

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>

刘晓辉
编

QUANNENG WANGGUAN BINGQIPU

全能网管兵器谱

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)

本书如有印刷、装订等质量问题,本社负责调换

版权所有,请勿擅自翻印和用本书

制作各类出版物及配套用书,违者必究

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

武器一：刀

工具名称：Windows 系统内置工具——IPconfig 2

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。作为普通网管而言，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。

武器二：枪

工具名称：网络监控工具——netstat 5

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”！

武器三：叉

工具名称：MAC 地址解析工具——Arp 8

叉是古代作战时长刺武器之一，属十八般兵器之列。在我国民间，每当春节、元宵佳节或庙会及盛行“出会”活动，那寒光闪闪，鸣声铿锵的飞叉表演总是在各种游艺节目的前面，担负着“开路”的任务。对于职业网管来说，的确需要这样一个开路先锋，帮助自己来解决工作中的问题，那么 MAC 地址解析工具——Arp 就可以担当这个任务。

武器四：剑

工具名称：IP 网络连通性测试——Ping 10

剑是武器中传说最多，也最感人的兵器，比如干将、莫邪铸剑的传说就感人至深。对于网管而言，他们可能什么“兵器”都不会使用，但对轻快、敏捷的“Ping”命令一定要能熟练掌握。它不仅是一种实战工具，而且它更是展示网管真正实力的象征。

武器五：戟

工具名称：路径信息提示——Pathping 16

戟初为兵器，后深化为仪仗和装饰物。如帝王驾前卫士执戟侍立。列戟是官爵的象征。富户条案上古瓶中插银戟，取戟与“给”谐音，象征富贵、自给自足。墙壁上挂有戟图，上画之戟，中为双月青龙戟，两旁斜插有单月青龙戟。对于普通网管来说，掌握此类“戟”的功能的确有些困难，但是作为能够进入中高级网管的象征，学会使用“Pathping”命令还是相当有用的。

武器六：弓

工具名称：远程设备登录——Telnet 19

十八般兵器中，弓的地位是相当独特的，其他武器都有替代性，不用枪可以用刀，不用刀可以用鞭；而弓的远程打击能力是独一无二的。由此可见，一名网管如果能够学会远距离处理网络问题的方法，其“攻击力”肯定会提升一个档次。所以像 Telnet 这类“远程武器”肯定是要熟练掌握的。

武器七：槊

工具名称：设备管理控制台——超级终端 24

作为现在用处较少的超级终端，它的很多属性与槊有相似之处，威力巨大但比较笨重；失传已久但及其重要。可能很多网管看到上文，会非常诧异，快失传兵器，还需要掌握吗？答案自然是肯定的，要知道，很多交换机路由器都需要通过超级终端来进行控制，所以一个合格的网络管理员必须懂得如何使用这种“罕见”的常规武器。

武器八：斧

工具名称：文件传输命令——FTP 27

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。

武器九：铜

工具名称：NetBIOS名称解析工具——nbtstat 31

虽然我们普通网管不可能像秦叔宝一样威震大江南北，但是学习几招“撒手铜”还是相当必要的。而nbtstat命令就有这样的效能。它可以很快地解析局域网中多种信息，尤其是NetBIOS名称，是我们平时使用相当频繁的工具。

武器十：拐

工具名称：访问控制列表工具——Showacl 35

我们下面介绍的访问控制列表工具Showacl颇有“拐”的风范，使用它之前，我们先要安装Windows Resource Kit工具软件。但是这个软件使用起来还是相当有用，处理一些疑难杂症相当有效。

武器十一：矛

工具名称：路由跟踪命令——tracert 37

当年张飞当阳桥前喝断流水时，手中握的就是丈八蛇矛。当然网管不可能握着长矛去管理服务器，但是拥有和长矛一样的远距离攻击武器还是相当必要的。比如经常需要使用的路由跟踪命令：tracert。该命令可以查询数据包访问过的路径，帮助读者了解当前网络的一些状况。

