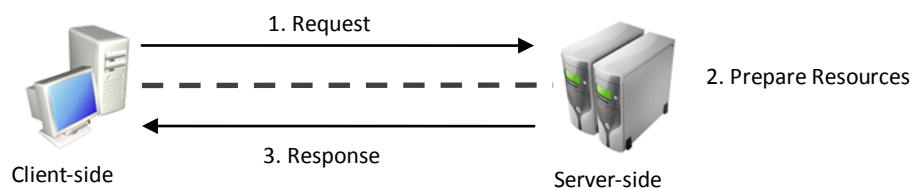


# Web 应用基础 - Lab 1

2009.2.20

## Web 服务器

在网络中为实现信息发布、资料查询、数据处理等诸多应用搭建基本平台的服务器。Web 服务器可以解析 HTTP 协议。当 Web 服务器接收到一个 HTTP 请求(request)，会返回一个 HTTP 响应 (response)，例如送回一个 HTML 页面。为了处理一个请求(request)，Web 服务器可以响应(response)一个静态页面或图片，进行页面跳转(redirect)，或者把动态响应(dynamic response)的产生委托(delegate)给一些其它的程序例如 CGI 脚本、JSP 脚本、servlets 或 ASP 脚本等服务器端(server-side)技术。工作原理大致如下图。



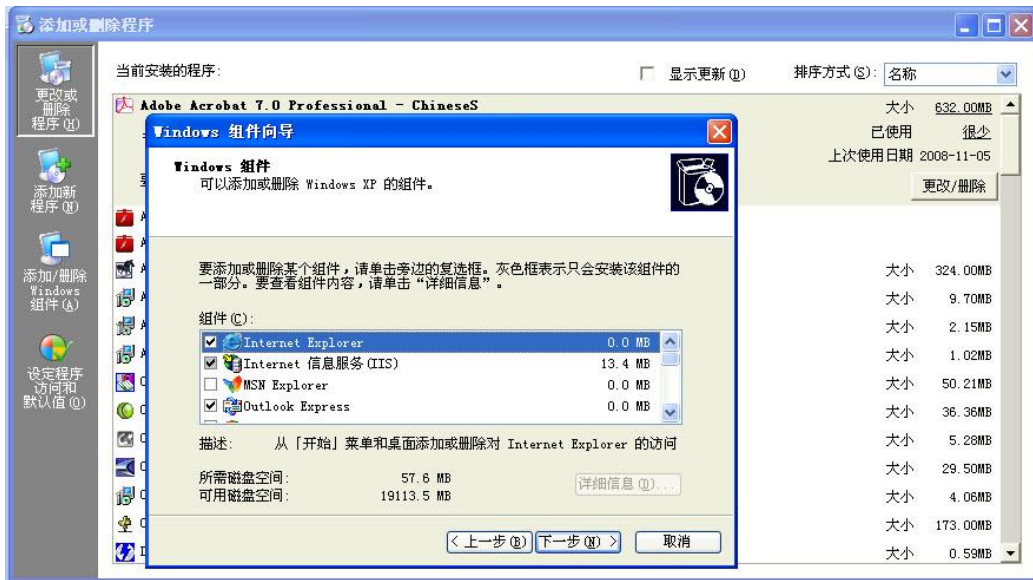
## Web 服务器软件

安装在 Web 服务器端用来配置服务器资源、处理用户请求的软件。主流的 Web 服务器软件有：Microsoft IIS、IBM WebSphere、BEA WebLogic、Apache、Apache Tomcat 等。

# 1 Microsoft IIS 的安装与配置

## IIS 的安装

网上下载 IIS5.1 或 IISXP 安装文件，或者从 WINDOWS XP 系统安装盘中直接安装。  
安装 IIS 组件，在添加或删除程序界面上，点击添加/删除 Windows 组件，弹出对话框如下图所示，选中 Internet 信息服务(IIS)项。



