

## 第8章 地址发现协议(BOOTP和DHCP)

作者：Rima S. Regas

本章内容包括：

- 引导协议(BOOTP)
- 动态主机配置协议(DHCP)
- 管理地址池
- DHCP能处理的其他分配

当一个网络大到不受它的建造者直接控制时，它就是难以控制的。在 IP地址通过手工分发的网络环境中最常见的问题是 IP地址冲突。处理这个问题的惟一方法是为客户机动态分配 IP地址。引导协议能在一定程度上完成这个任务，因为它主要为无盘工作站提供 IP信息而设计。它主要是提供 IP地址和用于定位引导目录的路径信息。正因为 BOOTP有限制，才产生了 DHCP。

动态主机配置协议(Dynamic Host Configuration Protocol, DHCP)从一个地址池中把 IP地址分配给请求主机。DHCP也能提供其他信息，如网关 IP、DNS服务器、缺省域和网络范围内 HOSTS文件的位置。设计 DHCP并不为了给无盘工作站提供引导信息，而是为了减轻管理员跟踪记录手工分配 IP地址的负担。DHCP服务器能够完成分发地址的工作，一些服务器甚至有为将来的主机隐藏特定 IP地址的功能。

本章将对这两个协议进行讨论，但重点是 DHCP，因为它是今天的主流技术。BOOTP虽然还以某种方式使用，但它是旧的且不被经常升级的协议。如果为适应时代需要而更新的话，BOOTP在适当场合内还是能很好工作的(比如，远程引导 MacOS X 服务器)。

### 8.1 “引导”协议(BOOTP)

BOOTP协议虽然简单，却可以为许多应用提供服务，主要是远程引导(客户机不包括引导盘)。这一章要重点介绍的 DHCP实际上是 BOOTP的改进。二者的基本原理一样，读者会在本章的后续节中理解这一点。

和 DHCP一样，BOOTP是一个主机配置协议。二者都使用 UDP封装报文。报文也都是 576 字节长(虽然 DHCP的选项域更多一些)。二者都使用端口 67进行输入/输出，使用端口 68进行服务器间通信。二者在客户机启动时分配 IP地址。以上就是二者的相似之处。相对比较而言，BOOTP是静态的而 DHCP是动态的。

设计 BOOTP协议的目的是用作远端引导。DHCP为移动工作组而设计，这个工作组时而与网络连接时而和网络断开。BOOTP限制在一定功能和范围内。DHCP是动态可配置的。BOOTP主要是告诉连接客户机引导文件的位置。DHCP有一个动态 IP分配策略，这个策略在整个子网掩码范围内汇集永久和短期租借的地址。

这些是二者的主要区别，不必太费力就能确定现在支持哪个协议。除非用户所关心的只是引导几百台网络计算机，否则 DHCP是自然的选择。DHCP容易配置，易于管理，排错方便，

购买容易。任何移动设备有自引导的方法，所以无需 BOOTP。DHCP为刚连到网络上发出请求的设备分配可用的IP地址。

## 8.2 动态主机配置协议(DHCP)

DHCP是为大量客户机提供快速、方便、有效地分配 IP的方法，这种方法不会造成混乱。BOOTP不能再满足网络和Internet快速增长的需要。网络管理人员需要有一种方法定义一个 IP范围，以使DHCP把它们自动分配给网络客户机。DHCP也需要一种方法来定义IP的生存时间范围(这些地址是租用的，本章后面会详述)，以及在无需访问每台工作站手工输入所有细节的情况下完成动态配置。

当然，手工输入IP是曾经使用的方法，并且一些人仍使用此法(虽然有越来越多的管理工具，自动化程序和DHCP)。在一些情况下，手工配置地址更可靠。一些管理员仍然创建一些详细的桌面清单，并把它们放在机器上或机器附近以便于手工分配 IP地址，配置网关、子网掩码及DNS的IP地址，他们认为这种方法更简单。虽然这种方法提供的对计算机重要统计数据的立即访问DHCP做不到，而且这种方法相当费时且容易出错或丢失信息。这一章讨论了DHCP的内部工作机理并考查了它的一些高效方面。

