3 李海军,卢清萍.第三层交换技术与 VLAN 在计算机实验室中的应用.实验室研究与探索,2006,25(11):1387–1389.

4 罗江涛.基于 SNOOPING 的安全 DHCP 系统研究与实现[学位论文].西安:西安电子科技大学,2007.

5 李澍,姚磊.实验室搭建复杂网络环境下的 DHCP 服务及安全防护.实验室研究与探索,2014,33(1):143–148.

6 王东.OSPF 路由协议在多区域中的应用.重庆科技学院学报(自然科学版),2010,12(2):172–174.

7 史罕初,彭毓涛.基于 IP DHCP Snooping 的大型局域网安全策略研究.网络安全技术与应用,2009,(11):20–23.

8 王东.Ethereal 工具在园区网络维护中的应用.重庆科技学院学报(自然科学版),2011,13(2):159–160,179.

9 陈建红,王志谦.基于 DHCP 服务器状态的动态负载均衡算法.电视技术,2013,37(23):109–111,121.

10 何智勇,沈苏彬,毛燕琴.DHCP 协议优化方案研究.计算机技术与发展,2010,20(9):5–9.