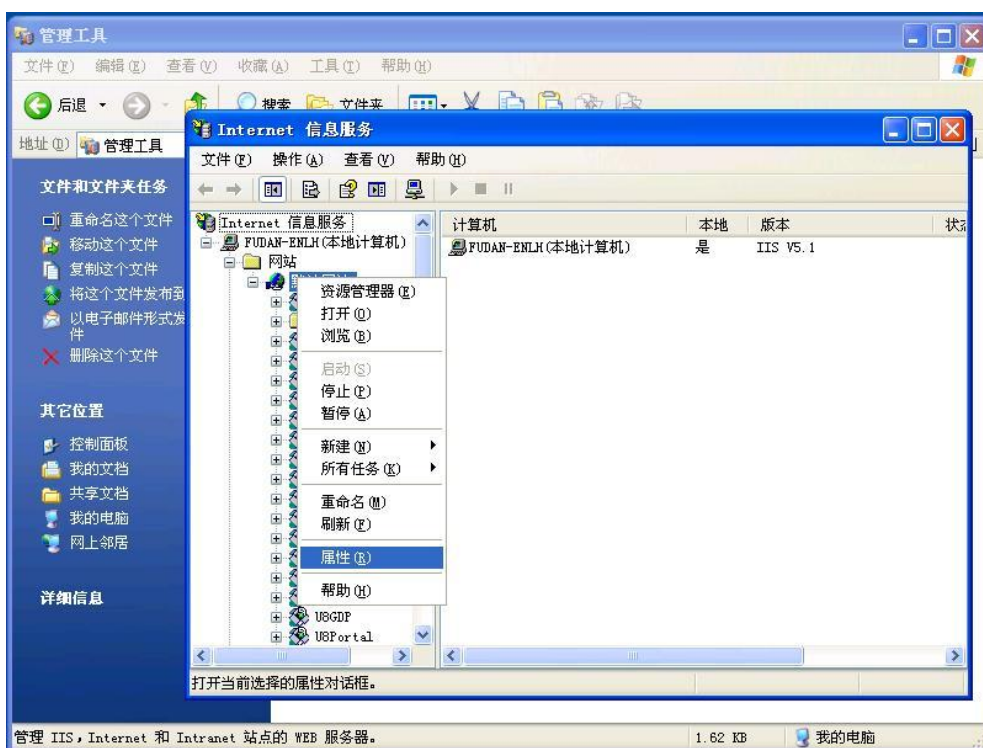
点击下一步，安装过程要求用户确认 IIS 组件的安装文件位置，默认是系统安装光盘，否则通过浏览文件夹选择下载好的 IIS 组件安装文件所在的位置。然后按照提示，完成其余的安装过程。

在浏览器中输入 <http://127.0.0.1>，如果出现下面的页面，说明 IIS 安装成功。



## IIS 的配置

IIS 参数配置主要通过 Windows 系统自带的 Internet 信息服务管理工具进行。如下图所示。



点击属性，可以在弹出的窗口中配置 IIS 服务器的参数，包括 TCP 端口、客户端连接时间限制、服务器主目录及其安全等配置，当然，也可以在特定网站的属性窗口中对网站进行单独的参数配置。

