

TCP/IP协议和网络安全

传输控制协议/因特网协议（TCP/IP）组是由美国国防部（DoD）所创建的，主要用来确保数据的完整性及在毁灭性战争中维持通信。如果能进行正确的设计和应用，TCP/IP 网络将是可靠的并富有弹性的网络。

本章将详细阐述 TCP/IP 的层次结构，以及每层包含的协议，讲解了传输层两个协议 TCP 和 UDP 协议的应用场景，应用层协议和传输层协议的关系，应用层协议和服务之间的关系。并且演示了在 Windows Server 2003 上安装配置 FTP 服务、Web 服务、POP3 服务、SMTP 服务和 DNS 服务，启用服务器的远程桌面，并且配置客户端连接这些服务器。

TCP/IP 是 Transmission Control Protocol/Internet Protocol 的简写，中文译名为传输控制协议/因特网互联协议，又叫网络通信协议，这个协议是 Internet 最基本的协议、Internet 国际互联网络的基础，简单地说，就是由网络层的 IP 协议和传输层的 TCP 协议组成的。

配置 Windows 防火墙保护 Windows XP 安全和使用 TCP/IP 筛选配置服务器安全，防止主动入侵计算机。配置 IPSec 严格控制进出服务器的数据流量，避免木马程序造成威胁。

同时展示使用捕包工具排除网络故障。

本章主要内容：

- TCP/IP 协议和 DoD 模型
- 传输层协议
- 应用层协议

- 应用层协议和服务的关系
- 配置服务器网络安全
- 使用捕包工具排除网络故障

2.1 OSI 和 DoD 模型

DoD 模型基本上是 OSI 模型的一个浓缩版本，它只有 4 个层次，而不是 7 个，它们是：

- 应用层
- 传输层
- 网络层
- 网络接口层

其中，如果在功能上和 OSI 参考模型互相对应的话，如图 2-1 所示。

- DoD 模型的 Process/Application 层对应 OSI 参考模型的最高 3 层。
- DoD 模型的 Host-to-Host 层对应 OSI 参考模型的 Transport 层。
- DoD 模型的 Internet 层对应 OSI 参考模型的 Network 层。
- DoD 模型的 Network Access 层对应 OSI 参考模型的最低 2 层。

OSI	DoD	TCP/IP 协议集
应用层	应用层	Telnet, FTP, SMTP, DNS, HTTP 以及其他应用协议
表示层		
会话层		
传输层	传输层	TCP, UDP
网络层	网络层	IP, ARP, RARP, ICMP
数据链路层		
物理层	网络接口层	各种通信网络接口（以太网等） (物理网络)

▲图 2-1 OSI 与 DoD 的比较

2.2 传输层协议

通常情况一个数据包最大 1500 个字节，在网络上的通信有以下两种情况。

一种情况是，一个数据包就能完成通信用务，例如，我们上网时输入网址 www.91xueit.com，你的计算机需向要域名解析服务器（DNS）发送一个数据包查询该域名对应的 IP 地址，DNS 服务器向你的计算机返回一个数据包告你的计算机该网址对应的 IP 地址，这类通信一个数据包就能完成。再比如 QQ 聊天，你给好友发送一个信息“你好！新年快乐”，这几个字一个数据包就能发送给你的好友。

另一种情况是，一个数据包不能完成的通信用务，需要把信息分成多个数据包传输，比如，我们打开 IE 浏览器，访问网站，网页中有很多文字和图片，一个数据包不能发送到客户端，需要把数据分成段，编上号，然后分段传递到客户端。针对以上两种情况，在 TCP/IP 协议栈，传输层有两个协议——TCP 和 UDP。

TCP (Transmission Control Protocol, 传输控制协议): 一个数据包不能完成通信任务的通信在传输层大多使用 TCP 协议。传输前数据分段，编号，客户端和服务器建立会话，可靠传输----传输过程数据包丢失，要求服务器重传。

UDP (User Data Protocol, 用户数据报协议): 一个数据包就能完成的任务在传输层大多使用 UDP 协议，不可靠传输，服务器和客户端不建立会话，比 TCP 建立会话节省服务器资源，数据不分段，不编号。也有一些多播通信使用 UDP 协议。

理解了 TCP 和 UDP 的应用场景之后，你可以针对某种应用推断出其传输层使用的是 TCP 协议还是 UDP 协议，比如，发送电子邮件，一个数据包是不能完成电子邮件传输的，发送电子邮件的 SMTP 协议在传输层是 TCP；使用 FTP 上传文件和下载文件，一个数据包也不能完成文件的上传和下载，因此你可以推断 FTP 在传输层使用的也是 TCP 协议；访问 Web 站点，一个数据包也不能将 Web 页面的图片和文字传送到客户端，你可以推断其在网络层使用的是 TCP 协议。

**提
示**

大家可以推断一下，使用 QQ 聊天时，传输层使用的是什么协议；使用 QQ 给好友传文件时，传输层使用的是什么协议。由于 QQ 聊天，是交互的，通常不需要连续传递大量数据，和好友聊天的信息，使用一个数据包通常就能传输到客户端，因此 QQ 聊天在传输层使用的是 UDP 协议；QQ 传文件，需要传递的文件通常需要将文件分成多个数据包进行连续传输，在传输过程中不允许出现丢包，因此在传输层使用 TCP 协议。可见一个程序中不同的应用在传输层可能选择不同的协议。

2.2.1 传输控制协议

传输控制协议（TCP）通常从应用程序中得到大段的信息数据，然后将其分割成若干个数据段。TCP 会为这些数据段编号并排序，这样，在目的方的 TCP 协议栈才可以将这些数据段再重新组成原来应用数据的结构。由于 TCP 采用的是虚电路连接方式，这些数据段在被发送出去后，发送方的 TCP 会等待接收方 TCP 给出一个确认性应答，那些没有收到确认应答的数据段将被重新发送。

当发送方主机开始沿分层模型向下发送数据段时，发送方的 TCP 协议会通知目的方的 TCP 协议去建立一个连接，也就是所谓的虚电路。这种通信方式被称为是面向连接的。在这个初始化的握手协商期间，双方的 TCP 层需要对接收方在返回确认应答之前，可以连续发送多少数量的信息达成一致。随着协商过程的深入，用于可靠传输的信道就被建立起来。

TCP 是一个全双工的、面向连接的、可靠的并且是精确控制的协议，但是要建立所有这些条件和环境并附加差错控制，并不是一件简单的事情。所以，毫无疑问，TCP 是复杂的，并在网络开销方面是昂贵的。然而，由于如今的网络传输同以往的网络相比，已经可以提供更高的可靠性，因此，TCP 所附加的可靠性就显得没那么必要了。

