BOOK
远望图书

网管道

全能网管

兵器谱

精选网管必备工具·多年实战经验荟萃

十八般武器
江湖独门兵器　传世神兵利器
少林七十二式

刘晓辉 编

重庆大学出版社
http://www.cqup.com.cn

全能网管兵器谱

QUANNENG WANGGUAN BINGQIPU

刘晓辉 编

重庆大学出版社

内 容 提 要

本书针对网络管理员管理局域网时需要的各种工具进行了详细的阐述。主要内容包括IP/MAC地址工具、流量检测与分析工具、网络监控诊断分析工具、网络设备管理工具、局域网服务器管理工具等内容。我们通过通俗易懂的方式对这些内容进行介绍，读者通过一种娱乐的方式掌握相关的技术问题。本书内容丰富，适合广大大学生、网络爱好者以及网络从业人员阅读。

图书在版编目（CIP）数据

全能网管兵器谱／刘晓辉编．—重庆：重庆大学出版社，2008.1

ISBN 978-7-5624-4355-1

Ⅰ.全… Ⅱ.刘… Ⅲ.局部网络－管理 Ⅳ.TP393.107

中国版本图书馆CIP数据核字（2007）第204371号

全能网管兵器谱

刘晓辉 编

责任编辑：黄 成 版式设计：曾 俐

责任校对：夏 宇 责任印制：赵 晟

*

重庆大学出版社出版发行

出版人：张鸽盛

社址：重庆市沙坪坝正街174号重庆大学（A区）内

邮编：400030

电话：(023) 65102378 65105781

传真：(023) 65103686 65105565

网址：http://www.cqup.com.cn

邮箱：fxk@cqup.com.cn（市场营销部）

全国新华书店经销

重庆科情印务有限公司印刷

*

开本：787×1092 1/16 印张：22 字数：420千

2008年1月第1版 2008年1月第1次印刷

ISBN 978-7-5624-4355-1 定价：38.00元（含1CD）

前言

如今，随着局域网的不断普及，网络管理与维护越来越受到大家的重视。对于很多初中级网管来说，他们在实际网络管理工作中可能会遇到各种各样的问题，由于工作经验不够丰富，面对这些问题，他们感到束手无策。此时，他们脑海中肯定会冒出这样一句话："工欲善其事，必先利其器"——如果自己手中有武林高手那些威力无比的"兵器"，还能被这些小问题难住？

在本书中，笔者以兵器谱的方式，向大家介绍网管在日常工作中应该掌握的各种工具以及使用方法。本书开创网管工具书籍写作手法之先河，率先以兵器谱的模式，将各种武林兵器的象征意义与解决网络实际问题的工具相结合，从初中级网络管理者的角度，针对目前各种网络常用到的网络管理工具，进行了深入的介绍，并给出详细的使用方法。

全书共分4个板块，各大板块既各自成章，又相互关联，涉及网络管理中的多种管理软件。读者可以根据自己的实际情况，选择相应的软件加以应用。全书采用全程图解形式，即便是初学入门的读者也能够随学随用、即查即知，最终成为一名网管高手，在"江湖"中潇洒走一回！

《全能网管兵器谱》是一本为广大网管工作者定制的工具入门指导图书，内容涵盖了当今网管应用的各大领域，文章中的4个板块包括：第1部分介绍的是"十八般武器"，里面主要介绍网管工作中常用的基础软件，如Windows系统内置工具——IPconfig、获取远程计算机MAC地址——nbtstat等，通过这些知识的学习，帮助读者掌握基础的网管知识，为后面的学习打好基础；第2部分介绍的是"江湖独门兵器"，介绍的主要是一些应用范围比较广泛、功能全面的工具软件，比如IP地址管理——IPMaster、网卡地址获得工具——MAC扫描器等，通过这些学习，让读者的水平得到快速提升，真正成为一个可以登堂入室的"侠客"；在第3部分，则介绍了"传世的神兵利器"，其中包括思科交换机管理工具——CNA、HP OpenView NNM等工具软件，本章内容是提升网管水平的一个重要章节，里面涉及了思科、HP等网络大公司的专有管理软件，帮助读者了解并掌握相关的使用方法，大大提升了网管的"攻击力"；第4部分我们命名为"少林七十二式"，内容主要是介绍高级网管常用的工具软件——微软公司的MOM 2005服务器管理软件，因为服务器是网络中的核心部件，只有掌握了它的管理方法，才能让网管的工作水平得到认可，从此成为真正的"武林高手"！