### 8.2.1 DHCP如何工作

如前所述，DHCP是BOOTP的重大改进版。DHCP实现了一个客户机/服务器模型，并且如BOOTP一样依赖于代理。被依赖的代理负责管理客户机和服务器之间的交互。在这种情况下，由于客户机是基本的通信主机，客户机和服务器进行所有的会话。这些会话发生在引导阶段。DHCP有下列功能：

- 支持动态分配
- 支持静态分配
- 和BOOTP一起工作
- 租用地址
- 支持永久租用地址
- 恢复中止的租用地址

实质上，DHCP负责处理两种基本的数据：租用地址(已分配的IP)和地址池中的地址(可用的IP)。给一台客户机分配IP地址涉及到一些过程，但是这并不复杂。实际上，DHCP不复杂，但是要记住一些事项。

#### 1. 客户机如何取得一个地址

以下各步说明了一台客户机获得地址的基本方法：

- 1) 客户机通过 DhcpDiscover广播提出请求。如果客户机有一个永久性的租用地址，它可以直接请求那个地址。
- 2) 服务器一旦收到 IP请求，会从地址池中取出一个地址并返回一个附有可用 IP地址的 DhcpOffer报文。
- 3) 如果客户机收到多个IP，它会选择第一个或其所请求的那一个。
- 4) 客户机广播标识服务器的 DhcpRequest报文并等待。
- 5) 每一个服务器检查报文，若发现不是它的标识，它会丢弃报文。当被标识的服务器接

收了报文后，它会发回一个 DhcpAck报文，如果所请求的 IP被分配也就是说租用已中止，会发回DhcpNak报文。

6) 如果客户机收到DhcpAck报文，它可以开始使用IP地址。如果它收到DhcpNak，它会重新开始整个过程。假如IP有问题，客户机会发送一个DhcpDecline报文给服务器并重新开始。

注意 一个永久性地址和一台机器永久地结合在一起。实际上，没有这样的永久性地址，因为一段时间之后所有的租用必须中止。但是一个永久性的租用可以在一段时间内连续使用几个月，每当机器和网络相连接请求IP地址时要重置时钟。

虽然看起来无需重复，但在这些步骤在 DHCP环境是下是正确操作所必须的。这些功能也是DHCP区别于BOOTP的地方。

## 2. 中继代理如何工作

中继代理能中继服务器和客户机之间的报文。这样可以使服务器能处理没有服务器的子网。这意味着不必为每一个子网设置一个服务器，为每一个子网设置一个服务器开销很大，以下几步说明了中继代理如何工作：

- 1) DHCP客户机广播一个消息。
- 2) 中继代理把收到报文的接口对应的IP地址放到消息的giaddr域中，然后单目广播至服务器。
- 3) 服务器给中继代理返回应答(通过单目广播)。应答包括与客户机所请求相同的giaddr域。
- 4) 中继代理会从giaddr域中IP地址对应的接口中广播应答。

## 8.2.2 理解租用地址

DHCP通过提供租用地址来处理分布的 IP地址。租用就和现实中的租用一样工作，只是没有利益关系。基本地讲，要定义一个 IP地址分配给一台主机的时间。如果租用中止（在连接被再次使用之前计时器超时），客户机需要申请新的IP地址。

一个客户机可以申请一个特定的 IP地址，如果此IP是可用的，DHCP服务器会分配这个地址给客户机。这也在动态网络环境中，有很少量的可用 IP地址情况下处理永久性租用的方法，但是DHCP还会保留一些特殊的 IP地址以给特定的用户。假如另一台机器很需要此地址，DHCP会分配给它。但是当地址再次可用时，它能重新分配给请求机（注意客户机为了再次请求IP地址，需要和网络断开）。