2.2.2 用户数据报协议

用户数据报协议（UDP）适用于一个数据包就能完成的数据通信任务。比如 QQ 聊天发送的数据，域名解析（DNS）一个数据包就能完成。这类通信不需要在客户端和服务器端建

立会话，节省服务器资源。如果网络不稳定，发送数据包失败，客户端会重试。

UDP 协议也广泛应用到多播和广播，比如多媒体教室程序将屏幕广播给学生的计算机，教室中的计算机接收教师计算机电脑屏幕。这类通信虽然一个数据包不能完成数据包通信，但这类通信不需要客户端和服务端连接会话。

UDP 无须排序所要发送的数据段，而且不关心这些数据段到达目的方时的顺序。在发送完数据段后，就忘记它们。它不去进行后续工作，如去核对它们，或者产生一个安全抵达的确认，它完全放弃了可以保障传送可靠性的操作。正是因为这样，UDP 被称为是一个不可靠的协议，但这并不意味着 UDP 就是无效率的，它只表明，UDP 是一个不处理传送可靠性的协议。

更进一步讲，UDP 不去创建虚电路，并且在数据传送前也不联系对方。正因为这一点，它又被称为是无连接的协议。由于 UDP 假定应用程序能保证数据传送的可靠性，因而它不需要对此做任何的工作。这给应用程序开发者在使用因特网协议栈时多提供了一个选择：使用传输可靠的 TCP，还是使用传输更快的 UDP。

因此，如果你正在使用语音 IP (VoIP)，那么你就不会再使用 UDP，因为如果数据段未按顺序到达（在 IP 网络中这是很常见的），那么这些数据段将只会以它们被接收到的顺序传递给下一个 OSI (DoD) 层面。而与之不同的是，TCP 则会以正确的顺序来重组这些数据段，以保证秩序上的正确，UDP 却做不到这一点。

2.3 应用层协议

传输层协议添加端口就可以标识应用层协议。应用层协议代表着服务器上的服务，服务器上的服务如果对客户端提供服务，必须在 TCP 或 UDP 端口侦听客户端的请求。

2.3.1 应用层协议和传输层协议的关系

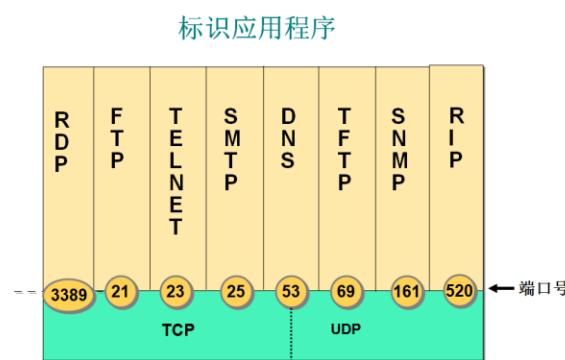
传输层的协议 TCP 或 UDP 加上端口就可以标识一个应用层协议，TCP/IP 协议中的端口范围是从 0~65535。

1. 端口的作用

端口有什么用呢？我们知道，一台拥有 IP 地址的主机可以提供许多服务，比如 Web 服务、FTP 服务、SMTP 服务等，这些服务完全可以通过 1 个 IP 地址来实现。

那么，主机是怎样区分不同的网络服务呢？显然不能只靠 IP 地址，因为 IP 地址与网络服务的关系是一对多的关系。实际上是通过“IP 地址+端口号”来区分不同的服务的。

服务器一般都是通过知名端口号来识别的，如图 2-2 所示。例如，对



▲图 2-2 应用层协议和传输层协议的关系

于每个 TCP/IP 实现来说，FTP 服务器的 TCP 端口号都是 21，每个 Telnet 服务器的 TCP 端口号都是 23，每个 TFTP（简单文件传送协议）服务器的 UDP 端口号都是 69。任何 TCP/IP 实现所提供的服务都用知名的 1~1023 之间的端口号。这些知名端口号由 Internet 号分配机构（Internet Assigned Numbers Authority, IANA）来管理。

2. 应用层协议和传输层协议的关系

下面是一些常见的应用层协议和传输层协议之间的关系。

- HTTP 默认使用 TCP 的 80 端口标识
- FTP 默认使用 TCP 的 21 端口标识
- SMTP 默认使用 TCP 的 25 端口标识
- POP3 默认使用 TCP 的 110 端口
- HTTPS 默认使用 TCP 的 443 端口
- DNS 使用 UDP 的 53 端口
- 远程桌面协议（RDP）默认使用 TCP 的 3389 端口
- Telnet 使用 TCP 的 23 端口
- Windows 访问共享资源使用 TCP 的 445 端口

3. 知名端口

知名端口即众所周知的端口号，范围从 0~1023，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（文件传输协议）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。

网络服务是可以使用其他端口号的，如果不是默认的端口号则应该在地址栏上指定端口号，方法是在地址后面加上冒号“：“（半角），再加上端口号。比如使用“8080”作为 WWW 服务的端口，则需要在地址栏里输入“<http://www.cce.com.cn:8080>”。

但是有些系统协议使用固定的端口号，它是不能被改变的，比如 139 端口专门用于 NetBIOS 与 TCP/IP 之间的通信，不能手动改变。

客户端在访问服务器时，源端口一般都是动态分配的 1024 以上的端口。

2.3.2 应用层协议和服务的关系

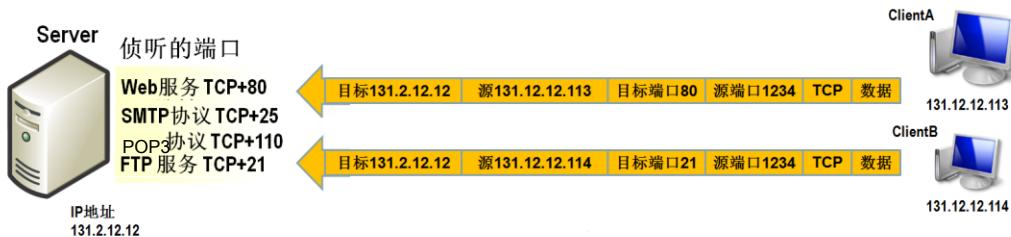
应用层协议代表的是服务器上的服务。

不管是 Windows XP 还是 Windows 7，无论是 Windows Server 2003 还是 Windows Server 2008 都有内置的一些服务。这些服务有的是为本地计算机提供服务的，比如停止了 Network Connections 服务，你就不能打开网络连接修改 IP 地址；有的是为网络中的其他计算机提供服务，这类服务使用 TCP 或 UDP 的特定端口侦听客户端请求。

