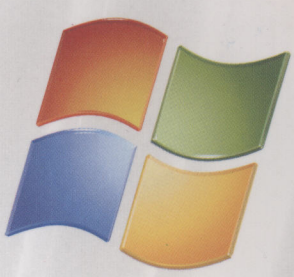
Windows Server 2008系统工程师 视频突击

典藏



Windows Server 2008 网络基础架构

韩立刚 韩利辉 李文斌 编著

超值赠送 2 DVD

30小时的Windows Server 2008网络基础架构视频操作
20小时的Windows Server 2003网络基础架构视频操作
10小时CCNA视频教程 8小时企业培训视频

清华大学出版社

Windows Server 2008 系统工程师视频突击

贯彻 Windows Server 2008 网络基础架构

韩立刚　韩利辉　李文斌　编著

清华大学出版社
北　京

内 容 简 介

本书以 Windows Server 2008 的网络基础服务为重点，全书共 13 章，主要内容包括：使用 Windows Server 2008 做 DHCP 服务器、DNS 服务器、WINS 服务器；使用公共密钥基础结构实现网络安全，包括电子邮件数字签名、数字加密，配置网站使用 Https 通信；实现针对 DHCP、远程访问和 IPSec 的网络接入保护，将 Windows 配置成为软路由，配置 NAT 实现内网到 Internet 的连接，配置 VPN 连接，配置站点间 VPN，配置 Web 服务器场，远程管理 Web 服务器，配置 FTP 站点，配置权限管理服务；使用 Windows Server 2008 配置流媒体服务器，配置 WSUS 实现系统补丁更新，配置 Windows 部署服务实现远程安装。

本书遵循先理论、后实战的原则。在实战部分，分为实战目标、实战场景、实战中的服务器环境、在各个服务器上的配置步骤以及配置成功后的验证，以让读者触类旁通，将这些实战场景在自己的企业中实施。

随书赠送两张 DVD 光盘，包含超过 60 小时的视频讲解教程。

本书读者对象为：企业 IT 部门系统管理员，想进入 IT 领域的大学生，想考取微软新一代认证 MCITP 的在职人员或在校学生。

图书在版编目(CIP)数据

贯彻 Windows Server 2008 网络基础架构/韩立刚，韩利辉，李文斌编著. —北京：清华大学出版社，2010.3
(Windows Server 2008 系统工程师视频突击)
ISBN 978-7-302-21890-6

Ⅰ. 贯…　Ⅱ. ①韩…　②韩…　③李…　Ⅲ. 服务器—操作系统(软件)，Windows Server 2008　Ⅳ. TP316.86

中国版本图书馆 CIP 数据核字(2010)第 012963 号

责任编辑：栾大成
装帧设计：杨玉兰
责任印制：王秀菊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：210×280　**印　张**：43.5　**字　数**：1249 千字
附光盘 2 张
版　　次：2010 年 3 月第 1 版　　**印　　次**：2010 年 3 月第1次印刷
印　　数：1～5000
定　　价：79.00 元

韩立刚 河北师范大学软件学院讲师，2002年获得微软认证系统工程师（MCSE）、微软认证数据库管理员（MCDBA）认证、2002年获得微软认证讲师（MCT）资格以及微软认证IT专家（MCITP）、2005年获得微软企业护航专家资格。精通Windows、SQL Server、 Exchange、 ISA 2006产品。
在项目实施中，屡次委以重任，广受领导、同事以及客户的好评。

韩利辉 河北金中华通讯服务有限公司资深网络和系统工程师，2002年获得微软认证系统工程师（MCSE）、微软认证数据库管理员（MCDBA）认证，精通网络安全和Windows Server 、Exchange 管理、ISA Server的规划/部署/排错、Windows XP/Vista与网络基础架构的规划（改造）、实施企业信息安全的规划、实施SQL Server的维护、排错与优化。

李文斌 1999年获微软认证系统工程师（MCSE），微软认证产品专家及微软认证Internet专家认证。2008年获网络安全相关证书。2001年攻读计算机软件与理论工学硕士学位。2003年提前攻读博士学位，2007年7月获计算机应用技术工学博士学位。

前　言

Windows Server 2008 是微软最新的服务器操作系统，继承于 Windows Server 2003。Windows Server 2008 是一套相当于 Windows Vista 的服务器系统，两者很可能拥有很多相同功能；Windows Vista 及 Windows Server 2008 与 Windows XP 及 Windows Server 2003 间存在相似的关系。