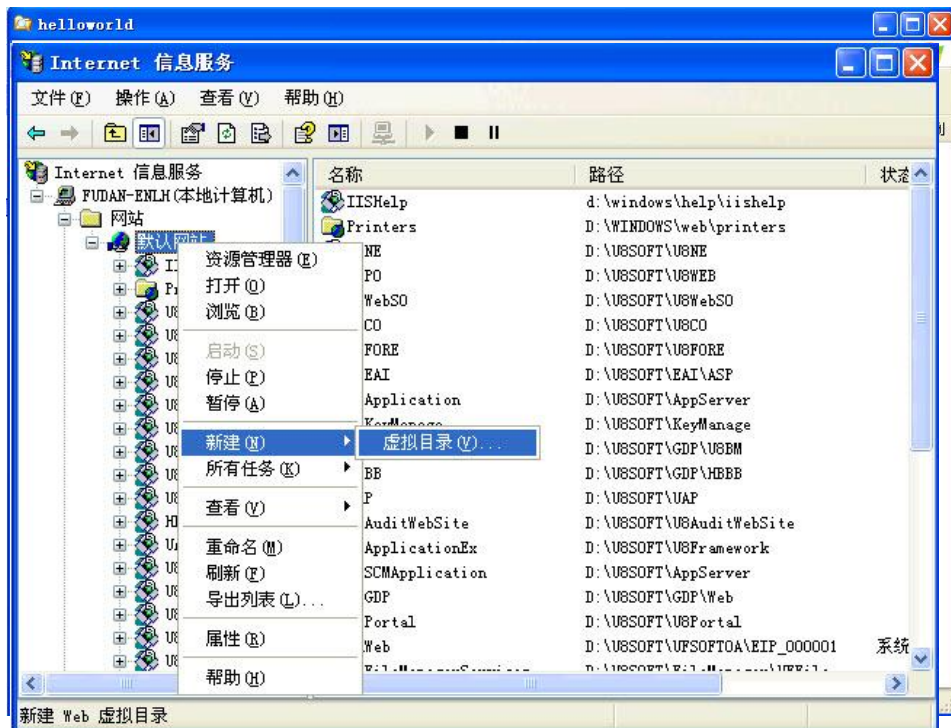


在不指定端口的情况下，TCP 默认端口为 80。若 IIS 将 TCP 端口设为 80，则在访问该服务器资源时无需指定端口号。

## 简单的网站部署

XP 下的 IIS5.1 对 ASP、ASP.NET 的支持很充分，而对 PHP、JSP 等其他语言则需要通过安装其他插件才能够支持。比较简单的网站部署如下所示：

将要发布的网站准备好，包括目录层次以及文件。比如，发布 D:\inetpub\wwwroot\helloworld 文件夹下的所有文件：



在 Internet 信息管理的默认网站下新建新的虚拟目录，如下图所示。

输入虚拟目录的别名 HelloWorldWebSite，然后将虚拟目录指向 D:\inetpub\wwwroot\helloworld，创建成功后，默认网站的树形结构上将会出现网站 HelloWorldWebSite。

在浏览器中输入 <http://127.0.0.1/HelloWorldWebSite/TEST4.html>，测试部署是否成功。

可以修改 HelloWorldWebSite 站点的属性（通过该网站下的属性窗口修改），然后检查该站点对客户端请求的控制是否正确，比如允许客户端浏览站点、站点的默认主页等。

### 练习：

将目录 IIS\_Test 部署到 IIS 服务器，使访问以下网址访问时显示 iis.html 的内容。

<http://127.0.0.1:8000/IIS/>

## 2 Apache Tomcat 的安装与配置

Tomcat 服务器是一个免费的开放源代码的 Web 应用服务器，目前最新版本是 6.0.18(截止至 2009-2-20)。Tomcat 是一个小型的轻量级应用服务器，在中小型系统和并发访问用户不是很多的场合下被普遍使用，是开发和调试 JSP 程序的首选。