举例说明，如图 2-3 所示，Server 服务器安装了 Web 服务、FTP 服务、SMTP 服务和 POP3 服务。Web 服务在 TCP 的 80 端口侦听客户端请求，SMTP 服务在 TCP 的 25 端口侦听客户端的请求，POP3 在 TCP 的 110 端口侦听客户端请求，FTP 在 TCP 的 21 端口侦听客户端请求。

Client A 访问 Server 的 Web 服务，数据包的目标端口为 80，Client B 访问 Server 的 FTP

服务，数据包的目标端口为 21。这样，服务器 Server 就可以根据数据包的目标端口来区分客户端要请求的服务。



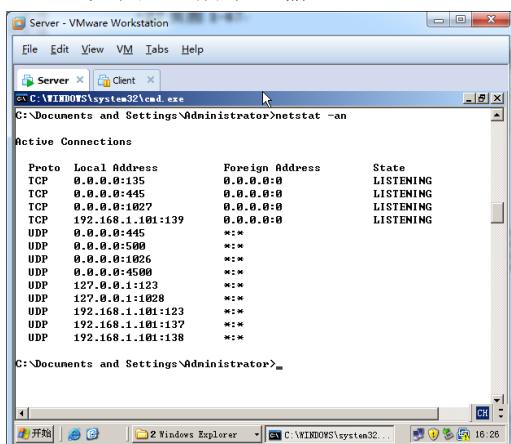
▲图 2-3 服务与端口

总结 数据包中的目标 IP 地址用来定位服务器，而数据包中的目标端口用来定位服务器上的服务。

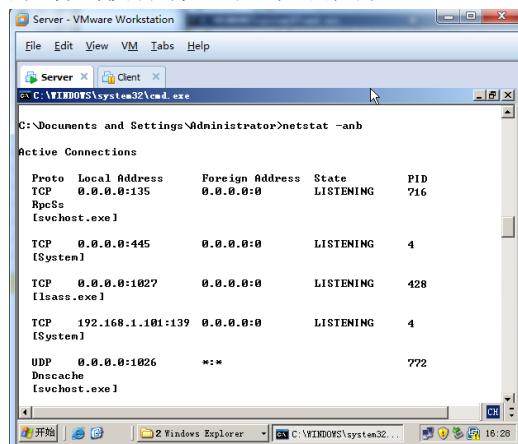
2.3.3 示例 1：查看远程桌面侦听的端口

本示例将会在 Server 上启用远程桌面，来查看远程桌面的侦听端口。

- (1) 如图 2-4 所示，在 Server 的计算机上运行 netstat -an 可以看到在 TCP 和 UDP 侦听的端口。其中 TCP 的 445 端口是为其他计算机访问其共享资源侦听的端口。注意观察在 TCP 协议侦听的没有 3389 端口。
- (2) 如图 2-5 所示，输入 netstat -anb 还可以看到侦听端口的进程或程序。

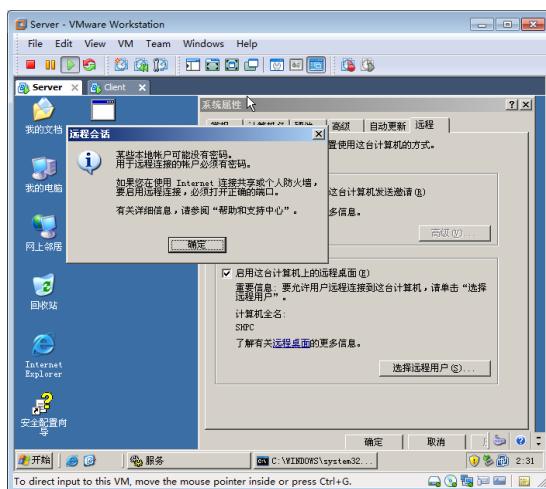


▲图 2-4 查看侦听端口

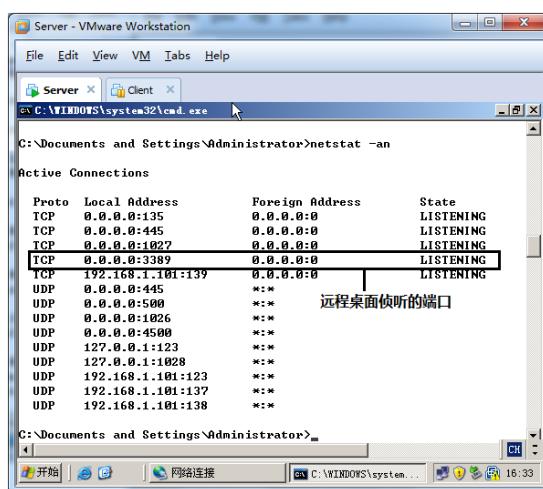


▲图 2-5 查看侦听端口的进程

- (3) 如图 2-6 所示，右击桌面上的“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令。
- (4) 如图 2-6 所示，在出现的“系统属性”对话框的“远程”选项卡中，选中“启用这台计算机上的远程桌面”复选框，在出现的提示对话框中，提示空密码不允许远程登录，单击“确定”按钮。如图 2-7 所示，在 Server 上查看侦听的端口，可以看到在 TCP 协议侦听的有 3389 端口。



▲图 2-6 启用远程桌面

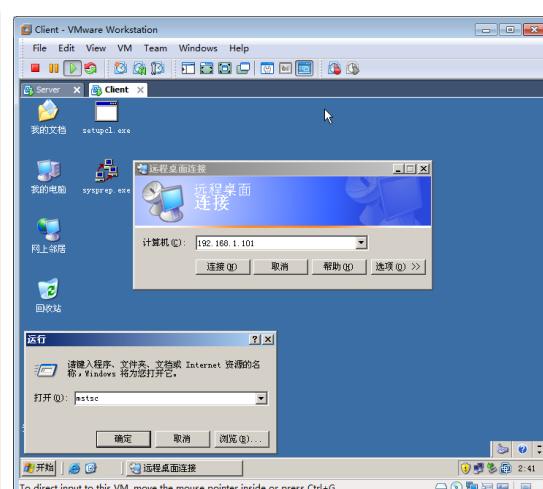


▲图 2-7 查看侦听的端口

- (5) 如图 2-8 所示, 输入 net user administrator a1! 重设 administrator 的密码为 a1!。
- (6) 如图 2-8 所示, 输入 ipconfig 查看 IP 地址。
- (7) 如图 2-9 所示, 在 Client 计算机上, 选择“开始”→“运行”命令, 在弹出的对话框中输入“mstsc”, 单击“确定”按钮。
- (8) 如图 2-9 所示, 在打开的远程桌面客户端对话框中, 输入 Server 的 IP 地址, 单击“连接”按钮。

