DHCP服务器配置与管理

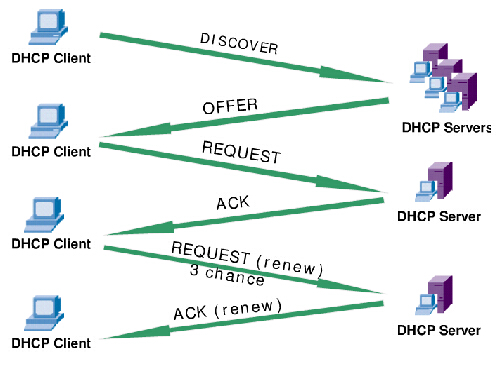
# DHCP服务概述

在tcp/ip网络中要连入互联网，我们的电脑必须要有唯一的ip。它可以动态指定，也可以通过DHCP(Dynamic Host Configuration Protocol动态主机配置协议)获取。它能集中管理IP地址，减轻了TCP/IP网络的管理维护负担。

## DHCP中常用概念

|  |
| --- |
| **DHCP Client**：DHCP客户端，通过DHCP协议请求IP地址的客户端。DHCP客户端是接口级的概念，如果一个主机有多个以太接口，则该主机上的每个接口都可以配置成一个DHCP 客户端。交换机上每个Vlan接口也可以配置成一个DHCP客户端。  **DHCP Server**：DHCP 服务端，负责为DHCP客户端提供IP地址，并且负责管理分配的IP地址。  **DHCP Relay**：DHCP中继器，DHCP客户端跨网段申请IP地址的时候，实DHCP报文的转发功能。  **DHCP Security**：DHCP安全特性，实现合法用户IP地址表的管理功能  **DHCP Snooping**：DHCP监听，记录通过二层设备申请到IP地址的用户信息 |

## 工作原理



### 发现阶段

DHCP客户端寻找DHCP服务端的过程，对应于客户端发送DHCP Discovery，因为DHCP Server对应于DHCP客户端是未知的，所以DHCP 客户端发出的DHCP Discovery报文是广播包，源地址为0.0.0.0**目的地址为255.255.255.255**。网络上的所有支持TCP/IP的主机都会收到该DHCP Discovery报文，但是只有DHCP Server会响应该报文。如果网络中存在多个DHCP Server，则多个DHCP Server均会回复该DHCP Discovery报文。

如果同一个vlan内没有DHCP Server，而该VlanIf配置了DHCP Relay功能，则该Vlanif即为DHCP中继，DHCP中继会将该DHCP报文的源IP地址修改为该Vlanif的IP地址，而目的地址则为DHCP Relay配置的DHCP Server的IP地址。同时修改DHCP报文中，giaddress为VlanIf的IP地址。并以单播将DHCP Discovery发送到DHCP Server端。

### DHCP Server 提供阶段

DHCP Server收到DHCP Discovery报文后，解析该报文请求IP地址所属的Subnet。并从dhcpd.conf文件中与之匹配的subnet中取出一个可用的IP地址(从可用地址段选择一个IP地址后，首先发送ICMP报文来ping该IP地址，如果收到该IP地址的ICMP报文，则抛弃该IP地址，重新选择IP地址继续进行ICMP报文测试，直到找到一个网络中没有人使用的IP地址，用以达到防治动态分配的IP地址与网络中其他设备IP地址冲突，这个IP地址冲突检测机制，可配置)，设置在DHCP Discovery报文中yiaddress字段中，表示为该客户端分配的IP地址，并且为该Lease设置该Subnet配置的Option，例如默认leases租期，最大租期，router等信息。

DHCP从地址池中选择IP地址，以如下优先级进行选择：

* 当前已经存在的Ip Mac的对应关系
* Client以前的IP地址
* 读取Discovery报文中的Requested Ip Address Option的值，如果存在并且IP地址可用
* 从配置的Subnet中选择IP地址：DHCP Server解析DHCP Discovery请求的IP所属的Subnet，首先看该DHCP Discovery报文中giaddress是否有DHCP Relay，如果有，则从giaddress所述的subnet中可用IP地址段中获取，并分配IP。如果giaddress没有IP地址，则从该DHCP Server绑定的接口的IP地址所属的网段分配IP地址。

### DHCP Client 选择阶段

DHCP Client收到若干个DHCP Server响应的DHCP Offer报文后，选择其中一个DHCP Server作为目标DHCP Server。选择策略通常为选择第一个响应的DHCP Offer报文所属的DHCP Server。