本书内容活泼，可读性强，适合广大网管爱好者阅读。当然，在文章当中也可能有一些不足之处，希望广大读者指正。

光盘导航

一、光盘内容说明

组网视频教学
网络监控软件
服务器工具软件
网络管理及维护软件

二、使用方法

把光盘放入光盘驱动器后，光盘会自动运行。也可以点击光盘根目录下的Autorun.exe运行光盘。

注意：第一次运行光盘时，如果出现片头片尾无法播放的情况，请安装光盘中目录“software\多媒体软件”下面的视频播放软件暴风影音“StormCodec604.exe”。安装完成后，重新运行光盘即可。

三、推荐运行环境

1.操作系统：Windows 9x/Me/XP。
2.CPU：Pentium及兼容芯片300MHz以上。
3.内存：64MB以上。
4.显示模式：支持800 × 600以上分辨率、16位以上色彩。
5.其他：DVD-ROM驱动器、16位声卡、IE4.0以上版本浏览器。

目录

第1章 十八般武器 样样精通

目录

网管不能像黑旋风李逵一样鲁莽，但是“板斧”的强大用法还是应该学习。我们这里指的“斧”就是TCP和UDP链接测试工具netstat。它功能相当强大，可以查找到相当有用的数据。

目录

目录

目录

第1章

十八般武器 样样精通

在古典小说和传统评书中，常说武艺高强的人是“十八般武艺样样精通”，其实就是说这个人对各种武器使用得非常熟练。那么“十八般兵器”究竟是什么时候开始出现的呢？到底指的是什么呢？

在我国古籍记载里认为，刀、枪、弓、箭为黄帝所造；“十八般兵器”是战国时代军事家孙膑、吴起所创。其实这些兵器中很多可能在中石器时期就已经出现。我们的祖先为了防身和狩猎需要，就开始懂得制造和使用木棒、石刀、石斧等一类原始的兵器，或者我们可以称之为生产工具。

到了商代，我们的祖先开始使用青铜铸造刀、枪、钺等兵器。战国时代，懂得使用铁来铸造制兵器。到了汉代和魏晋时期，由于我国南方冶金事业的进一步发展，开始普遍使用铁和钢铸造刀、枪、剑，各种各样的兵器也开始多了起来。南北朝以后，铜制的兵器逐渐淘汰，都由铁和钢代替。到了明代，“十八般兵器”基本上已完全定型。

“十八般兵器”一词在古书中还找不到，明代谢肇《五杂俎》、清代褚人获《坚瓠集》两书中都只有“十八般武艺”之说。显然，“十八般兵器”一词是后人所造。“十八般兵器”究竟指的是哪些兵器，因为年代、地区和流派的不同，对“十八般兵器”的解说也各异。汇总起来。今天，我们将十八般兵器可以看作是刀、枪、剑、戟、斧、钺、钩、叉、鞭、锏、锤、抓、镗、棍、槊、棒、拐、流星锤。

当然，对于网管而言，不可能让他们去舞刀弄枪，带着大刀长矛去维护服务器。我们这里所说的“十八般兵器”是指在平时使用最普通也是最基础的网络工具。作为一名合格的职业网管，首先就要熟练掌握这些工具。它们不仅仅能够帮助我们行走“江湖”，而且是称为“一代大侠”的前提条件。还在等什么，赶快让我们看看这些武器是哪些吧。

武器一：刀

工具名称：Windows系统内置工具——IPconfig

说明：刀是古代一种用于劈砍的单面侧刃格斗兵器，由刀身和刀柄两部分构成。刀身刃部狭长，刀柄有短柄和长柄之分。在西汉时期，我国刀有了长足发展，最有代表性的为环首刀（也称环柄刀），一般为钢铁制造直背直刃，刀背较厚，刀柄常呈圆环状，刀形细长。两汉时代刀的长度多为1 m左右。