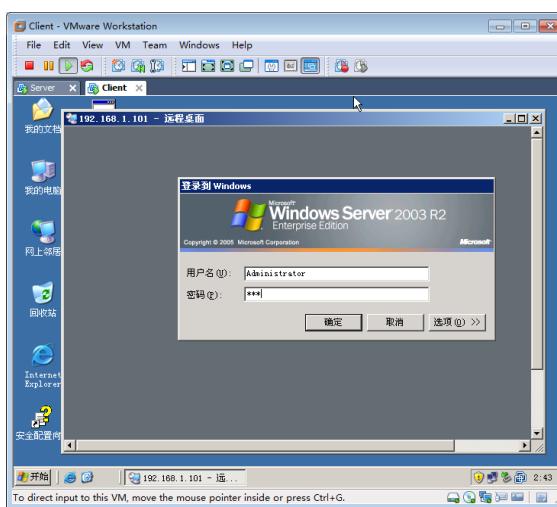


▲图 2-8 重设密码和查看 IP 地址

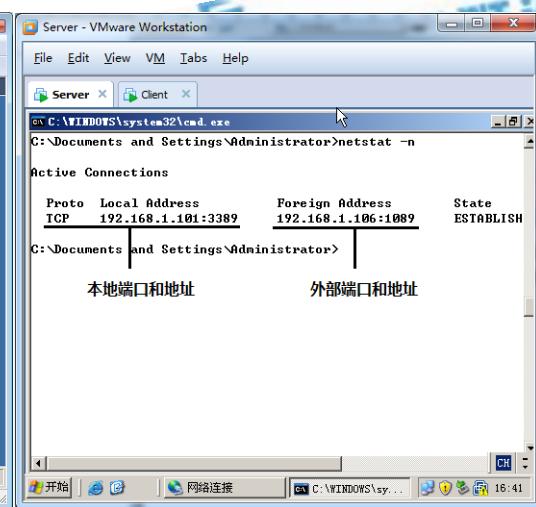


▲图 2-9 使用远程桌面连接

- (9) 如图 2-10 所示, 在“登录到 Windows”对话框中输入账号和密码, 单击“确定”按钮。
- (10) 如图 2-11 所示, 在 Server 上查看远程桌面建立的会话。



▲图 2-10 输入账号和密码



▲图 2-11 查看建立的会话

2.3.4 示例 2：端口冲突造成服务启动失败

服务器上的服务侦听的端口不能冲突。否则将会造成服务启动失败。

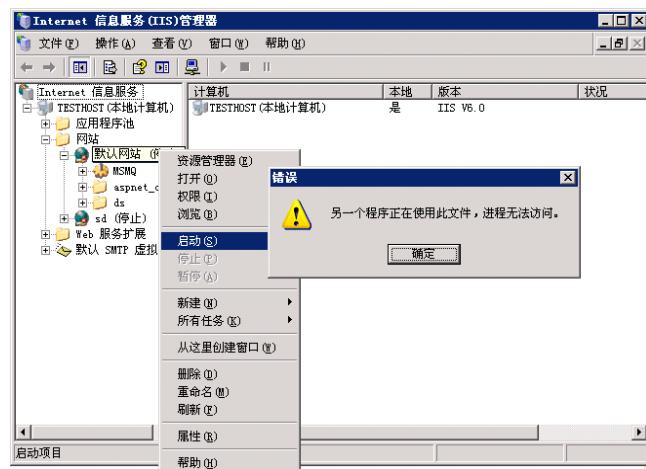
某家公司的网站不能访问了，操作系统是 Windows 2003。打电话求助微软企业护航技术支持中心，技术支持工程师通过远程桌面登录到服务器，选择“开始”→“程序”→“管理工具”→“Internet 信息服务管理器”命令，发现该 Web 站点停止，如图 2-12 所示。右击“默认网站”节点，在弹出的快捷菜单中选择“启动”命令，启动服务出现错误提示：另一个程序正在使用此文件，进程无法访问。根据经验判断，这是服务端口冲突造成的服务启动失败。

这台服务器上就一个 Web 站

点，肯定是其他程序占用了该 Web 站点使用的 80 端口，如何确认哪个程序占用了该端口呢？

操作步骤：

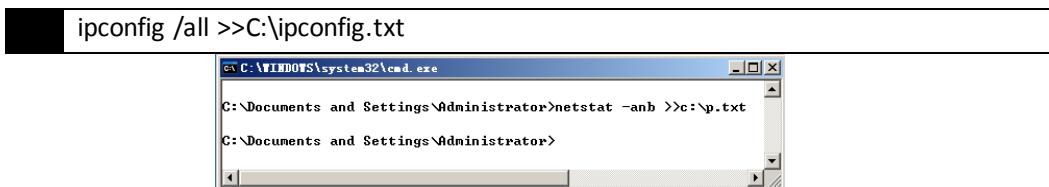
- (1) 如图 2-13 所示，在命令提示符下输入 `netstat -aonb >>C:\p.txt`，这样，就可将输出结果保存在 C:\p.txt。
- (2) 打开 C 盘根目录下的 p.txt。



▲图 2-12 端口被占用

注意

所有用命令提示符显示的结果都可以使用 >> 路径\文件名.txt 保存到文件。如



▲图 2-13 将输出保存到记事本

(3) 如图 2-14 所示, netstat -aonb 命令能够查看侦听的端口、侦听端口的进程号和应用程序的名字。发现是 Web 迅雷占用了 80 端口, 造成服务器 Web 服务启动失败。

Active Connections				
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:25 [inetinfo.exe]	0.0.0.0:0	LISTENING	1592
TCP	0.0.0.0:53 [dns.exe]	0.0.0.0:0	LISTENING	1548
TCP	0.0.0.0:80 [WebThunder.exe]	0.0.0.0:0	LISTENING	4244
TCP	0.0.0.0:88 [lsass.exe]	0.0.0.0:0	LISTENING	472
TCP	0.0.0.0:100 [WebThunder.exe]	0.0.0.0:0	LISTENING	392

▲图 2-14 查看占用 80 端口的程序

(4) 解决办法就是卸载 Web 迅雷。

原来该单位的系统管理员使用服务器上安装的 Web 迅雷下载了软件, 重启服务器后, Web 迅雷比 Web 服务先启动, 占用了 TCP 的 80 端口, 造成 Web 服务启动失败。

2. 4 应用层协议和服务

下面就以 Web 服务、FTP 服务、SMTP 服务、POP3 服务和 DNS 服务为例, 帮助读者理解传输层协议和应用层协议的关系, 并深刻理解服务和应用层协议之间的关系。