### 官方下载

官方网站: <http://tomcat.apache.org/>

左侧导航栏 Download 下选择 [Tomcat 6.x](#)。

选择适当的下载镜像。

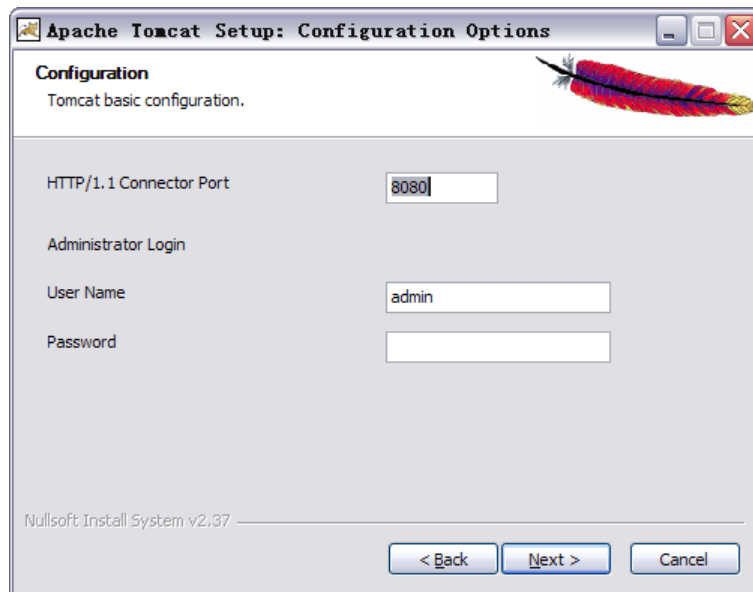
在 Binary Distributions 下选择任意文件格式下载。

### Tomcat 的安装

#### - WSI 安装

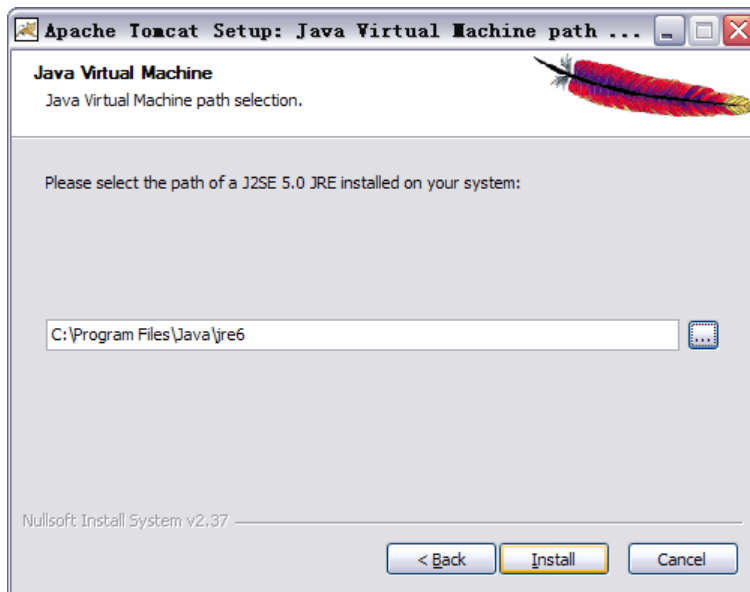
若使用 Windows Service Installer 进行安装：运行 apache-tomcat-6.0.18.exe。

点击 Next 或 I Agree 直到出现如下界面：




设置 HTTP 连接的端口号，默认使用 8080。

下面是 Tomcat 后台管理员登陆的账户设置，自由设置，Next。



为 Tomcat 设置 Java 运行库(Tomcat 6 需要 J2SE5.0 以上的运行库, Java 运行库默认安装路径为 C:\Program File\Java\jre+版本号目录或 C:\Program File\Java\jdk+版本号下的 jre 目录下)。选择完毕后 Install。完成后可以选择运行 Tomcat。

双击右下角状态栏的  图标, 可以配置 Tomcat 的一些属性, 并控制 Tomcat 服务的开始或结束。点击 General 面板下的 Start 按钮, 服务器就开始运转了。

#### - zip/tar.gz 安装

若使用压缩包进行部署, 首先配置环境变量。右击“我的电脑”选择“属性”, 在“高级”选项卡下点击“环境变量”按钮。在系统变量中新建变量名为“JAVA\_HOME”, 值为 JDK 或 JRE 的目录, 如“C:\Program Files\Java\jre6”。确定。



将压缩包中的 `apache-tomcat-6.0.18` 文件夹解压到想要安装 Tomcat 的位置。运行该文件夹下 `bin` 目录下的 `startup.bat`, 就启动了 Tomcat。同一目录下的 `shutdown.bat` 用来停止服务。