Windows Server 2008 代表了下一代 Windows Server。使用 Windows Server 2008，IT 专业人员对其服务器和网络基础结构的控制能力更强，从而可重点关注关键业务需求。Windows Server 2008 通过加强操作系统和保护网络环境提高了安全性。通过加快 IT 系统的部署与维护，使服务器和应用程序的合并与虚拟化更加简单，并且提供直观管理工具。Windows Server 2008 还为 IT 专业人员提供了灵活性。Windows Server 2008 为任何组织的服务器和网络基础结构奠定了最好的基础。

Windows Server 2008 用于在虚拟化工作负载、支持应用程序和保护网络方面向组织提供最高效的平台，它为开发和可靠地承载 Web 应用程序和服务提供了一个安全、易于管理的平台。从工作组到数据中心，Windows Server 2008 都提供了很有价值的新功能，对基本操作系统做出了重大改进。

本书遵循先理论、后实战的原则。在实战部分，分为实战目标、实战场景、实战中的服务器环境、在各个服务器上的配置步骤以及配置成功后的验证，以让读者能够触类旁通，将这些实战场景在自己的企业中实施。

本书的实战环境均是在一台 DELL D630 的笔记本电脑上实现的，配置为 Intel Core2 Duo CPU T7300，内存为 3GB，读者可以在 3GB 内存的计算机上使用 VMWare WorkStation 6.02 虚拟机实现所有的实战演练。

本书的知识相互之间有交叉，为了避免这些交叉影响读者对知识的理解，各章节之间进行了周密的部署。下面是各章内容的简要介绍。

- **第 1 章 DHCP 服务器**，使用 DHCP 为客户端配置 IP 地址，在跨路由的网络中实现 IP 地址自动分配，实现 DHCP 容错。
- **第 2 章 配置 DNS 服务器**，明白域名的层次结构、域名解析过程，安装 DNS 服务器，创建区域和主机记录，实现域名解析委派，实现域名解析转发，添加 MX 记录支持邮件服务器，使用 Hosts 文件实现计算机名解析。
- **第 3 章 配置 WINS 服务器**，本章学习在企业内网的计算机名称的解析过程，以及配置 WINS 服务器实现跨网段计算机名解析。
- **第 4 章使用 PKI 实现安全**，本单元将学习如何利用 Windows Servers 2008 提供的公共密钥基础结构配置网络安全性，如何安装、配置、请求和管理证书服务。
- **第 5 章 配置路由和 NAT**，配置静态路由，在路由器上配置数据包过滤，配置内网使用 NAT 访问连接 Internet，配置端口映射允许 Internet 用户访问内网 Web 站点，配置端口映射允许 Internet 用户访问内网远程桌面。
- **第 6 章 远程访问**，掌握什么是远程访问，配置远程访问，配置 PPTP VPN 客户端，配置 L2TP VPN 客户端，配置 SSTP VPN 客户端，配置远程访问网络环境中的防火墙。

- **第 7 章 配置站点间 VPN**，配置站点间 VPN，创建请求拨号接口，配置静态路由触发请求拨号，配置拨入拨出凭据，测试站点间 VPN 连接，配置多站点间 VPN，测试多站点间 VPN 连接，NAT、远程访问和站点间 VPN 集成。
- **第 8 章 创建 Web 站点和 FTP 站点**，安装 Web 服务器，Web 站点的标识，安装 FTP 功能，创建 FTP 站点，创建隔离用户的 FTP 站点，创建允许匿名用户访问的目录。
- **第 9 章 配置网络接入保护(NAP)**，介绍网络接入保护，配置 NAP for DHCP，配置 NAP for VPN，实现 NAP for IPSec。
- **第 10 章 权限管理服务**，理解权限管理服务、权限管理需要的环境、权限管理工作过程，安装和配置权限管理服务，使用权限管理保护文档，使用权限策略模板保护文档。
- **第 11 章 配置和管理系统更新服务**，了解 Microsoft Windows Server Update Services (WSUS)，能够在网络上部署 WSUS 3.0，能够安装 WSUS、配置 WSUS 3.0 以获取更新，将客户端计算机配置为从 WSUS 3.0 安装更新，以及批准、管理和分发更新，在域环境中配置 WSUS 客户端，在工作组环境中配置 WSUS 客户端，WSUS 服务器常规管理。
- **第 12 章 使用 WDS 部署操作系统**，什么是 WDS，WDS 需要的环境，安装和配置 WDS 服务，从安装光盘制作安装映像，从参考计算机制作安装映像，配置 DHCP 支持跨网段远程安装，在路由环境使用 WDS 安装操作系统。
- **第 13 章 流媒体服务器**，了解 Windows Media Service、Windows Media Services 新增功能、流媒体的分发方法，能够搭建 Windows 流媒体服务，创建点播站点，创建视频点播网站，安装流媒体播放软件，创建单播广播站点，创建多播广播站点，收看多播广播节目，创建和编辑播放列表。

