**常用端口号与对应的服务以及端口关闭**

端口简介：本文介绍端口的概念，分类，以及如何关闭/开启一个端口

　　21端口：21端口主要用于FTP（File Transfer Protocol，文件传输协议）服务。

　　23端口：23端口主要用于Telnet（远程登录）服务，是Internet上普遍采用的登录和仿真程序。

　　25端口：25端口为SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）服务器所开放，主要用于发送邮件，如今绝大多数邮件服务器都使用该协议。

　　53端口：53端口为DNS（Domain Name Server，域名服务器）服务器所开放，主要用于域名解析，DNS服务在NT系统中使用的最为广泛。

　　67、68端口：67、68端口分别是为Bootp服务的Bootstrap Protocol Server（引导程序协议服务端）和Bootstrap Protocol Client（引导程序协议客户端）开放的端口。

　　69端口：TFTP是Cisco公司开发的一个简单文件传输协议，类似于FTP。

　　79端口：79端口是为Finger服务开放的，主要用于查询远程主机在线用户、操作系统类型以及是否缓冲区溢出等用户的详细信息。

　　80端口：80端口是为HTTP（HyperText Transport Protocol，超文本传输协议）开放的，这是上网冲浪使用最多的协议，主要用于在WWW（World Wide Web，万维网）服务上传输信息的协议。

　　99端口：99端口是用于一个名为“Metagram Relay”（亚对策延时）的服务，该服务比较少见，一般是用不到的。

　　109、110端口：109端口是为POP2（Post Office Protocol Version 2，邮局协议2）服务开放的，110端口是为POP3（邮件协议3）服务开放的，POP2、POP3都是主要用于接收邮件的。

　　111端口：111端口是SUN公司的RPC（Remote Procedure Call，远程过程调用）服务所开放的端口，主要用于分布式系统中不同计算机的内部进程通信，RPC在多种网络服务中都是很重要的组件。

　　113端口：113端口主要用于Windows的“Authentication Service”（验证服务）。

　　119端口：119端口是为“Network News Transfer Protocol”（网络新闻组传输协议，简称NNTP）开放的。

　　135端口：135端口主要用于使用RPC（Remote Procedure Call，远程过程调用）协议并提供DCOM（分布式组件对象模型）服务。

　　137端口：137端口主要用于“NetBIOS Name Service”（NetBIOS名称服务）。

　　139端口：139端口是为“NetBIOS Session Service”提供的，主要用于提供Windows文件和打印机共享以及Unix中的Samba服务。

　　143端口：143端口主要是用于“Internet Message Access Protocol”v2（Internet消息访问协议，简称IMAP）。

　　161端口：161端口是用于“Simple Network Management Protocol”（简单网络管理协议，简称SNMP）。

　　443端口：43端口即网页浏览端口，主要是用于HTTPS服务，是提供加密和通过安全端口传输的另一种HTTP。

　　554端口：554端口默认情况下用于“Real Time Streaming Protocol”（实时流协议，简称RTSP）。

　　1024端口：1024端口一般不固定分配给某个服务，在英文中的解释是“Reserved”（保留）。

　　1080端口：1080端口是Socks代理服务使用的端口，大家平时上网使用的WWW服务使用的是HTTP协议的代理服务。

　　1755端口：1755端口默认情况下用于“Microsoft Media Server”（微软媒体服务器，简称MMS）。

　　4000端口：4000端口是用于大家经常使用的QQ聊天工具的，再细说就是为QQ客户端开放的端口，QQ服务端使用的端口是8000。

　　5554端口：在今年4月30日就报道出现了一种针对微软lsass服务的新蠕虫病毒——震荡波（Worm.Sasser），该病毒可以利用TCP 5554端口开启一个FTP服务，主要被用于病毒的传播。

　　5632端口：5632端口是被大家所熟悉的远程控制软件pcAnywhere所开启的端口。

　　8080端口：8080端口同80端口，是被用于WWW代理服务的，可以实现网页

端口概念

　　在网络技术中，端口（Port）大致有两种意思：一是物理意义上的端口，比如，ADSL Modem、集线器、交换机、路由器用于连接其他网络设备的接口，如RJ-45端口、SC端口等等。二是逻辑意义上的端口，一般是指TCP/IP协议中的端口，端口号的范围从0到65535，比如用于浏览网页服务的80端口，用于FTP服务的21端口等等。我们这里将要介绍的就是逻辑意义上的端口。