现在在 Windows Server 2003 上安装 Web 服务、FTP 服务、SMTP 服务、POP3 服务和 DNS 服务并配置这些服务, 查看这些服务侦听的端口, 并且配置客户端访问这些服务。配置服务器和客户端不使用默认端口进行通信。

通过更改服务侦听的端口, 可以迷惑入侵者, 入侵者通过端口扫描工具, 查看服务器侦听的端口, 就可以判断服务器运行的服务。如果你的服务器只对内网的用户提供服务, 或者不对 Internet 上的用户提供服务, 你都可以更改服务不使用默认端口, 这样可以迷惑攻击者, 增强服务器的安全。

2.4.1 在 Windows Server 2003 上安装服务

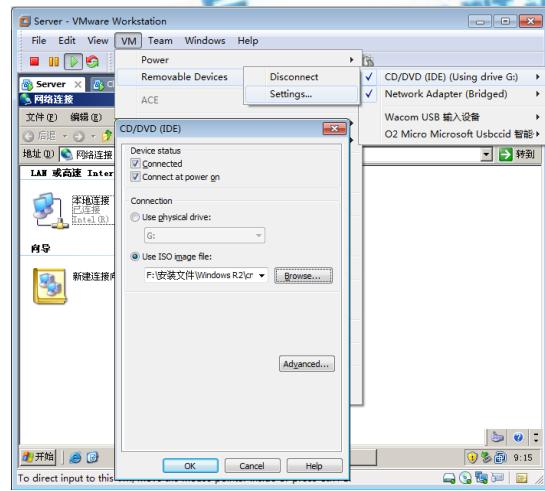
读者朋友们对在计算机上安装程序一定非常熟悉。现在介绍一下在 Server 计算机上安装 Web 服务、FTP 服务、SMTP 服务、POP3 服务和 DNS 服务。

(1) 如图 2-15 所示, 在 Server 上更改 DNS 指向自己的 IP 地址。

(2) 如图 2-16 所示, 选择 VM→Removable Devices→CD/DVD (IDE) →Settings 菜单命令。

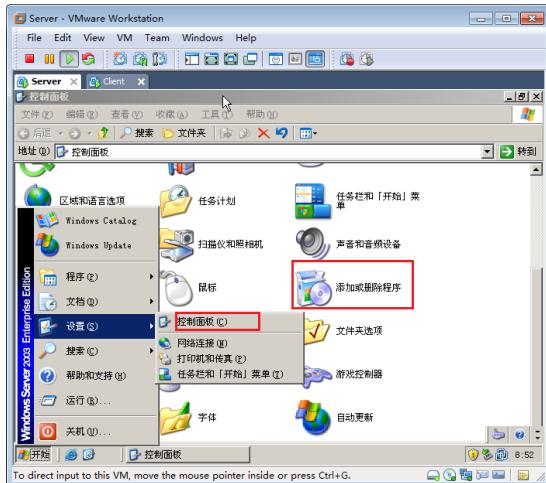


▲图 2-15 配置 IP 地址



▲图 2-16 选择 Windows 安装盘

- (3) 在弹出的 CD/DVD 对话框中, 选中 Use ISO image file 单选按钮, 单击 Browse 按钮, 浏览到 Windows Server 2003 的安装盘, 单击 OK 按钮。
- (4) 如图 2-17 所示, 选择“开始”→“设置”→“控制面板”命令, 在弹出的“控制面板”窗口中, 单击“添加或删除程序”图标。
- (5) 如图 2-18 所示, 在打开的“添加或删除程序”窗口中, 单击“添加/删除 Windows 组件”图标。

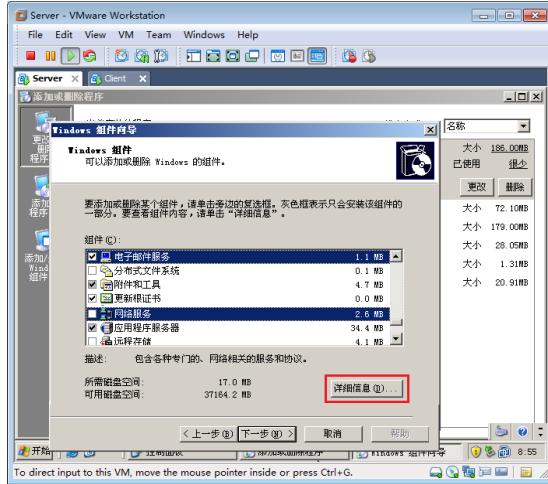


▲图 2-17 单击“添加或删除程序”图标

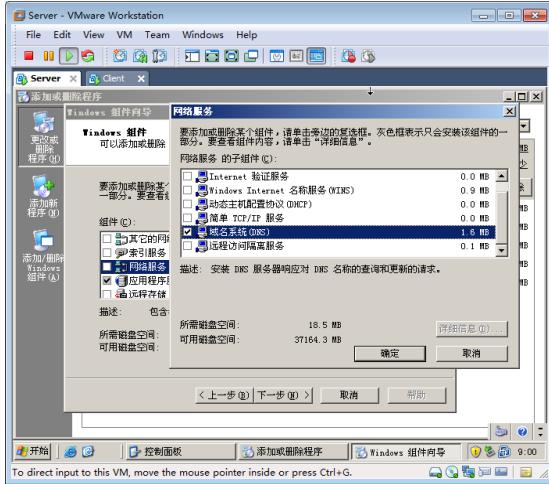


▲图 2-18 添加或删除 Windows 组件

- (6) 如图 2-19 所示, 在弹出的“Windows 组件向导”对话框中, 选中“电子邮件服务”复选框, 以及“网络服务”复选框, 单击“详细信息”按钮。
- (7) 如图 2-20 所示, 在弹出的“网络服务”对话框中, 选中“域名系统 (DNS)”复选框, 单击“确定”按钮。