本书读者对象为：企业 IT 部门系统管理员，想进入 IT 领域的大学生，想考取微软新一代认证 MCITP 的在职人员或在校学生。

致　　谢

任何一本书的出版，都离不开家人、朋友等的关心和帮助。以下诸位为本书提供了极大帮助：河北师范大学的蒋春澜教授、邓明利教授为作者创造了优越的写作条件与实验环境，河北师范大学的赵书良教授、河北经贸大学的王顶老师等对本书的组织、行文提出了许多好的建议。感谢河北师范大学软件学院的全体教师，他们中的大多数人阅读了本书初稿，指出了书中的不少错误，并配合录制了本书视频。

需要特别感谢的是河北师范大学软件学院的管理层，他们开明的态度和支持使我能有充分的时间和空间写作本书，包括罗忠华先生、赵胜老师等。

在书稿编辑方面，清华大学出版社的栾大成先生和其他编校人员给予了很大帮助，对他们为本书出版所做的一切工作衷心地表示感谢。

要感谢我的父母、妻子和孩子，没有家人的大力支持，写作将是件令人痛苦的事情。而本书的成文过程却始终充满了动力与快乐。

韩立刚

Email: onesthan@hotmail.com

目　录

第1章　配置DHCP服务器

在TCP/IP 网络上的每台设备，如客户端计算机和各种网络设备，都必须有合法的独一无二的IP地址和配置数据。TCP/IP配置数据包括IP地址、子网掩码和附加的IP数据。例如路由器信息和DNS服务器地址、WINS服务器地址等。

网络管理员可以手工配置和维护网络中客户端的 IP 配置，也可以使用DHCP为网络中的各种设备自动分配、配置和维护TCP/IP配置数据。

DHCP(Dynamic Host Configuration Protocol，动态主机配置协议)，可以对网络中的IP地址进行集中管理，这样就避免了地址冲突并减少了管理员的工作量。通过在网络中部署 DHCP，整个过程可以自动集中进行管理。DHCP服务器拥有一个IP地址池，当任何启用DHCP的客户机登录网络时，可从它那里租借一个IP地址。因为IP地址是动态的(租借)而不是静态的永久分配，不使用的IP地址就自动返回地址池供再分配。

关键词

- 掌握客户机请求IP地址过程
- 能够在Windows Server 2008上安装和配置DHCP服务
- 学会配置DHCP选项
- 能够设置计算机使用DHCP服务分配地址
- 能够在Windows Server Core上安装和配置DHCP服务
- 能够使用图形界面管理工具管理Windows Server Core上的DHCP服务
- 能够配置 DHCP 服务的故障转移群集
- 能够使用VMware模拟多网段环境
- 学会在跨路由网络中配置和使用DHCP
- 掌握DHCP解决方案的最佳实践

1.1 DHCP 概述

动态主机配置协议(DHCP)是一个 TCP/IP 标准，用于减少网络客户机 IP 地址配置的复杂度和管理开销。Windows Server 2008 提供 DHCP 服务，该服务允许一台计算机作为 DHCP 服务器并配置用户网络中启用 DHCP 的客户计算机。DHCP 在服务器上运行，能够自动集中管理 IP 地址和用户网络中客户计算机所配置的其他 TCP/IP 设置。DHCP 还提供一体化的活动目录服务和域名系统(Domain Name System，DNS)服务、高级 DHCP 服务器监视和统计信息报告、特定厂商选项和用户类别支持、组播地址分配和诈骗 DHCP 服务器检测。