端口分类

　　逻辑意义上的端口有多种分类标准，下面将介绍两种常见的分类：

1. 按端口号分布划分

　　（1）知名端口（Well-Known Ports）

　　知名端口即众所周知的端口号，范围从0到1023，这些端口号一般固定分配给一些服务。比如21端口分配给FTP服务，25端口分配给SMTP（简单邮件传输协议）服务，80端口分配给HTTP服务，135端口分配给RPC（远程过程调用）服务等等。

　　（2）动态端口（Dynamic Ports）

　　动态端口的范围从1024到65535，这些端口号一般不固定分配给某个服务，也就是说许多服务都可以使用这些端口。只要运行的程序向系统提出访问网络的申请，那么系统就可以从这些端口号中分配一个供该程序使用。比如1024端口就是分配给第一个向系统发出申请的程序。在关闭程序进程后，就会释放所占用的端口号。

　　不过，动态端口也常常被病毒木马程序所利用，如冰河默认连接端口是7626、WAY 2.4是8011、Netspy 3.0是7306、YAI病毒是1024等等。

2. 按协议类型划分

　　按协议类型划分，可以分为TCP、UDP、IP和ICMP（Internet控制消息协议）等端口。下面主要介绍TCP和UDP端口：

　　（1）TCP端口

　　TCP端口，即传输控制协议端口，需要在客户端和服务器之间建立连接，这样可以提供可靠的数据传输。常见的包括FTP服务的21端口，Telnet服务的23端口，SMTP服务的25端口，以及HTTP服务的80端口等等。

　　（2）UDP端口

　　UDP端口，即用户数据包协议端口，无需在客户端和服务器之间建立连接，安全性得不到保障。常见的有DNS服务的53端口，SNMP（简单网络管理协议）服务的161端口，QQ使用的8000和4000端口等等。

查看端口

　　在Windows 2000/XP/Server 2003中要查看端口，可以使用Netstat命令：

　　依次点击“开始→运行”，键入“cmd”并回车，打开命令提示符窗口。在命令提示符状态下键入“netstat -a -n”，按下回车键后就可以看到以数字形式显示的TCP和UDP连接的端口号及状态（如图）。

　　小知识：Netstat命令用法

　　命令格式：Netstat －a －e －n －o －s

　　－a 表示显示所有活动的TCP连接以及计算机监听的TCP和UDP端口。

　　－e 表示显示以太网发送和接收的字节数、数据包数等。

　　－n 表示只以数字形式显示所有活动的TCP连接的地址和端口号。

　　－o 表示显示活动的TCP连接并包括每个连接的进程ID（PID）。

　　－s 表示按协议显示各种连接的统计信息，包括端口号。

关闭/开启端口

　　在介绍各种端口的作用前，这里先介绍一下在Windows中如何关闭/打开端口，因为默认的情况下，有很多不安全的或没有什么用的端口是开启的，比如Telnet服务的23端口、FTP服务的21端口、SMTP服务的25端口、RPC服务的135端口等等。为了保证系统的安全性，我们可以通过下面的方法来关闭/开启端口。

　　关闭端口

　　比如在Windows 2000/XP中关闭SMTP服务的25端口，可以这样做：首先打开“控制面板”，双击“管理工具”，再双击“服务”。接着在打开的服务窗口中找到并双击“Simple Mail Transfer Protocol （SMTP）”服务，单击“停止”按钮来停止该服务，然后在“启动类型”中选择“已禁用”，最后单击“确定”按钮即可。这样，关闭了SMTP服务就相当于关闭了对应的端口。

　　开启端口

　　如果要开启该端口只要先在“启动类型”选择“自动”，单击“确定”按钮，再打开该服务，在“服务状态”中单击“启动”按钮即可启用该端口，最后，单击“确定”按钮即可。

　　提示：在Windows 98中没有“服务”选项，你可以使用防火墙的规则设置功能来关闭/开启端口。  
79端口

　　端口说明：79端口是为Finger服务开放的，主要用于查询远程主机在线用户、操作系统类型以及是否缓冲区溢出等用户的详细信息。比如要显示远程计算机www.abc.com上的user01用户的信息，可以在命令行中键入“finger user01@www.abc.com”即可。