武器十二：鞭

工具名称：DNS检测工具——Nslookup 40

如果要想使用好Nslookup，不掌握一定的网络基础知识是不行的。只有在自己拥有一定能力的基础上，才能使用这条“软鞭”，打击“敌人”。

武器十三：匕首

工具名称：计算机计划制定——at 42

匕首作为侠客短兵相接的重要武器，主要是因其短小精悍，携带方便。而at命令也具有同样的功效，虽然只有两个字母，但是她可以制定系统计划，让计划在制定时间和日期执行。其威力相当惊人，如果使用不当，反而会被“黑客”所用。所以网管对此兵器的使用要慎之又慎。

武器十四：锤

工具名称：组策略查看工具——gpresult 46

虽然锤的运用不是很多，但大家对于用锤的名将也应该有所耳闻。锤也非常人可以运用自如的。我们这里介绍的兵器就和锤有相似之处，它就是组策略查看工具gpresult，虽然不常用，但是很必要。因为网管可能随时需要对服务器中组策略进行查看和分析，而该命令简单方便，功能强大。但是如果能力不足之人，使用起来就显得相当费力。

武器十五：钩

工具名称：组策略刷新工具——gpupdate 50

钩是一种多刃的兵器，系由古兵器戈演变而来。而网管所用的“钩”比较独特，他就是组策略刷新工具gpupdate。可以快速刷新本地组策略设置，包括一些安全设置，具有钩灵巧快速的特点。

武器十六：禅杖

工具名称：系统状态备份工具——ntbackup 52

禅杖给人的感觉是大巧若工，大智若愚的感觉。其攻击力不足，但是防御性能强，就如同ntbackup命令一样，多做一些防御性的工作，网管日常管理维护工作非常需要这样的工具。

目录

武器十七：盾牌

工具名称：磁盘数据恢复工具——recover 55

我们讲了很多种攻击武器，对于网络管理员来说，有些时候防御也很重要。如果磁盘出现问题，再强的武器也没有发挥作用的地方，此时使用如盾牌一样的 recover 命令，可以帮我们渡过难关。

武器十八：棍

工具名称：网络工具命令——net 57

棍为无刃兵器，素有“百兵之首”之称。棍的历史悠久，是原始社会主要生产工具之一，也是最早用于战争中的武器之一。棍的攻守兼备，功能强大，是十八般武器中获得最为方便，也是最难以使用的。而 net 命令就是网管手中的棍，它可以让读者轻松解决很多网络问题，而且使用方便，威力巨大。

第2章 江湖独门兵器

武器一：雁翎刀

工具名称：IP 地址管理——IPMaster 69

该形状类似于燕子翅膀的单面刀，造型优美，但是攻击力较弱，最大的好处在于刀身较灵巧。对于我们网络管理员来说，有些时候就需要这样灵巧的“武器”来解决工作上的问题，比如像 IP 地址管理工具——IPMaster。

武器二：柳叶刀

工具名称：局域网监控专家——LanSee 73

在金庸小说当中，我们会经常看到江湖人士使用这样的武器。这类武器轻便而且使用方便，对于应付通常的问题都有自己的解决之道。我们网络管理员也是需要类似的兵器，可以信手拈来，而且使用方便，这里我们推荐使用局域网监控专家——LanSee。

武器三：银弧刀

工具名称：Windows 系统内置工具——IPSubnetter 77

对于我们网络管理员来说，有些工具就如同银弧刀一样，可能使用的机会很少，但是这个工具很管用，比如子网掩码计算工具。一般用户很难使用到这样的软件，但是一旦使用，肯定是很重要的时候。这里，就介绍一款子网掩码计算工具——IPSubnetter。

武器四：九环刀

工具名称：网卡地址获得工具——MAC 扫描器 79

这种比较“霸道”的武器对于网管来说也是非常必要的，比如说在某些时候需要获得一些网络信息时，就需要用一些“强制”手段来完成，如用户的 MAC 地址。这里我们推荐使用 MAC 扫描器，他是专门针对网络中 MAC 地址开发的，相当有用。

武器五：紫金八卦刀

工具名称：超级 IP 工具——IP-Tools 81

对于网管员来说，管理网络就需要这样锋利厚重的“武器”，对于局域网中的一些信息能够轻松获得。我们推荐用户使用超级 IP 工具——IP-Tools。它可以在第一时间获得网络中的运行情况，是网管手中的绝对“利器”。