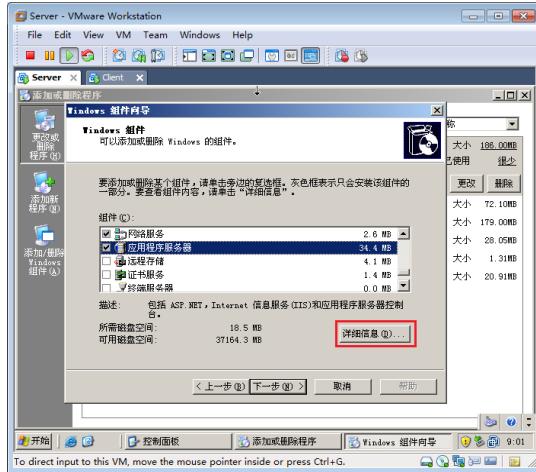


▲图 2-19 选择“电子邮件服务”复选框

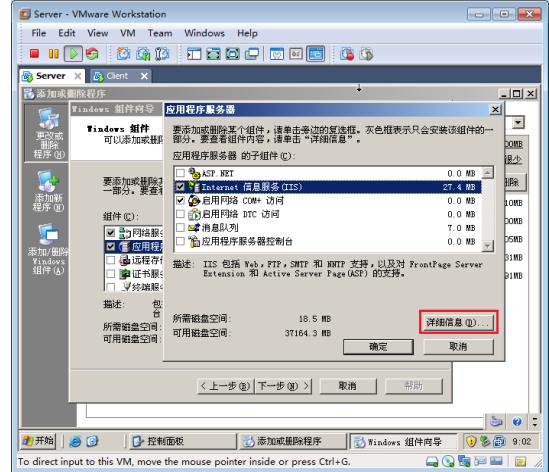


▲图 2-20 选择 DNS 服务

- (8) 如图 2-21 所示, 在“Windows 组件向导”对话框中, 选中“应用程序服务器”复选框, 单击“详细信息”按钮。
- (9) 如图 2-22 所示, 在弹出的“应用程序服务器”对话框中, 选中“Internet 信息服务 (IIS)”复选框, 单击“详细信息”复选框。



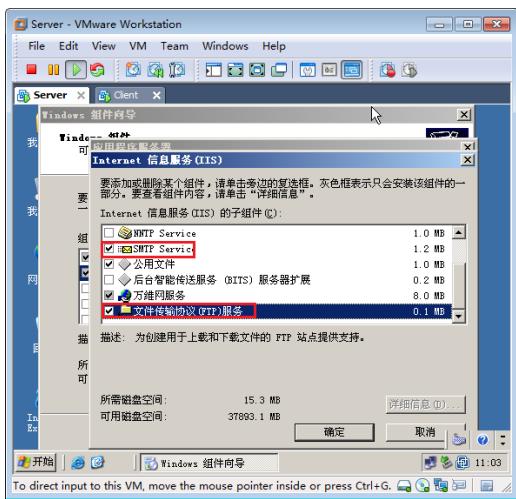
▲图 2-21 选择应用程序服务器



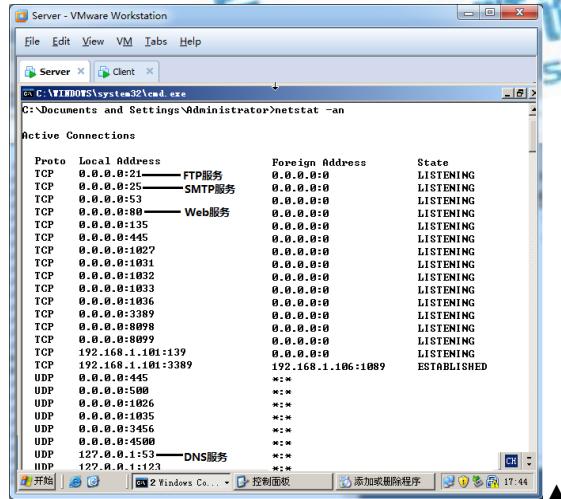
▲图 2-22 选择 IIS 服务

- (10) 如图 2-23 所示, 在弹出的“Internet 信息服务 (IIS)”对话框中, 选中 SMTP Service 复选框和“文件传输协议 (FTP) 服务”复选框, 单击“确定”按钮。
- (11) 在“Windows 组件向导”对话框中, 单击“下一步”按钮, 完成服务安装。
- (12) 如图 2-24 所示, 安装完成后, 在命令提示符下, 输入 netstat -an 命令可以查看安装服务侦听的端口。可以发现没有进程在 TCP 的 110 端口侦听。这是为什么呢?

TCP/IP 协议



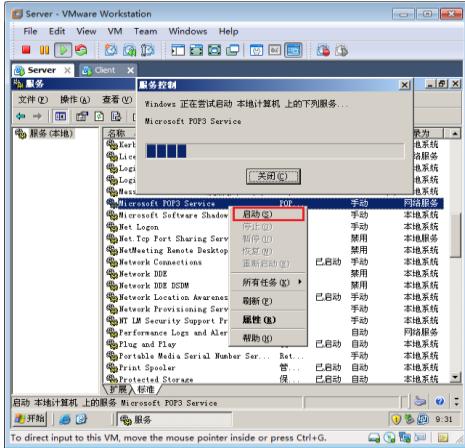
2-23 安装 FTP 和 SMTP 服务



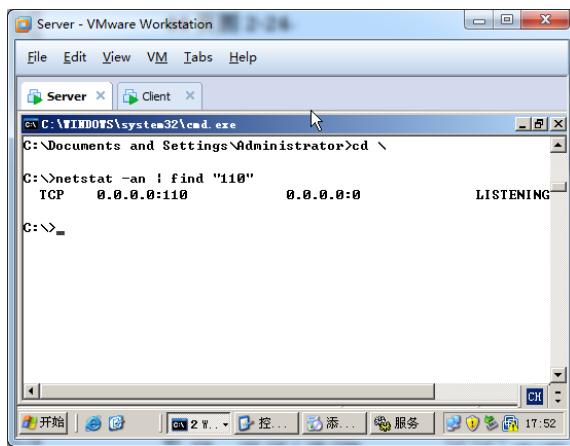
▲图 2-24 查看侦听的端口

- (13) 选择“开始”→“程序”→“管理工具”→“服务”命令，打开服务管理器。
 - (14) 如图 2-25 所示，可以看到 POP3 服务的状态为“未启动”。右击该服务，在弹出的快捷菜单中，选择“启动”命令。
 - (15) 如图 2-26 所示，查看 TCP 的 110 端口是否侦听。在命令提示符下输入 netstat -an | find “110” 可以筛选查看有 110 的行。

由此可知计算机在哪些端口侦听，是由运行的服务决定的。如果你的计算机只安装了某个服务，但是没有运行，该服务的端口照样不侦听，客户端无法访问。



▲图 2-25 启动服务



▲图 2-26 查看侦听的端口

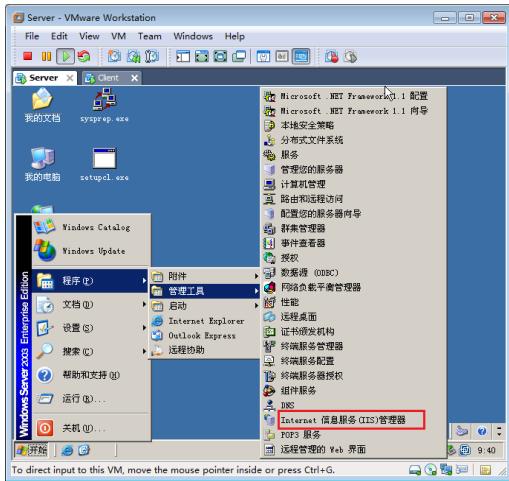
2.4.2 配置 FTP 服务器

FTP 是 File Transfer Protocol（文件传输协议）的英文简称，而中文简称为“文传协议”。用于 Internet 上控制文件的双向传输。同时，它也是一个应用程序（Application），用户可以通过它把自己的 PC 与世界各地所有运行 FTP 协议的服务器相连，访问服务器上的大量程序。