1.1.1 DHCP 的优点

1. 自定义的 TCP/IP 配置方式

对于基于 TCP/IP 的网络，必须要进行 IP 数据的配置，例如 IP 地址、子网掩码或默认网关等。可以使用两种方式进行自定义的 TCP/IP 配置。

1) 手动 TCP/IP 配置

可以通过手动输入的方式为网络上的每个设备设置其 IP 配置数据，其操作界面如图 1-1 所示。

手工输入不可避免地会产生输入错误。这些错误也许会导致通信无法正常进行或 IP 地址冲突。而且某些情况下，网络中的计算机(例如笔记本电脑)会经常性地变换其所处的网段，手工输入方式不适合比较大的网络，管理负担会过于繁重。

2) 自动 TCP/IP 配置

自动 TCP/IP 配置的操作界面如图 1-2 所示。

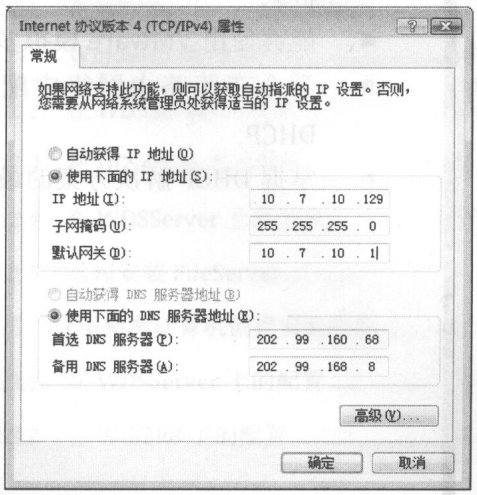


图 1-1 手动配置 IP 地址

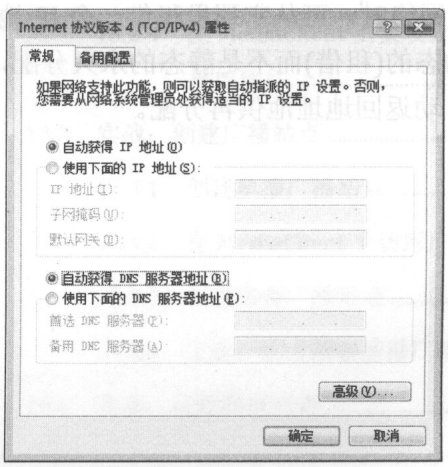


图 1-2 自动获得 IP 地址和 DNS

使用 DHCP 进行自动化配置，当将 DHCP 服务器设置为支持 DHCP 客户端时，DHCP 服务器将自动将相关的配置信息提供给 DHCP 客户端。

自动 TCP/IP 配置方式可以保证网络中的客户端得到正确配置。而且，如果需要对某些客户端的 IP 配

置数据做出调整，只需在 DHCP 服务器上一次完成， DHCP 服务器将自动更新这些客户端上的配置信息以使这些调整生效。

2. 使用 DHCP 的优点

DHCP 具有如下优点。

- 安全可靠地配置 DHCP 可以把手工 IP 地址配置所导致的配置错误减小到最低程度，比如输入错误或者把当前已分配的 IP 地址再分配给另一台计算机所造成的地址冲突等。
- 减少网络管理工作量。
- TCP/IP 配置是集中化和自动化的。网络管理员能集中定义全局和特定子网的 TCP/IP 配置。使用 DHCP 选项可以自动给客户机分配全部范围的附加 TCP/IP 配置值。
- 客户机配置的地址变化必须经常更新。比如远程访问客户机经常到处移动，这样便于它在新的地点重新启动时，高效而又自动地进行配置。

提示： 大部分路由器能转发 DHCP 配置请求，这就减少了在每个子网设置 DHCP 服务器的必要，除非有其他原因。

例如：在一个中型网络中，需要设置 200 台计算机的 IP 配置信息。如果没有 DHCP，需要一台接一台地手工设置这 200 台计算机。设置完成后，还需要牢记这 200 个设置。如果要对这些计算机的 IP 配置做出变动，需要再做一遍以上的工作。

有了 DHCP，只需为服务器添加一个 DHCP 服务器角色就可以支持这 200 个网络客户端。当需要对 IP 设置做变动的时候，只需在 DHCP 服务器上一次完成，每个 TCP/IP 网络上的主机将会更新其 DHCP 客户端配置。

1.1.2　DHCP 地址租约

DHCP 集中管理 IP 地址设置。DHCP 既可以被配置为单一子网中的计算机分配 IP 地址，也可以被配置为多个子网的计算机分配 IP 地址。DHCP 服务器会自动将 IP 地址配置数据分配给 DHCP 客户端。