武器六：紫薇软剑

工具名称：网络故障诊断工具——Netdiag 89

网络管理员最怕的就是遇到网络故障。如果我们随时配一把称心如意的兵刃，遇到这样的问题也不再担心。在这里我们推荐大家使用 Netdiag，她是 WindowsSupport Tools 的一个组件，她可以通过一系列测试来判断局域网的状态，是非常有用的工具，而且它适应性强，附送在 Windows Server 2003 的光

目录

盘当中，也非常容易获得。

武器七：白虹剑

工具名称：局域网助手——LanHelper 93

这里我们推荐读者使用 LanHelper，她是 Windows 平台上局域网的综合管理软件，可以完成大多数高端企业软件才可以完成的工作。它使用起来也相当方便，是普通网管的不二选择。

武器八：真武剑

工具名称：超级网络嗅探器——Sniffer-Pro 102

这里向广大读者介绍一下网管应该掌握的一把“宝剑”——Sniffer-Pro（下文简称 Sniffer）。它可以分析出网络中潜在的问题，帮助网管诊断出大量不可见的模糊问题，而且可以随时发现网络中计算机的异常流量，从而保证整个网络的安全。

武器九：温侯银戟

工具名称：吞吐率测试——Qcheck 111

网络管理员很多时候就需要掌握一些这样的工具，可以随时对局域网进行检测。甚至要把这个兵器掌握得如同自己的双手一样熟练。这个就是网络吞吐率测试工具——Qcheck。它主要通过向网络发送数据流来测试网络的吞吐率、回应时间，从而测试网络的响应时间和数据传输率。非常适合局域网内部进行各种网络性能测试。

武器十：金蛇剑

工具名称：漏洞检测工具——X-Scan 114

金蛇剑可以说是一把具有两面性的武器，在恶人手中，它就是凶神恶煞，但是在大侠手中，就是保护弱小的兵刃。而 X-Scan 也是如此，如果在黑客手中，它就是攻击局域网的绝佳工具，但是在网管手中，它可以帮助网管提升局域网的安全性能。

武器十一：玄铁剑

工具名称：服务器状态监控——Servers Alive 122

有些时候，网络管理员的确需要这样“大巧不工”的工具来帮我们完成一些重要工作，比如检测服务器的运行状况。这里我们推荐使用 Servers Alive，它使用方便，功能强大，完全契合玄铁剑“大巧不工”的属性。

武器十二：飞刀

工具名称：远程控制——pcAnywhere 128

当然，我们这里将飞刀引申出另外一种意义，那就是远距离攻击武器。对于网络管理者来说，凡事不可能亲力亲为，如果能够远程控制，那将会节约我们大量的时间和精力。在这里，我们就向大家介绍一下网管手中的“飞刀”——pcAnywhere。

武器十三：峨眉刺

工具名称：网络探测器——LanExplorer 140

网络管理员有些时候也需要这样一种武器，使用灵活，而且攻击力强大，这里我们就来看看这样一种武器：网络探测器——LanExplorer。网管利用该软件搜索同时在局域网上的所有的工作组、主机、打印机、共享文件，也可以自动搜索所有共享的其他资源。这样便于网管观察到网络中的各种共享资源，便于发现一些安全隐患。

武器十四：金钱镖

工具名称：路由拓扑利器——VisualNET 149

网管需要了解网络中设备的各种拓扑结构，这个时候用户可能就需要这样的远程暗器，不用惊动他人，在自己电脑上生成相关的数据。这里我们推荐大家使用 VisualNET，它可以实现对所有 IP 编址

目录

的网络设备的自动识别、拓扑发现、状态监视、服务监视、流量监视、事件报警等等，其中设备识别和拓扑发现功能比普通软件强大很多。

武器十五：锁喉枪

工具名称：网络服务器异常监控——IP Sentry 162

对于网管员来说，管理网络有时就需要这样一种能够一枪“锁喉”的武器。很多网络管理员最怕遇到的问题就是网络服务器的异常，这是因为这种异常要么不出现，一旦出现，就可能是非常严重的问题，如果能够及时发现些问题，网络管理员就可以将局域网中的损失减少到最小。这里，我们推荐用户使用网络服务器异常监控——IP Sentry。它可以说是网管手中的“锁喉枪”，一手掌控服务器的“生命线”。