在使用 **WSI** 或压缩包安装并启动 Tomcat 后,

使用浏览器访问 <http://localhost:8080/>, 如果见到如下界面, 则说明 Tomcat 安装成功。



## Tomcat 的简单配置

在 <http://localhost:8080/> 显示的 Tomcat 默认主页左上角, 提供了管理功能, 必须使用管理员帐户才可登陆。

若使用的是 WSI 安装, 则安装过程中曾配置过一个具有管理员权限的账户, 可使用该账户进行登录管理。

若使用压缩包进行安装, 则需要打开 `conf` 文件夹下的 `tomcat-users.xml`, 在 `<tomcat-users>` 元素中插入一条用户数据并保存:

```
<user name="admin" password="secret" roles="manager" />
```

重启 Tomcat 服务, 就可以进入 Status 和 Tomcat Manager 界面进行管理。

Status 界面主要显示了服务器运行的一些状态。

在 Tomcat Manager 中, 可以对当前运行在服务器上的 Web 站点(Web 应用)进行部署与管理。

在 Tomcat 安装目录的 `conf` 文件夹下的 `server.xml` 中可以设置 HTTP 连接使用的端口, 默认为 8080。

若使用 WSI 安装则安装过程中可以设置。

若使用压缩包安装或是安装完后需要修改, 则需修改 `server.xml`: 查找字符串 `"protocol="HTTP/1.1"` (非注释), 将其前面的端口号 `port` 值进行修改, 即可完成。

## 简单的网站部署

Tomcat 默认的站点根目录位于 `webapps`，将包含 HTML 文件的文件夹部署到此目录下，即可发布成功。其中 `webapps\ROOT` 是站点根节点所对应的目录。按默认的配置，`http://localhost:8080/` 对应 `webapps\ROOT`，`http://localhost:8080/docs` 对应 `webapps\docs`。Tomcat 还有很多更复杂的配置，如路径映射等。

### 练习：

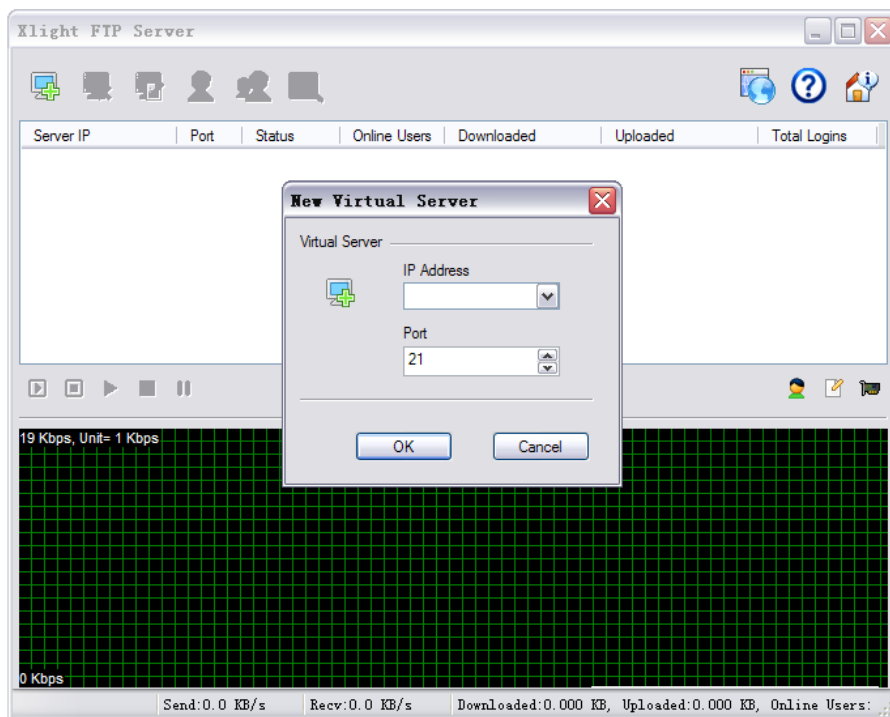
安装 Tomcat，可选用 WSI 安装或压缩包安装。查看 Tomcat Manager 页面。将目录 Tomcat\_Test 部署到服务器上，使访问如下地址时显示 tomcat.html。