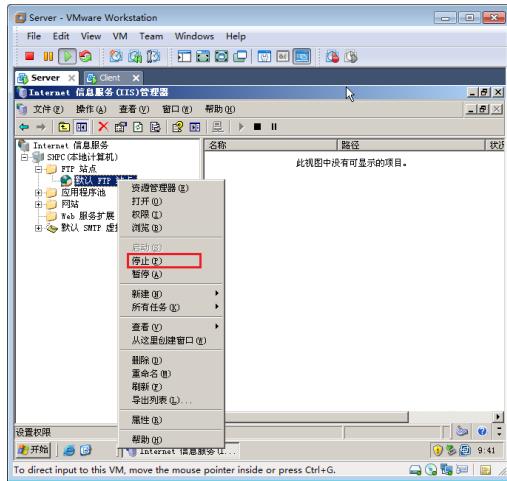
和信息。FTP 的主要作用，就是让用户连接上一个远程计算机（这些计算机上运行着 FTP 服务器程序）查看远程计算机上有哪些文件，然后把文件从远程计算机上复制到本地计算机，或把本地计算机的文件传送到远程计算机去。

以下步骤将会在 Server 上创建一个允许匿名访问的 FTP 站点，允许上传和下载。

- (1) 如图 2-27 所示，选择“开始”→“程序”→“管理工具”→“Internet 信息服务 (IIS) 管理器”命令。
- (2) 如图 2-28 所示，在打开的“Internet 信息服务 (IIS) 管理器”窗口中，右击“默认 FTP 站点”节点，在弹出的快捷菜单中选择“停止”命令。

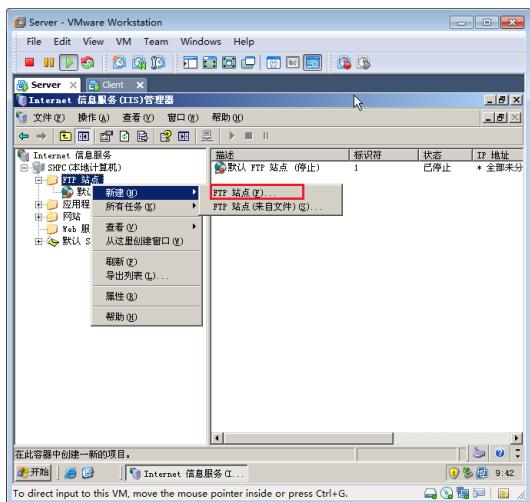


▲图 2-27 打开 IIS 管理器

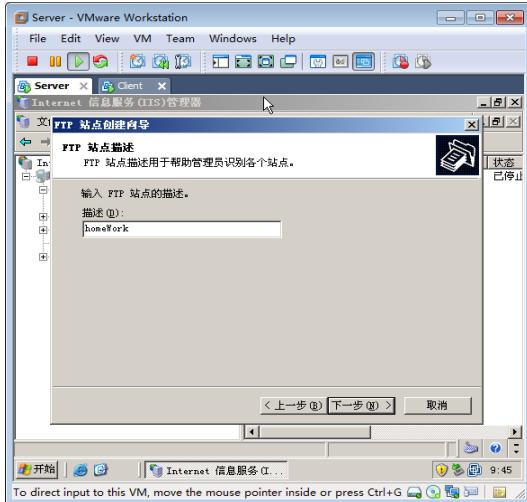


▲图 2-28 停止默认站点

- (3) 如图 2-29 所示，右击“FTP 站点”节点，在弹出的快捷菜单中选择“新建”→“FTP 站点”命令。
- (4) 在弹出的欢迎使用“FTP 站点创建向导”设置界面中，单击“下一步”按钮。
- (5) 如图 2-30 所示，在弹出的“FTP 站点描述”设置界面中，输入描述信息，单击“下一步”按钮。