武器十六：子午鸳鸯钺

工具名称：端口监控工具——Port Reporter 171

在管理网络时，有些时候我们就需要这样一种变化多端、短小使用的工具来监控服务器的端口。这里我们推荐用户使用端口监控工具——Port Reporter。它可以监控服务器的端口运行情况，随时掌握服务器端口的异常状况。

武器十七：紫七星刀

工具名称：多线程扫描器——SoftPerfect Network Scanner 175

对网管员来说，有时就需要使用一些简单有效的工具来扫描系统，这种方法虽然简单，但是非常有效。我们推荐用户使用多线程扫描器——SoftPerfect Network Scanner。它可以快速扫描服务器中的各种线程，确保服务器的安全。

第3章 传世的神兵利器

武器一：承影

工具名称：思科交换机管理工具——CNA 179

在我们网络管理中，也有这样一把“承影”剑，那就是思科网络助理（CAN），它可以帮助用户对局域网设备进行图形化管理，是一个用户界面非常友好的配置工具。它可以帮助网络管理员优雅地处理网络中各种日常管理工作。

武器二：七星龙渊

工具名称：使用SDM配置路由器 197

对于广大网管来说，他们能够管理并部署思科的路由器是一件值得兴奋的事情，因为它标志着你的技术达到了一定的水平，同时也得到了认可。那么要管理这些昂贵的设备，自然需要掌握一把“高贵”的武器。这里，我们就向大家介绍一下Cisco SDM路由器配置软件的使用方法。

武器三：泰阿

工具名称：Cisco ASDM配置安全设备 209

对于我们网络管理员来说，日常工作中最重要的就是网络安全问题，如果管理不当，就会让一些不法之徒有了可乘之机。这里就向大家介绍这样一把威道之剑——Cisco ASDM安全设备管理器，

武器四：鱼肠剑

工具名称：思科产品动态配置工具 224

对于网络管理员来说，在对思科网络设备进行选购是会遇到各种各样的问题，此时我们也需要这样一把使用方便，能够解决问题的“鱼肠剑”，这里，我们推荐大家使用思科产品动态配置工具，它就像是菜谱一样，用户可以自由选择搭配符合自己要求的网络设备，使用非常方便有效。

武器五：湛卢剑

目录

工具名称:HP OpenView NNM	227
----------------------------	-----

在局域网中,各种交换机路由器就如同君王、诸侯一样,他们的异动会直接影响整个局域网的性能,所以我们网管手中必须有一把“湛卢剑”,来监控网络中各种设备的异动。这里,我们就向大家介绍一下网络/系统管理解决方案——HP OpenView 的使用方法。

武器六:纯钧剑

工具名称:CiscoWorks 2000	250
----------------------------	-----

同样的,对于网络管理员来说,思科公司的 CiscoWorks 系统可以说是一把“纯钧剑”,它功能强大,性能优秀,可以有效地管理局域网中各种思科设备,是高级网管必知软件。相信高级网络管理人员掌握该软件后,一定会大大提升自己的网络管理能力。

武器七:赤霄

工具名称:广通网管系统(Broadcom IT-View Lancop)	256
--	-----

并不是每个网管都有机会接触各种思科设备和管理软件,但是他们平时又不得不去管理这些网络设备。这个时候就需要第三方的管理软件来帮助我们解决问题。这里,我们就向大家介绍一下广通网管系统(Broadcom IT-View Lancop),它可以实现大多数网络管理功能,是一款不可多得的网络管理软件。

第4章 少林七十二式

兵器一:少林马步

工具名称:MOM 2005 入门简介	273
--------------------------	-----

对于学习 MOM 2005 的网管来说,首先要做的肯定是练习基本的“马步”——该软件的基本知识。这些看似简单的知识,在实际工作中相当重要,如果相关内容理解不当,会给日后的工作带来很多不必要的麻烦。现在让我们开始快速掌握相关的知识。

兵器二:少林罗汉拳

工具名称:微软操作系统管理专家——Microsoft Operations Manager 2005	277
--	-----

我们这里介绍的是 MOM 2005 的基本安装方法和使用介绍,可以说是网管的入门学习的“罗汉拳”。虽然内容比较简单,但是作为“正宗功夫”的入门,读者还是需要认真阅读,否则对日后学习造成一定的困难。