刀有单刀双刀之分。单刀一般较长，计有：斩马刀、柳叶刀、朴刀、雁翎刀、大砍刀等。单刀一般式样较大，重量也大。双刀的式样和重量都较单刀为小，计有：鸳鸯刀、蝴蝶刀等。刀的基本用法有劈、砍、驾、挡、拍等，气势雄伟。刀的好处就是杀敌的效率特别高。

作为普通网管，首先就应该了解系统中最常用，也是使用最方便的“兵器”——IPconfig的用法。它使用简单，功能强大，可以帮助我们解决很多最基本的问题。

IPconfig是内置于Windows的TCP/IP应用程序，用于显示本地计算机网络适配器的物理地址和IP地址等配置信息，这些信息一般用来检验手动配置的TCP/IP设置是否正确。当在网络中使用DHCP服务时，IPconfig可以检测计算机中分配到了什么IP地址，是否配置正确，并且可以释放、重新获取IP地址。这些信息对于网络测试和故障排除有重要的作用。

攻击力：★★　　实用性：★★★

兵器谱

1.查看网络适配器信息

在本地计算机运行不带任何参数的IPconfig命令，可以检测本地网络连接的IP地址配置信息。例如，在本机的命令提示符中直接运行“ipconfig”命令，可以显示所有网络连接的IP地址配置信息，同时也包括ADSL信息，使我们可以了解到ADSL租用了哪个IP地址。在这里显示的IP信息有：IP地址（IP Address）、子网掩码（Subnet Mask）和默认网关（Default Gateway），如图1-1所示。

有时，网络管理员需要得到计算机网卡的MAC地址，用它进行MAC地址绑定、远程管理等，这可以用ipconfig命令加“/all”参数命令来实现。在命令提示符下运行命令：

ipconfig /all

回车，即可显示出本地计算机中所有网卡的MAC地址，如图1-2所示。其中，“Physical Address”显示的就是网卡的MAC地址。

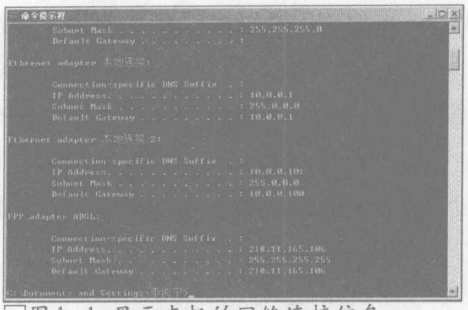

图1-1 显示本机的网络连接信息

同时也显示了该网卡的其他信息，如网卡类型描述信息（Description）、是否启用了DHCP服务（Dhcp Enabled）以及IP地址配置信息等。另外也显示了其他一些Windows配置信息，在“Windows IP Configuration”区域中，显示了主机名（Host Name）、主DNS后缀（Primary Dns Suffix）、节点类型（Node Type）、是否开启了IP路由（IP Routing Enabled）、是否开启了WINS代理（WINS Proxy Enabled）。

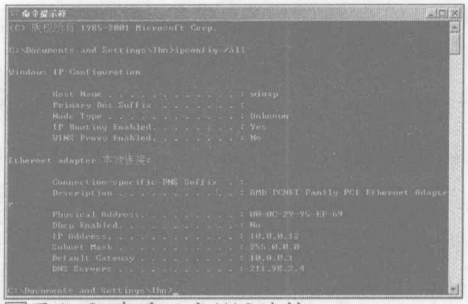

图1-2 查看网卡MAC地址

2. 重新获取IP地址

如果网络中使用了DHCP服务，客户端计算机就可以自动获得IP地址。但有时因DHCP服务器或网络故障等原因，使一些客户端计算机不能正常获得IP地址，此时系统就会自动为网卡分配一个169.254.x.x的IP地址；或者有些计算机IP地址的租约到期，需要更新或重新获得IP地址，这就可以使用ipconfig配合参数-renew和-release来实现。