`http://localhost:8088/Tomcat_Test/tomcat.html`

## 3 FTP 服务器的配置

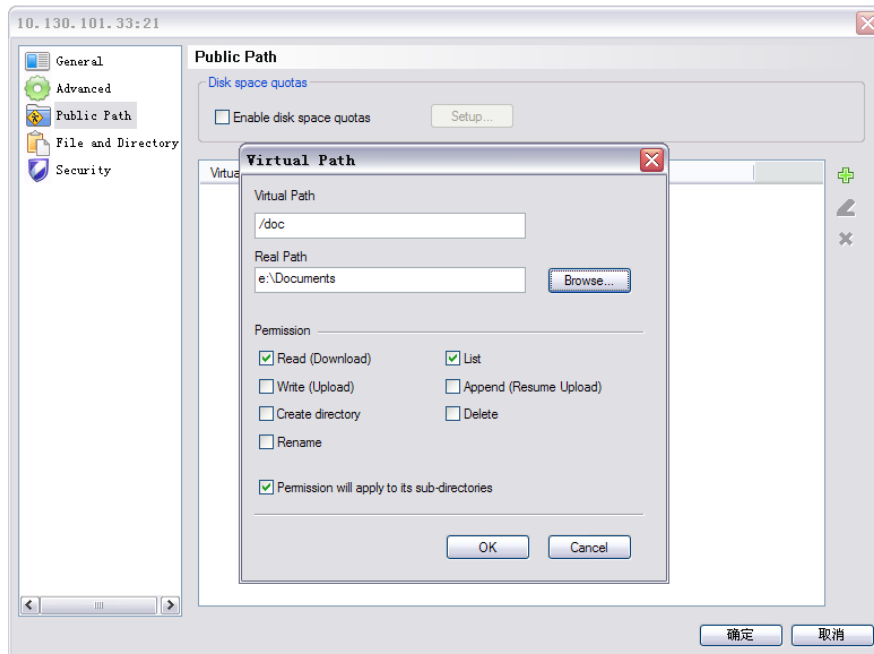
使用 Xlight 作为 FTP 服务器软件，直接双击打开 `xlight.exe`。