兵器三:少林棍

工具名称:MOM 2005 监控平台的使用	315
-----------------------------	-----

前面我们介绍了几种“少林功夫”,可以说是一些入门的功夫,现在介绍的是真正的正宗功夫:“少林棍”——MOM 2005 监控平台的使用。它是 MOM 2005 的核心,只有真正了解了监控平台的应用方法,网络管理员才能真正了解该软件如何管理局域网中的服务器。

兵器四:少林刀

工具名称:Active Directory 监控组件	327
----------------------------------	-----

说到刀法,我们这里就不得不提及 MOM 2005 的 Active Directory 监控组件,这个组件可以说是该软件的精华所在,它可以快速提升用户对服务器的管理和监控能力,可以这样说,掌握了它,你就是服务器的“统帅”,服务器的大部分功能你都可以得到监控,而且可以应用自如。

兵器五:少林剑

工具名称:SQLServer 监控组件	336
---------------------------	-----

这里我们向大家推荐 MOM 2005 的 SQLServer 的监控组件,虽然不是每个人都需要用到它,但是一旦出现问题,它会发挥其独特的功能,帮助网管完成任务。

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臆、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、铜、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，刀柄窄呈圆环状，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。

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)。

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。

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:

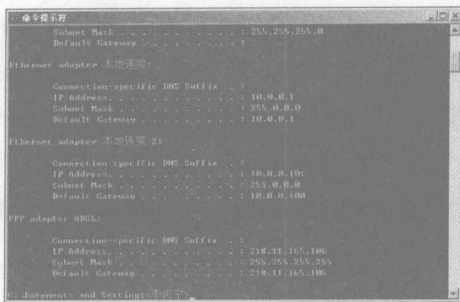


图1-1 显示本机的网络连接信息

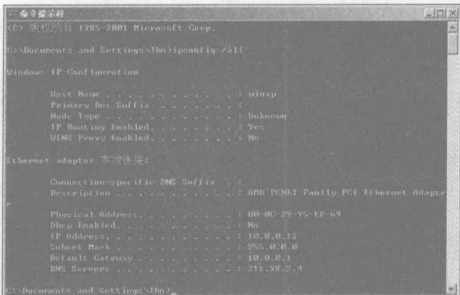


图1-2 查看网卡MAC地址

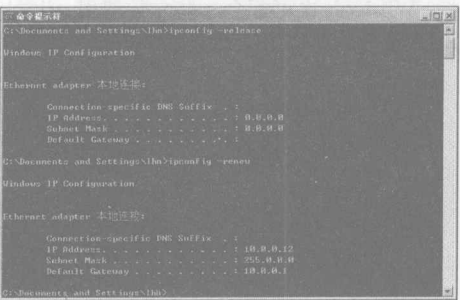


图1-3 重新获取IP地址

-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。

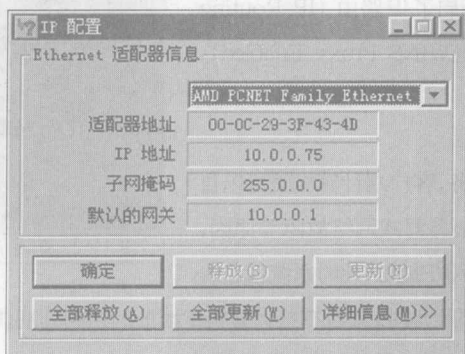


图1-4 简要IP配置信息

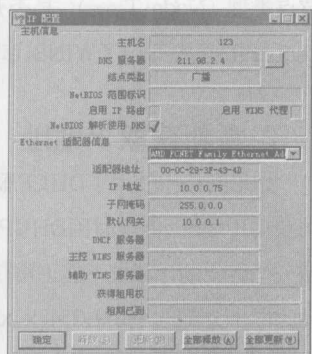


图1-5 详细IP配置信息

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：★★★★

兵器谱

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。

(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。

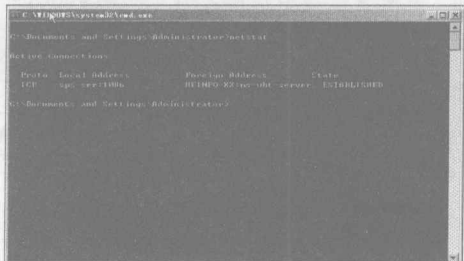


图 1-6 利用主机名查看远程主机的 NetBIOS 名称表

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。