例如，客户端计算机没有正确获得IP地址时，就需要管理员先将原先获得的IP地址释放掉。在命令提示符下键入如下命令：

ipconfig -release

回车，系统就会将原IP地址释放，释放掉以后，可以看到IP地址和子网掩码均变成 0.0.0.0，然后，就可以重新获得一个新的IP地址了。在命令提示符下键入如下命令：

ipconfig -renew

回车，系统就会自动从DHCP服务器获得一个新的IP地址，以及子网掩码、默认网关等信息，如图1-3所示。

当我们使用ADSL Modem时，也可能会因网络原因造成不能正确获得IP地址，此时也可先使用ipconfig命令释放掉IP地址，然后再重新获得IP地址即可。

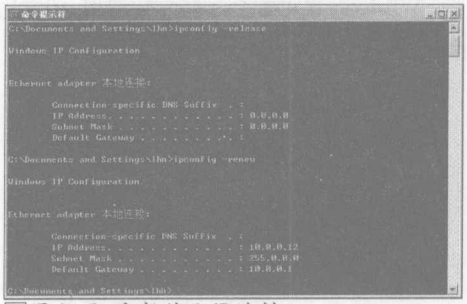

图1-3 重新获取IP地址

3. ipconfig命令参数

在使用Ipconfig命令时，如果不带参数，将只显示简单的IP地址配置信息，如果配合参数使用，还可以实现其他的一些管理功能。ipconfig自带的参数并不多，它的参数为：

ipconfig [-all | -renew [adapter] | -release [adapter]]

参数说明：

-all：显示网卡的完整信息。若不带该参数将只显示IP地址、子网掩码和默认网关。

-renew [adapter]：更新DHCP配置参数。该选项只在运行DHCP客户端服务的系统上可用。要指定适配器名称，可键入使用不带参数的ipconfig命令显示的适配器名称。

-release [adapter]：发布当前的DHCP配置。该选项禁用本地系统上的TCP/IP，并只在 DHCP 客户端上可用。要指定适配器名称，请键入使用不带参数的ipconfig命令显示的适配器名称。

4. Winipcfg

winipcfg命令类似ipconfig命令，同样用于显示IP地址配置信息和网卡的MAC地址，还能以图形窗口的格式显示配置信息，用户还可以修改其中的某些信息。不过，它只存在于Windows 9x/Me/2000 系统。

在MS_DOS窗口或从“开始”菜单中的“运行”中运行“winipcfg”命令，显示如图1-4所示“IP配置”对话框，显示了网卡MAC地址（适配器地址）、IP地址、网关等信息。如果计算机中安装有多块网卡，可在下拉列表中选择其他网卡以查看其信息。

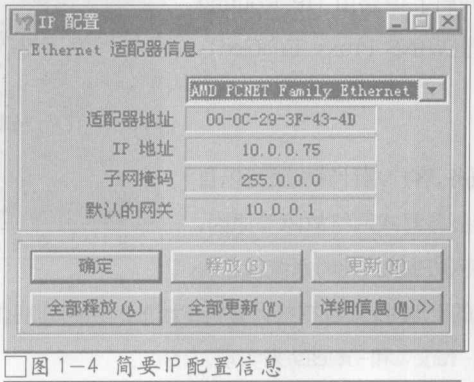

图 1-4 简要IP配置信息

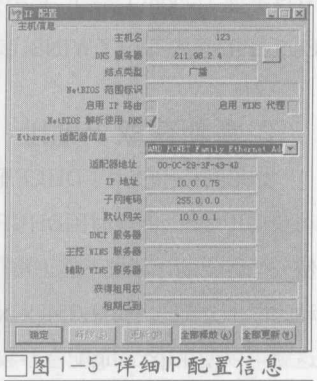

图 1-5 详细IP配置信息

如果网络中安装有DHCP服务器，并且该计算机是自动获得IP地址，单击“释放”按钮可释放网卡的IP地址，并重新获得IP地址；单击“更新”按钮则可更新所获得的IP地址。

如果要查看详细配置信息，单击“详细信息”按钮，显示如图1-5所示对话框，显示了该计算机的主机名、DNS服务器等信息。

Winipcfg也可配合一些参数使用，但常用的命令参数并不多，一般使用“-all”参数用于显示详细配置信息。

武器二：枪

工具名称：网络监控工具——netstat

说明：枪是一种在长柄上装有锐利尖头的兵器。枪的别名叫“肩二”，《清异录》：“蜀王建军中隐语，枪曰‘肩二’。”枪亦称为“一丈威”，《事物异志》：“隋炀帝易枪名为一丈威。”枪的历史可以追溯到原始社会。原始的长枪仅仅是将木棒头削尖而已。《通俗文》：“削木伤盗曰枪。”汉时的枪与矛的形制相似，多以长木杆或竹竿为杆，装上锐长枪头，配以枪缨即制成。枪的种类很多，宋代有双钩枪、单钩枪、锥枪、抓枪、环子枪等。枪以宋、明两代最为盛行，创造了样式繁多。用途各异的枪，广泛运用于步兵和骑兵。