点击左上角按钮添加新的服务器配置。输入本机的 IP 地址，端口号保持 21 不变。

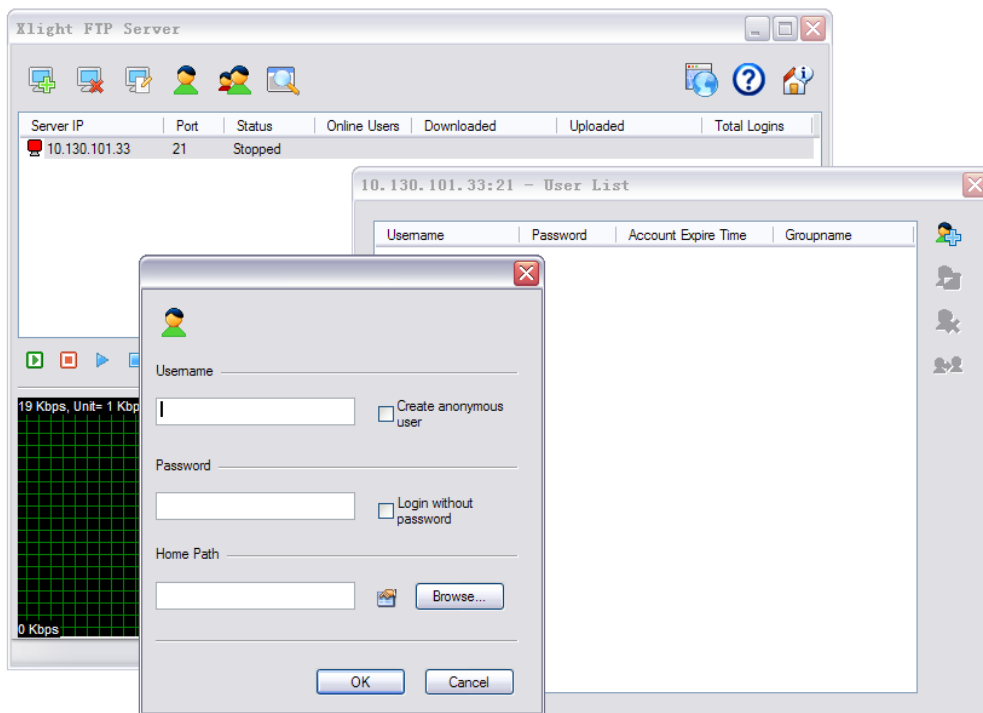


右击列表中刚刚创建的服务器，选择 **Modify Virtual Server Configuration**。从左边选择 **Public Path**，在右边选择需要共享在网络上的目录。如图，若设置 **Virtual Path**(虚拟路径)为 `/doc`，**Real Path**(真实路径)为 `e:\Documents`，则用户通过使用 ftp 协议访问 `[IP 地址]/doc` 时即可看到服务器物理路径 `e:\Documents` 下的文件。路径选择的下方，可选择该路径的权限，如是否可读(下载)、是否可写(上传)、可否建立文件目录等。





此时还需要建立用户账户，供客户端进行登陆。回到 Xlight 主界面，在列表中选中配置过的服务器，点击上方的 **User List** 按钮，在弹出的对话框中再点击右侧的添加按钮。



设置好用户名和密码，FTP 服务器配置就可以初步完成了。回到 Xlight 主界面，右击列表中配置过的服务器，选择 **Start Server**。在浏览器中输入相应地址就可访问服务器的文件目录了。

如上图所配置的 IP 地址，可通过如下地址访问：<ftp://10.130.101.33/>。

练习：

使用 Xlight 配置 FTP 服务器，文件路径配置随意。

# 网络常用 DOS 命令

## 1. ping

用来检查网络是否通畅或者网络连接速度的命令。它所利用的原理是在网络上的机器都有唯一确定的 IP 地址，我们给目标 IP 地址发送一个数据包，对方就会返回一个同样大小的数据包，根据返回的数据包我们可以确定目标主机是否存在，可以判断网络速度。在 DOS 窗口中键入：`ping /?` 回车，可以知道 ping 命令每一个参数的作用。在此，我们只需掌握一些基本的很有用的参数就可以了。

`-t` 表示将不间断向目标 IP 发送数据包，直到我们强迫其停止。试想，如果一方使用 100M 的宽带接入，而目标 IP 是 56K 的调制解调器，那么要不了多久，目标 IP 可能就会因为承受不了这么多的数据而掉线。

`-l` 定义发送数据包的大小，默认为 32 字节，我们利用它可以最大定义到 65500 字节。结合上面介绍的 `-t` 参数一起使用，会使目标 IP 的承受更多的数据量。

`-n` 定义向目标 IP 发送数据包的次数，默认为 3 次。如果网络速度比较慢，3 次对我们来说也浪费了不少时间，如果我们的目的仅仅是判断目标 IP 是否存在，那么就可设为 1 次。

如果 `-t` 参数和 `-n` 参数一起使用，ping 命令就以放在后面的参数为标准，比如“`ping IP -t -n 3`”，虽然使用了 `-t` 参数，但并不是一直 ping 下去，而是只 ping 3 次。另外，ping 命令不一定非得 ping IP，也可以直接 ping 主机域名，这样就可以得到主机的 IP。

在返回结果中，`time = 64ms` 表示从发出数据包到接受到返回数据包所用的时间是 64 毫秒，从这里可以判断网络连接速度。TTL (Time To Live) 是 IP 协议包中的一个值，它告诉网络路由器包在网络中的时间是否太长而应被丢弃。有很多原因使包在一定时间内不能被传递到目的地。例如，不正确的路由表可能导致包的无限循环。一个解决方法就是在一段时间后丢弃这个包，然后给发送者一个报文，由发送者决定是否要重发。TTL 的初值通常是系统缺省值，是包头中的 8 位的域。TTL 的最初设想是确定一个时间范围，超过此时间就把包丢弃。