然后以广播方式回答一个DHCP Request报文，该报文中包含向目标DHCP请求的IP地址等信息。之所以是以广播方式发出的，是为了通知其他DHCP Server自己将选择该DHCP Server所提供的IP地址。

### DHCP Server确认阶段

当DHCP Server收到DHCP Client发送的DHCP Request后，确认要为该DHCP Client提供的IP地址后，便想该DHCP Client响应一个包含该IP地址以及其他Option的报文，来告诉DHCP Client可以使用该IP地址了。然后DHCP Client即可以将该IP地址与网卡绑定。另外其他DHCP Server都将收回自己之前为DHCP Client提供的IP地址。

### DHCP Client重新登录网络

当DHCP Client重新登录后，发送一个以包含之前DHCP Server分配的IP地址信息的DHCP Request报文，当DHCP Server收到该请求后，会尝试让DHCP客户端继续使用该IP地址。并回答一个ACK报文。

但是如果该IP地址无法再次分配给该DHCP Client后，DHCP回复一个NAK报文，当DHCP Client收到该NAK报文后，会重新发送DHCP Discovery报文来重新获取IP地址。

### DHCP Client更新租约

DHCP获取到的IP地址都有一个租约，租约过期后，DHCP Server将回收该IP地址，所以如果DHCP Client如果想继续使用该IP地址，则必须更新器租约。更新的方式就是，当当前租约期限过了一半后，DHCP Client都会发送DHCP Renew报文来续约租期。

# DHCP安装与启动

|  |
| --- |
| #安装  yum -y install dhcp  #启动  service dhcpd restart/stop/start/status |

# DHCP服务器和客户端配置

## 配置解析

|  |
| --- |
| #主配置文件/etc/dhcp/dhcpd.conf  #模板配置文件：/usr/share/doc/dhcp-4.1.1/dhcpd.conf.sample  cp /usr/share/doc/dhcp-4.1.1/dhcpd.conf.sample /etc/dhcp/dhcpd.conf  vi /etc/dhcp/dhcpd.conf |
| # dhcpd.conf  #  # Sample configuration file for ISC dhcpd  #  #默认搜索域  option domain-name "example.org";  #域名服务器，多个用逗号隔开  option domain-name-servers ns1.example.org, ns2.example.org;  #默认租期  default-lease-time 600;  #最大租期  max-lease-time 7200;  subnet 10.152.187.0 netmask 255.255.255.0 {  }  #定义子网10.254.239.0/255.255.255.224  subnet 10.254.239.0 netmask 255.255.255.224 {  #ip地址池  range 10.254.239.10 10.254.239.20;  #默认网关  option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;  }  subnet 10.254.239.32 netmask 255.255.255.224 {  range dynamic-bootp 10.254.239.40 10.254.239.60;  option broadcast-address 10.254.239.31;  option routers rtr-239-32-1.example.org;  }  # A slightly different configuration for an internal subnet.  subnet 10.5.5.0 netmask 255.255.255.224 {  #ip地址池  range 10.5.5.26 10.5.5.30;  #DNS服务器  option domain-name-servers ns1.internal.example.org;  option domain-name "internal.example.org";  #默认网关  option routers 10.5.5.1;  #广播地址  option broadcast-address 10.5.5.31;  #默认租期，单位秒  default-lease-time 600;  #最大租期，单位秒  max-lease-time 7200;  }  #绑定固定ip给客户端  host passacaglia {  #mac地址  hardware ethernet 0:0:c0:5d:bd:95;  filename "vmunix.passacaglia";  server-name "toccata.fugue.com";  }  host fantasia {  #硬件地址  hardware ethernet 08:00:07:26:c0:a5;  #指定固定ip  fixed-address fantasia.fugue.com;  }  class "foo" {  match if substring (option vendor-class-identifier, 0, 4) = "SUNW";  }  shared-network 224-29 {  subnet 10.17.224.0 netmask 255.255.255.0 {  option routers rtr-224.example.org;  }  subnet 10.0.29.0 netmask 255.255.255.0 {  option routers rtr-29.example.org;  }  pool {  allow members of "foo";  range 10.17.224.10 10.17.224.250;  }  pool {  deny members of "foo";  range 10.0.29.10 10.0.29.230;  }  } |

## 查看ip分配情况

服务器端：vim /var/lib/dhcpd/dhcpd.leases(ip分配情况)