枪是一种刺兵器，杀伤力很大，长而锋利，灵活快速，取胜之法之多，其他兵器难与匹敌，有“百兵之王”的美誉。而对于职业网管而言，能够快速获得电脑的全面而有效的信息，对于处理故障和问题来说相当有用。所以netstat是每个网管必备的“长兵器”！

攻击力：★★　　实用性：★★★

Netstat命令作为Windows内置的一个工具为使用者提供了强大的功能，它可以查看本地TCP、ICMP、UDP、IP协议的使用，查看各个端口的开放情况，显示活动的TCP连接、计算机侦听的端口、以太网统计信息、IP路由表、IPv4统计信息（对于IP、ICMP、TCP和UDP协议）以及IPv6统计信息（对于IPv6、ICMPv6、通过IPv6的 TCP以及通过IPv6的UDP协议）。使用时如果不带参数，netstat显示活动的TCP连接。

1. 语法

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

2.参数说明

-a：显示所有连接和监听端口。

-b：显示包含于创建每个连接或监听端口的可执行组件。在某些情况下已知可执行组件拥有多个独立组件，并且在这些情况下包含于创建连接或监听端口的组件序列被显示。这种情况下，可执行组件名在底部的[ ]中，顶部是其调用的组件，等等，直到TCP/IP部分。注意此选项可能需要很长时间，如果没有足够权限可能失败。

-e：显示以太网统计信息。此选项可以与-s：选项组合使用。

-n：以数字形式显示地址和端口号。

-o：显示与每个连接相关的所属进程ID。

-p proto：显示proto指定的协议的连接；proto可以是下列协议之一：TCP、UDP、TCPv6或UDPv6。如果与-s选项一起使用以显示按协议统计信息，proto可以是下列协议之一：IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP或UDPv6。

-r：显示路由表。

-s：显示按协议统计信息。默认地，显示IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息；

3.实用案例

从以上列举出来的参数来看，netstat的功能是非常强大的，就用也是非常广泛的，可以用看查看实际网络连接，每个端口的状态以及路由表的状态信息等。

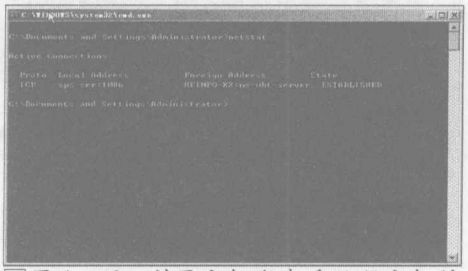

图1-6 利用主机名查看远程主机的NetBIOS名称表

(1)本地计算机的连接情况

当本地计算机访问远程计算机时，或者是本地计算机作为一台服务器来为远程计算机提供服务时，在通讯的过程中都会建立一个连接，如果要查看访问的端口开放情况，就可以在本地计算机的运行netstat命令进行查看，如图1-6所示。

窗口中显示的是本机的所有TCP的连接情况，其中，“Proto”表示协议的名称(TCP或UDP)，“Local Address”表示本地计算机的IP地址和正在使用的端口号。如果不指定 -n 参数，就显示与IP地址和端口的名称对应的本地计算机名称。如果端口尚未建立，端口以星号(*) 显示。“Foreign Address”表示连接远程计算机的IP地址和端口号码。如果端口尚未建立，端口以星号 (*) 显示。“state”表示TCP连接的状态，可能的状态有：“CLOSE_WAIT”、“CLOSED”、“ESTABLISHED”、“FIN_WAIT_1”、“FIN_WAIT_2”、“LAST_ACK”、“LISTEN”、“SYN_RECEIVED”、“SYN_SEND”、“TIMED_WAIT”几种。

(2)查看本机活动的连接情况

当怀疑有可疑的程序在计算机中运行时可以用netstat命令查看与本地计算机端口所建立的连接，这样一来，黑客与木马程序在本地计算机中所开放的与外界通讯所使用的端口将显露无疑，为管理员进一步查杀木马打下了基础。