租约(lease)是由 DHCP 服务器指定的，客户端计算机可使用指派的 IP 地址的时间期限。在租约过期之前，客户端需要续租或者从 DHCP 服务器得到新的租约。

通过向客户端提供 IP 地址配置租约，DHCP 管理着 IP 地址配置数据的分配和释放。租约决定了在将分配得到的 IP 配置信息返还给 DHCP 服务器并更新其配置信息之前，客户端可以使用它的持续时间。分配 IP 地址配置信息的这一过程被称为 DHCP 租约生成过程(DHCP lease generation process)。更新 IP 地址配置信息的过程被称为 DHCP 租约更新过程(DHCP lease renewal process)。图 1-3 描述了地址租约的产生过程，其含义说明如下。

当一个 DHCP 客户端首次加入到网络中来时，它将向 DHCP 服务器发出一个要求得到 IP 地址配置信息的请求。当 DHCP 服务器接收到这个请求后，将从网络管理员已经设定的作用域的 IP 地址范围中选择一个，并将这个 IP 地址配置信息提交给 DHCP 客户端。

一旦 DHCP 客户端接受了 DHCP 服务器为其分配的 IP 地址配置信息，DHCP 服务器将按照指定的时间将该 IP 地址配置信息以租约的方式提供给客户端。然后，客户端就可以使用这个 IP 地址配置信息来访问网络。

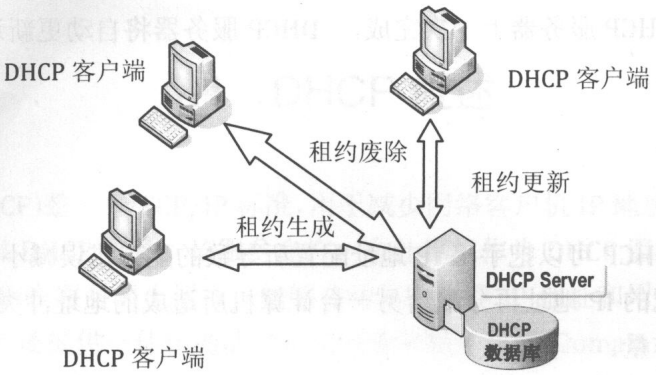


图 1-3　地址租约产生的过程

1.1.3　DHCP 分配 IP 地址信息过程

所谓 DHCP 租约生成过程就是 DHCP 客户端从 DHCP 服务器获得 IP 地址配置信息的过程。

1. DHCP 工作过程

如图 1-4 所示，DHCP 通过 4 个步骤将 IP 地址信息以租约的方式提供给 DHCP 客户端。这 4 个步骤分别以 DHCP 数据包的类型命名。

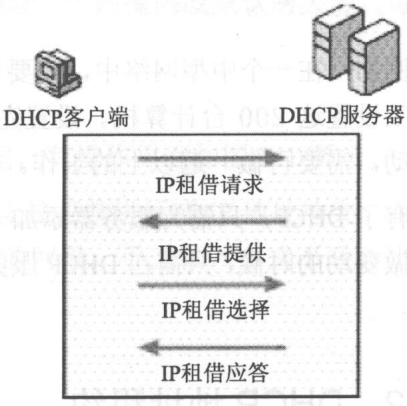


图 1-4　DHCP 工作过程

- DHCP 请求。
- DHCP 提供。
- DHCP 选择。
- DHCP 确认或 DHCP 拒绝。

步骤 1：DHCP 请求

① DHCP 客户端向网络广播一个 DHCPDISCOVER 数据包，请求一个 IP 配置信息。

② DHCP 客户端向网络广播一个 DHCPDISCOVER 数据包，以找到一个可用的 DHCP 服务器。所谓 DHCPDISCOVER 数据包就是当 DHCP 客户端首次尝试登录网络并向 DHCP 服务器请求 IP 地址信息时所发出的信息。

③ 在两种情况下将会开始租约产生过程。其一是当客户端计算机启动或首次初始化 TCP/IP 设置时；其二是当客户端尝试续租其租约而遭到拒绝时，如当客户端被从一个网段移动到另一个网段后，它的续租请求将被拒绝。