## 2. ipconfig

使 `ipconfig` 时不带任何参数选项，那么它为每个已经配置了的接口显示 IP 地址、子网掩码和缺省网关值。

`ipconfig -all`

当使用 `all` 选项时，`ipconfig` 能为 DNS 和 WINS 服务器显示它已配置且所要使用的附加信息（如 IP 地址等），并且显示内置于本地网卡中的物理地址（MAC）。如果 IP 地址是从 DHCP 服务器租用的，`ipconfig` 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。

`ipconfig /release` 和 `ipconfig /renew`

这是两个附加选项，只能在向 DHCP 服务器租用其 IP 地址的计算机上起作用。如果我们输入 `ipconfig /release`，那么所有接口的租用 IP 地址便重新交付给 DHCP 服务器（归还 IP 地址）。如果我们输入 `ipconfig /renew`，那么本地计算机便设法与 DHCP 服务器取得联系，并租用一个 IP 地址。请注意，大多数情况下网卡将被重新赋予和以前所赋予的相同的 IP 地址。

### 3. nbtstat

该命令使用 TCP/IP 上的 NetBIOS 显示协议统计和当前 TCP/IP 连接，使用这个命令你可以得到远程主机的 NETBIOS 信息，比如用户名、所属的工作组、网卡的 MAC 地址等。在此我们就有必要了解几个基本的参数。

- a 使用这个参数，只要你知道远程主机的机器名称，就可以得到它的 NETBIOS 信息
- A 这个参数也可以得到远程主机的 NETBIOS 信息，但需要你知道它的 IP。
- n 列出本地机器的 NETBIOS 信息。

当得到了对方的 IP 或者机器名的时候，就可以使用 nbtstat 命令来进一步得到对方的信息了。

### 4. netstat

这是一个用来查看网络状态的命令，操作简便功能强大。

- a 查看本地机器的所有开放端口，可以有效发现和预防木马，可以知道机器所开的服务等信息，这里可以看出本地机器开放有 FTP 服务、Telnet 服务、邮件服务、WEB 服务等。
- s 本选项能够按照各个协议分别显示其统计数据。如果我们的应用程序（如 Web 浏览器）运行速度比较慢，或者不能显示 Web 页之类的的数据，那么我们就可以用本选项来查看一下所显示的信息。我们需要仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。
- e 本选项用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量。这个选项可以用来统计一些基本的网络流量。
- r 本选项可以显示关于路由表的信息，除了显示有效路由外，还显示当前有效的连接。
- n 显示所有已建立的有效连接。

### 5. tracert

跟踪路由信息，使用此命令可以查出数据从本地机器传输到目标主机所经过的所有途径，这对我们了解网络布局 and 结构很有帮助。你可以用它来了解当前机器离某些主要网站的距离以此初步分析当前机器离主干网的距离。用法: tracert IP 或域名，如 tracert yahoo.com

### 6. net

这个命令是网络命令中比较重要的一个，因为它的功能十分强大。首先让我们来看一看它都有那些子命令，键入 net /?回车。在这里，我们重点掌握几个入侵常用的子命令。

net view 使用此命令查看远程主机的所以共享资源。

net start 使用它来启动远程主机上的服务。当你和远程主机建立连接后，如果发现它的什么服务没有启动，就使用这个命令来启动吧。

net stop 用它来关闭远程主机上的服务。

net user 查看和帐户有关的情况，包括新建帐户、删除帐户、查看特定帐户、激活帐户、帐户禁用等。这对我们入侵是很有利的，最重要的，它为我们克隆帐户提供了前提。键入不带参数的 net user，可以查看所有用户，包括已经禁用的。

net time 查看目标地址系统时间。