　　端口漏洞：一般黑客要攻击对方的计算机，都是通过相应的端口扫描工具来获得相关信息，比如使用“流光”就可以利用79端口来扫描远程计算机操作系统版本，获得用户信息，还能探测已知的缓冲区溢出错误。这样，就容易遭遇到黑客的攻击。而且，79端口还被Firehotcker木马作为默认的端口。

　　操作建议：建议关闭该端口。  
80端口

　　端口说明：80端口是为HTTP（HyperText Transport Protocol，超文本传输协议）开放的，这是上网冲浪使用最多的协议，主要用于在WWW（World Wide Web，万维网）服务上传输信息的协议。我们可以通过HTTP地址加“:80”（即常说的“网址”）来访问网站的，比如http://www.cce.com.cn:80，因为浏览网页服务默认的端口号是80，所以只要输入网址，不用输入“:80”。

　　端口漏洞：有些木马程序可以利用80端口来攻击计算机的，比如Executor、RingZero等。

　　操作建议：为了能正常上网冲浪，我们必须开启80端口。  
109与110端口

　　端口说明：109端口是为POP2（Post Office Protocol Version 2，邮局协议2）服务开放的，110端口是为POP3（邮件协议3）服务开放的，POP2、POP3都是主要用于接收邮件的，目前POP3使用的比较多，许多服务器都同时支持POP2和POP3。客户端可以使用POP3协议来访问服务端的邮件服务，如今ISP的绝大多数邮件服务器都是使用该协议。在使用电子邮件客户端程序的时候，会要求输入POP3服务器地址，默认情况下使用的就是110端口（如图）。

　　端口漏洞：POP2、POP3在提供邮件接收服务的同时，也出现了不少的漏洞。单单POP3服务在用户名和密码交换缓冲区溢出的漏洞就不少于20个，比如WebEasyMail POP3 Server合法用户名信息泄露漏洞，通过该漏洞远程攻击者可以验证用户账户的存在。另外，110端口也被ProMail trojan等木马程序所利用，通过110端口可以窃取POP账号用户名和密码。

　　操作建议：如果是执行邮件服务器，可以打开该端口。  
135端口

　　端口说明：135端口主要用于使用RPC（Remote Procedure Call，远程过程调用）协议并提供DCOM（分布式组件对象模型）服务，通过RPC可以保证在一台计算机上运行的程序可以顺利地执行远程计算机上的代码；使用DCOM可以通过网络直接进行通信，能够跨包括HTTP协议在内的多种网络传输。

　　端口漏洞：相信去年很多Windows 2000和Windows XP用户都中了“冲击波”病毒，该病毒就是利用RPC漏洞来攻击计算机的。RPC本身在处理通过TCP/IP的消息交换部分有一个漏洞，该漏洞是由于错误地处理格式不正确的消息造成的。该漏洞会影响到RPC与DCOM之间的一个接口，该接口侦听的端口就是135。

　　操作建议：为了避免“冲击波”病毒的攻击，建议关闭该端口  
　137端口

　　端口说明：137端口主要用于“NetBIOS Name Service”（NetBIOS名称服务），属于UDP端口，使用者只需要向局域网或互联网上的某台计算机的137端口发送一个请求，就可以获取该计算机的名称、注册用户名，以及是否安装主域控制器、IIS是否正在运行等信息。

　　端口漏洞：因为是UDP端口，对于攻击者来说，通过发送请求很容易就获取目标计算机的相关信息，有些信息是直接可以被利用，并分析漏洞的，比如IIS服务。另外，通过捕获正在利用137端口进行通信的信息包，还可能得到目标计算机的启动和关闭的时间，这样就可以利用专门的工具来攻击。

　　操作建议：建议关闭该端口。  
　139端口

　　端口说明：139端口是为“NetBIOS Session Service”提供的，主要用于提供Windows文件和打印机共享以及Unix中的Samba服务。在Windows中要在局域网中进行文件的共享，必须使用该服务。比如在Windows 98中，可以打开“控制面板”，双击“网络”图标，在“配置”选项卡中单击“文件及打印共享”按钮选中相应的设置就可以安装启用该服务；在Windows 2000/XP中，可以打开“控制面板”，双击“网络连接”图标，打开本地连接属性；接着，在属性窗口的“常规”选项卡中选择“Internet协议（TCP/IP）”，单击“属性”按钮；然后在打开的窗口中，单击“高级”按钮；在“高级TCP/IP设置”窗口中选择“WINS”选项卡，在“NetBIOS设置”区域中启用TCP/IP上的NetBIOS。