一些系统使用60分钟来保证动态客户机的活跃性和安全。ISP使用短期租用来保持IP地址的动态性(绝大多数ISP的IP地址比依靠它们同时进行连接的客户数少)并限制用户运行服务器的可能性。其他如Windows 2000服务器，缺省时间是三天。

注意 绝大多数(并非全部)服务器，在启用中止之后保持至少24小时的租用周期。这其中有许多原因，包括用户到另一个时区或地方旅行，而他的膝上电脑没有插座可用。

正确的管理租用需要时间和技能，因为没有两个网络是相同的。通常，有两种策略。一种策略是限制租用时间，强制客户机经常性的申请租用地址。这种方法对网络有强烈和长期的影响，所以要仔细考虑这个选择，因为它只适合于机器经常移动的情况，这样可以保证地址池经常被刷新。适用于这种环境的最好例子是计算机制造工厂，在这种环境中为了测试网卡，新的计算机要不断地换进换出。

另一个选择是租用期为5或6天，那时租用已经结束(但常见的情况是它们没有中止，因为

客户机可能会在这段时间内重新和网络连接)。这样极大地减少了网络流量,但是这种方法使网络缺乏动态性。会使一个潜在的黑客有大量时间使用一个IP。有一个折衷的方法工作最好,但是它需要个人经验。在移动用户和RAS用户之间,方便性和安全性之间作折衷,找到平衡点。我能作出的惟一建议是宁可让移动用户感到不满,也要满足系统的安全要求。堵住安全漏洞比让一些膝上用户感到满意更重要。

### 8.3 管理地址池

一个地址池,也称为一个地址范围,是DHCP客户机可用的一类地址范围。理解地址池需要一点地址类型和IP如何工作的知识。

有效的IP地址类是:

0.0.0.0

255.0.0.0

255.255.0.0

255.255.255.0

255.255.255.255

在每一类中是一个可用的IP地址范围。一个典型IP地址是204.76.150.20。虽然现在这并不意味着太多东西,但过一会儿读者会明白。

注意 有一些保留的地址。0.0.0.0用作缺省路由,127.0.0.0是loopback IP地址用于测试和其他局部操作。比如,从自己的机器上发送邮件至本机的邮件服务器上。还有一些范围为私有网络保留,它们是169.0.0.0和192.0.0.0,读者在Internet上不会找到这些IP地址范围。如果读者发现了这些地址说明出了问题。

这一节讨论IP地址,但是并不涉及IP地址究竟是什么以及它是如何组成的。理解IP结构最容易的方法是从类型角度考虑。一类地址就是共享顺序值范围和有共同数学限制的数值。

下面介绍类型如何工作。A类地址占用126个网络。因为IP地址的每一段用一个8位位组表示,一个8位位组是一个8位数。所有的模糊想法可用下式表示清楚:

$$2^7 - 2 = 126$$

这是因为每个IP地址的最高位(最左位)置为0,则只剩下7位,能从剩下的24位中得到最大主机数:

$$2^{24} - 2 = 16\,777\,214$$

用户能够得到1600多万个主机地址,但限制为126个网络。减2是因为0.0.0.0和127.0.0.0用于保留。在顶级看起来地址空间不是很大。下面是B类地址。

两个8位是16位,除去最左两位:

$$2^{14} = 16\,384$$

给出16 000多个网络,和A相比并不坏。因为B类地址的最左两位设为1和0,所以得到 $2^{14}$ 。下式指出B类网络支持的主机数:

$$2^{16} - 2 = 65\,534$$

失去了大量主机但却得到了大量的网络数。下面看一下C类地址,C类地址占用3/4的位数表示网络,因此有24位表示网络,C类网络数:

$$2^{21}=2\,097\,152$$

可以得到相当多的网络。和其他类差不多，最高三位设为 1、1、0，只剩下 21 位。主机数为：

$$2^8-2=254$$

主机数不多。所有这些能告诉读者有多少 IP 地址吗？很简单。下面解释了公式代表的含义。

A 类地址给出  $2^{31}$  个 IP，即 2 147 483 648

B 类地址给出  $2^{30}$  个 IP，即 1 073 741 824

C 类地址给出  $2^{29}$  个 IP，即 536 870 912

总共是 4 294 967 296 个 IP 地址。用户能使用的 IP：

- A 类——1.xxx.xxx.xxx 到 126.xxx.xxx.xxx
- B 类——128.0.xxx.xxx 到 191.255.xxx.xxx
- C 类——192.0.0.xxx 到 223.255.255.xxx

x 表示 0 到 255 中的任何数字。

这种方式会造成分配浪费，极大地减少了可用的 IP 地址。因此，产生了子网。图 8-1 显示了子网如何工作。

把主机号分成两部分使用新的子网号作为内部网标识，使没和 Internet 直接相连的一组计算机共享 IP，所以有一个具有 IP 地址 209.188.0.0 的路由器可以驻留 IP 地址为 209.188.1.0、209.188.2.0、209.188.3.0 的主机。路由器处理所有的内部路由，所以一个 C 类地址可以覆盖任何人。

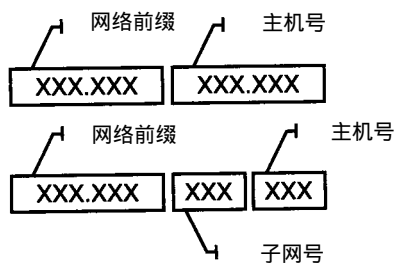


图8-1 上面一行是旧的IP格式，它被分为网络和主机地址。下面一行显示了子网如何工作，把主机号分成了两半，第三个八位位组表示子网号

## 8.4 DHCP能处理的其他分配

DHCP不仅能很好地给工作站分配 IP 地址，也能给工作站提供其在网络上能正常工作的所有细节。包括每个 NIC IP 地址分配、DNS 服务器 IP、任何一个 WINS 地址以及网关服务器的地址。

注意 所有的局域网及其他的私有网络至少有一个网关服务器，一般情况下是用于安全的防火墙。用户可以访问局部共享设备，但是通过网关访问就会出现问題。

### 8.4.1 注意重载

在典型的 DHCP 服务器安装中，服务器被设置为传送所有客户机连接网络时的参数请求。通过输入静态信息，这种分配信息可以被重载，通常情况下 DHCP 服务器会自动输入。如果要确信工作站总使用一个特殊的 DHCP，以保证安全或客户机负载均衡，用户可以从另一个服务器重载任何潜在的 IP 分配，通过在网络设置中输入想要的服务器 IP 地址实现。

### 8.4.2 其他分配

通过 DHCP 可以得到一些其他分配，其中两个是 DNS 和 WINS。二者功能相同，但采用不

同的方式。WINS是微软的专利格式，对基于 Windows的网络进行设置是高效和容易的。DNS 是世界上广泛接受的名字解析系统，而且成百万的人每天都在使用它（参考第6章）。虽然没有具体统计数据，但绝大多数 Windows NT使用DNS而不是WINS。工作站需要和DNS交换信息，所以需要向系统发送IP地址。工作站也需要知道子网掩码，所以也要发送该信息。

DHCP也处理DNS的主机域名和DNS项的匹配，以及各种形式的网关 IP、多Internet网卡IP 分配。

## 8.5 小结

这一章包括 IP地址如何生成及子网如何工作等内容。读者知道自己需要一个路由器和 Internet连接，以使得在整个内部网络中使用一个 IP。这一点对 DHCP服务结构来说很重要，因为它能让用户知道可以分配什么，不能分配什么。随着网络的增长，可用范围变得更加重要。

下一章仔细讨论IP协议家族。