客户端：vim /var/lib/dhclient/dhclient-eth0.leases（查看ip分配情况）

## 配置完整例子

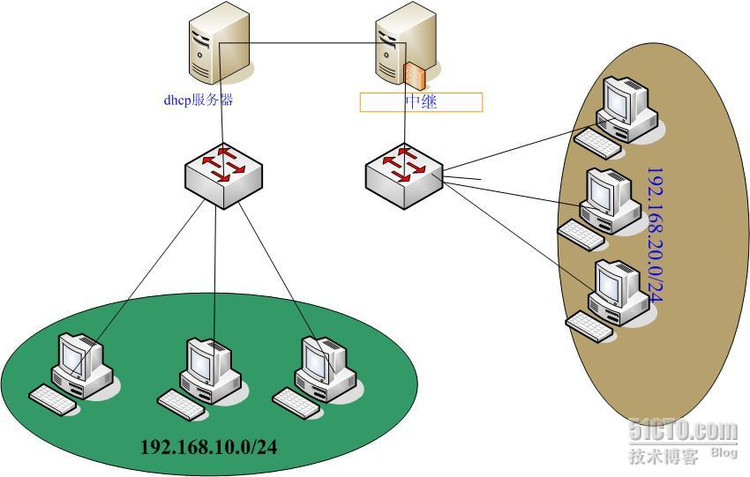
|  |
| --- |
| #dhcpd.conf  default-lease-time 600;  max-lease-time 7200;  subnet 172.16.0.0 netmask 255.255.0.0 {  range 172.16.0.100 172.16.0.200  option domain-name "abc.com"  option domain-name-servers 202.106.0.20,202.106.46.151;  option routers 172.16.0.1;  option broadcast-address 172.16.255.255;  }  host fileserver{  hardware ethernet 00:0C:5D:71:C4:3F;  fixed-address 172.16.0.10;  }  host printserver{  hardware ethernet 00:0C:5D:71:C4:3E;  fixed-address 172.16.0.20;  } |

注意：生产服务器一般不使用dhcp动态获取ip，服务器上的ip一般是静态。客户端的网络配置文件/etc/sysconfig/network-scripts/ifcfg-eth1，可以通过service network restart(获取ip)。

windows用户可以通过ipconfig/release 释放现在的ip地址，用ipconfig/renew重新获取现在的ip地址。

# 网段DHCP中继代理配置

在局域网中动态分配ip需要DHCP。但是DHCP的所有信息都是以广播的形式传送的，所以无法通过路由器。要给不同的网段分配ip，我们还要一台DHCP的中继代理服务器。



第一步：在DHCP服务器上/etc/dhcpd.conf中配置

sub 子网1

sub 子网2

第二步：配置中继代理服务器（有两个网络接口eth0,eth1）

vi /etc/sysconfig/dhcrealy

INTERFACES=”eth0 eth1”

DHCPSERVER=”DHCP服务器地址”

第三步：启动dhcrelay服务

service dhcrealy start

echo “1”>/proc/sys/net/ipv4/ip\_forword

# dhcp自动化安装

|  |
| --- |
| #!/bin/bash  #变量定义：网络，子网，地址池  NET=10.0.2.0  MASK=255.255.255.0  RANGE="10.0.2.10 10.0.2.100"  DNS=202.106.0.20  DOMAIN\_NAME="example.com"  ROUTER=10.0.2.1  #测试yum源  test\_yum(){  yum list dhcp &>/dev/null  if [ $? -ne 0 ] ;then  echo "there is an error to connect to Yum repository!"  exit  fi    }  #保存原有的配置文件  test\_conf(){  if [ -f /etc/dhcp/dhcpd.conf ] ;then  mv -f /etc/dhcp/dhcpd.conf /etc/dhcp/dhcp.conf.save  fi  }  #创建新的配置文件  create\_conf(){  cat > /etc/dhcp/dhcpd.conf <<EOF  #dhcpd.conf  default-lease-time 600;  max-lease-time 7200;  subnet $NET netmask $MASK {  range $RANGE;  option domain-name $DOMAIN\_NAME;  option domain-name-servers $DNS;  option routers $ROUTER;  }  host fileserver{  hardware ethernet 00:0C:5D:71:C4:3F;  fixed-address 10.0.2.10;  }  host printserver{  hardware ethernet 00:0C:5D:71:C4:3E;  fixed-address 10.0.2.20;  }  EOF  }  #安装DHCP服务器  test\_yum  yum install dhcp -y &>/dev/null  test\_conf  create\_conf  service dhcpd start |