　　端口漏洞：开启139端口虽然可以提供共享服务，但是常常被攻击者所利用进行攻击，比如使用流光、SuperScan等端口扫描工具，可以扫描目标计算机的139端口，如果发现有漏洞，可以试图获取用户名和密码，这是非常危险的

现在学入侵的刚开始大多都是利用135端口和3389端口~~~~听人说在默认情况下端口是开放的~~~但是我扫了N多IP还没找到一个开135端口的电脑~~~以下是关闭端口的方法~~是否正确有待考证（反正我是照上边做的~）  
默认情况下，Windows有很多端口是开放的，在你上网的时候，网络病毒和黑客可以通过这些端口连上你的电脑。为了让你的系统变为铜墙铁壁，应该封闭这些端口，主要有：TCP 135、139、445、593、1025 端口和 UDP 135、137、138、445 端口，一些流行病毒的后门端口（如 TCP 2745、3127、6129 端口），以及远程服务访问端口3389。下面介绍如何在WinXP/2000/2003下关闭这些网络端口：  
第一步，点击“开始”菜单/设置/控制面板/管理工具，双击打开“本地安全策略”，选中“IP 安全策略，在本地计算机”，在右边窗格的空白位置右击鼠标，弹出快捷菜单，选择“创建 IP 安全策略”，于是弹出一个向导。在向导中点击“下一步”按钮，为新的安全策略命名；再按“下一步”，则显示“安全通信请求”画面，在画面上把“激活默认相应规则”左边的钩去掉，点击“完成”按钮就创建了一个新的IP 安全策略。

第二步，右击该IP安全策略，在“属性”对话框中，把“使用添加向导”左边的钩去掉，然后单击“添加”按钮添加新的规则，随后弹出“新规则属性”对话框，在画面上点击“添加”按钮，弹出IP筛选器列表窗口；在列表中，首先把“使用添加向导”左边的钩去掉，然后再点击右边的“添加”按钮添加新的筛选器。   
第三步，进入“筛选器属性”对话框，首先看到的是寻址，源地址选“任何 IP 地址”，目标地址选“我的 IP 地址”；点击“协议”选项卡，在“选择协议类型”的下拉列表中选择“TCP”，然后在“到此端口”下的文本框中输入“135”，点击“确定”按钮，这样就添加了一个屏蔽 TCP 135（RPC）端口的筛选器，它可以防止外界通过135端口连上你的电脑。

点击“确定”后回到筛选器列表的对话框，可以看到已经添加了一条策略，重复以上步骤继续添加 TCP 137、139、445、593 端口和 UDP 135、139、445 端口，为它们建立相应的筛选器。

重复以上步骤添加TCP 1025、2745、3127、6129、3389 端口的屏蔽策略，建立好上述端口的筛选器，最后点击“确定”按钮。

第四步，在“新规则属性”对话框中，选择“新 IP 筛选器列表”，然后点击其左边的圆圈上加一个点，表示已经激活，最后点击“筛选器操作”选项卡。在“筛选器操作”选项卡中，把“使用添加向导”左边的钩去掉，点击“添加”按钮，添加“阻止”操作（右图）：在“新筛选器操作属性”的“安全措施”选项卡中，选择“阻止”，然后点击“确定”按钮。

第五步、进入“新规则属性”对话框，点击“新筛选器操作”，其左边的圆圈会加了一个点，表示已经激活，点击“关闭”按钮，关闭对话框；最后回到“新IP安全策略属性”对话框，在“新的IP筛选器列表”左边打钩，按“确定”按钮关闭对话框。在“本地安全策略”窗口，用鼠标右击新添加的 IP 安全策略，然后选择“指派”。

于是重新启动后，电脑中上述网络端口就被关闭了，病毒和黑客再也不能连上这些端口，从而保护了你的电脑。

以下是常用的一些股票软件使用的通讯端口：  
东方证券行情系统 TCP:8601  
东方证券委托系统 TCP:8002,8003,8004  
大智慧新一代高速行情分析系统 TCP:5188 TCP:6188  
大智慧证券信息港 TCP:22221、22223、22224  
广发证券至强版（国信证券鑫网通达信行情交易软件也同时会用到TCP:7708,7709） TCP:7711,7708,7709,7727  
招商证券全能版 TCP:7711,7708,7709,7727