④ DHCP 客户端发送完 DHCPDISCOVER 消息后，会等待 DHCP OFFER 消息。如果一台 DHCP 客户机在启动时未能从 DHCP 服务器接收到 DHCP OFFER 消息，它就会重试 4 次(相隔 2s、4s、6s、8s、16s，加上一个 0～1000ms 之间的随机时间数)。如果 DHCP 客户机经过 5 次尝试仍没收到 DHCP OFFER 消息，它就等待 5min，然后重新开始。

步骤 2：DHCP 提供

① DHCP 服务器向网络广播一个 DHCPOFFER 数据包来应答客户端的请求。

② 当 DHCP 服务器接收到 DHCP 客户端广播的 DHCPDISCOVER 数据包后，网络中的所有 DHCP 服务

器都会向网络广播一个 DHCPOFFER 数据包。所谓 DHCPOFFER 数据包就是 DHCP 服务器用来将 IP 地址提供给 DHCP 客户端的信息。

③ 做出反应的 DHCP 服务器在收到发出请求的客户端的确认之前将保留这个 IP 地址而不会将它提供给其他的客户端。

④ 如果 DHCP 客户端在发出 4 次请求后依然没有得到任何响应，则操作系统将自动为其分配一个范围从 169.254.0.1～169.254.255.254 的 IP 地址。这种自动分配技术可以确保在一个网段上即使没有可用的 DHCP 服务器，该网段上的客户端也可以互相通信。在这种情况下，DHCP 客户端将每隔 5min 进行一次寻找 DHCP 服务器的尝试。当 DHCP 服务器可用时，客户端将得到有效的 IP 地址，保证它们无论是否处于网段之中都能够与主机进行通信。

步骤 3：DHCP 选择

① DHCP 客户端向网络广播一个 DHCPREQUEST 数据包，来选择多个服务器提供的 IP 地址。

② 在 DHCP 客户端接收到服务器的 DHCPOFFER 数据包后，会向网络广播一个 DHCPREQUEST 数据包。所谓 DHCPREQUEST 数据包就是 DHCP 客户端向 DHCP 服务器发出的请求或者续租其 IP 地址租约的信息。

③ DHCP 客户端一收到 DHCPOFFER 提供的数据包就向网络广播一个 DHCPREQUEST 数据包接受分配。DHCPREQUEST 数据包包含为客户端提供该租约的 DHCP 服务器的标识，这样其他 DHCP 服务器收到这个数据包后就会撤销对这个客户端的分配而将该分配的 IP 地址收回用于响应其他客户端的租约请求。

步骤 4：DHCP 确认(或拒绝)

① 被选择的 DHCP 服务器向网络广播一个 DHCPACK 数据包确认客户端的选择。

② 在 DHCP 服务器接收到客户端广播的 DHCPREQUEST 数据包后，随即向网络广播一个 DHCPACK 确认数据包。所谓 DHCPACK 确认数据包就是一个 DHCP 服务器发给 DHCP 客户端的确认 IP 地址租约成功生成的信息。这个信息包含该 IP 地址的有效租约和其他的 IP 配置信息。

③ 当DHCP客户端收到该确认后，将使用DHCP服务器提供的IP配置数据初始化TCP/IP，并将TCP/IP协议绑定到网络服务和网络适配器，以使客户端可以在网络上进行通信。

④ 如果被提供的 IP 地址不再有效或已经被另一台计算机使用，DHCP 服务器将发出一个 DHCPNAK 数据包否决地址的确认。这时，DHCP 客户端必须开始一个新的租约产生过程。

注意：DHCP 服务器和 DHCP 客户端之间的所有通信都经由用户数据报协议(UDP)端口 67 和 68 进行。一些交换机和路由器默认情况下不会正常传递 DHCP 广播，为了 DHCP 能正常工作，需要配置这些设备，以使它们支持在这些端口传递广播数据包。

2．消息类型说明

- **DHCPDISCOVER**　在一台 DHCP 客户机第一次试图登录网络时，它通过广播 DHCPDISCOVER 包请求 DHCP 服务器的 IP 地址信息。该包的源 IP 地址是 0.0.0.0，因为此时客户机还没有 IP 地址。
- **DHCPOffer**　每个收到客户机 DHCPDISCOVER 包的 DHCP 服务器以一个 DHCP OFFER 包作为应答，其中包含一个未租借的 IP 地址和其他 DHCP 配置信息，比如子网掩码和默认网关。不止一个 DHCP 服务器能应答 DHCP OFFER 包。客户机将接受所收到的第一个 DHCP OFFER 包，该消息为 342 字节长。