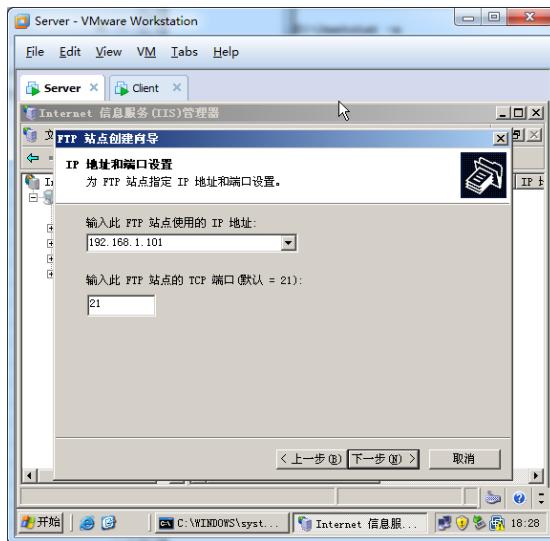
▲图 2-29 新建 FTP 站点



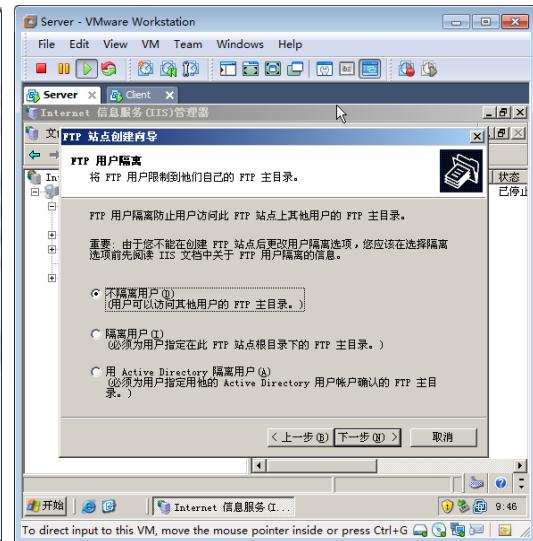
▲图 2-30 输入描述信息

(6) 如图 2-31 所示，在弹出的“IP 地址和端口设置”设置界面中，选择 IP 地址和默认端口 21，单击“下一步”按钮。

(7) 如图 2-32 所示，在弹出的“FTP 用户隔离”设置界面中，选中“不隔离用户”单选按钮，单击“下一步”按钮。



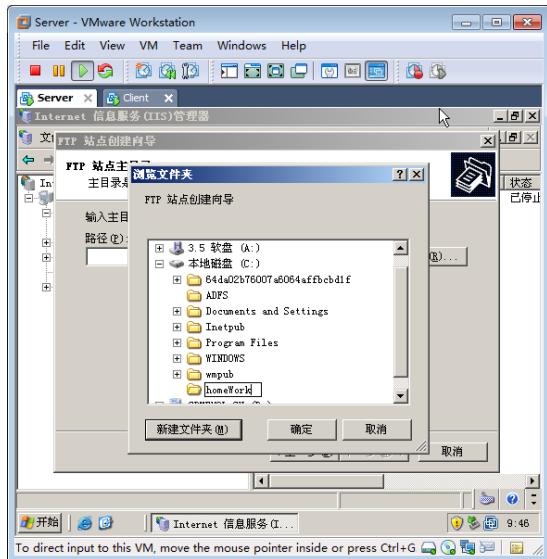
▲图 2-31 选择 IP 地址和端口



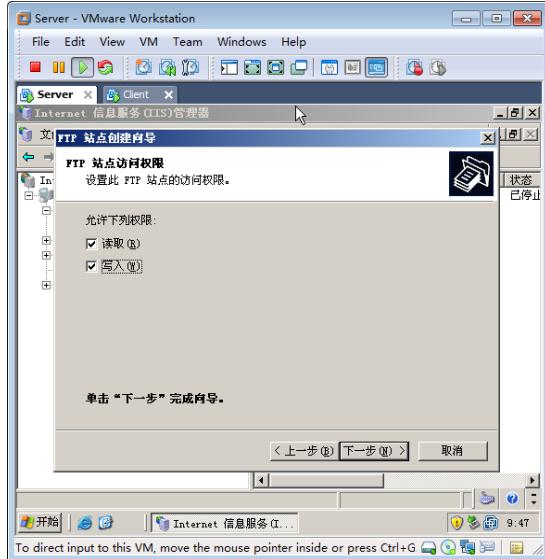
▲图 2-32 不隔离用户

(8) 如图 2-33 所示，在弹出的“FTP 站点主目录”设置界面中，单击“浏览”按钮，在弹出的“浏览文件夹”对话框中，单击“新建文件夹”按钮，在 C 盘根目录下新建文件夹“homeWork”，单击“确定”按钮。单击“下一步”按钮。

(9) 如图 2-34 所示，在弹出的“FTP 访问权限”设置界面中，选中“读取”复选框和“写入”复选框，单击“下一步”按钮。



▲图 2-33 选择 FTP 路径



▲图 2-34 选择 FTP 站点权限

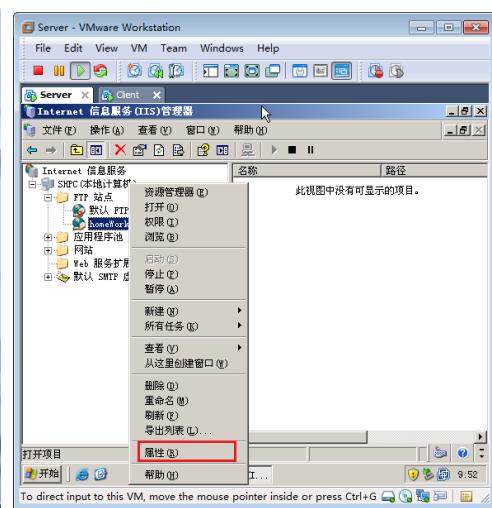
(10) 在弹出的“已成功完成 FTP 站点创建向导”设置界面中，单击“完成”按钮。

(11) 如图 2-35 所示, 在 Client 计算机上, 双击桌面上的“我的电脑”图标, 打开 Windows 资源管理器, 在“地址”栏中输入 `ftp://10.7.10.123` 访问刚才创建的 FTP 站点, 并将桌面上的记事本文件拖曳到 FTP 站点。说明客户端能匿名访问 FTP 站点且能够上传文件。

(12) 如图 2-36 所示, 在 Server 计算机上, 右击刚才创建的 `homeWork` FTP 站点, 弹出的快捷菜单中选择“属性”命令。



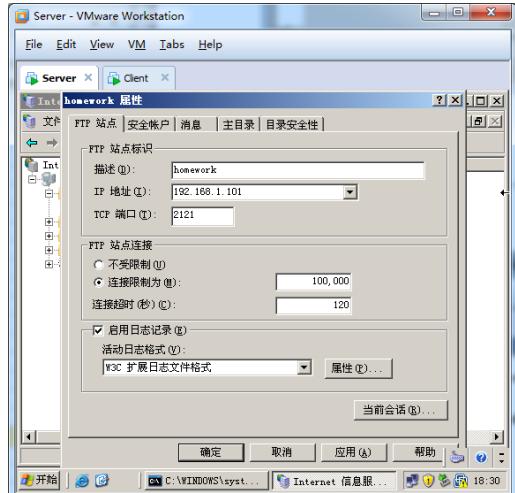
▲ 图 2-35 向 FTP 上传文件



▲ 图 2-36 FTP 属性

(13) 如图 2-37 所示, 在弹出的“`homeWork` 属性”对话框的“FTP 站点”选项卡中, 将 TCP 的端口更改为 2121, 然后单击“确定”按钮。

(14) 如图 2-38 所示, 在命令提示符下输入 `netstat -an | find "2121"`, 能够看到 FTP 倾听的端口变为 2121。



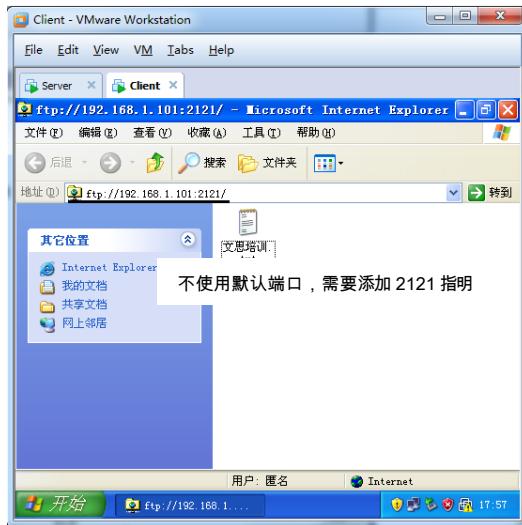
▲ 图 2-37 更改默认端口

```
C:\Documents and Settings\Administrator>cd \
C:\>netstat -an | find "2121"
TCP    0.0.0.0:2121        0.0.0.0:0      LISTENING
C:>
```

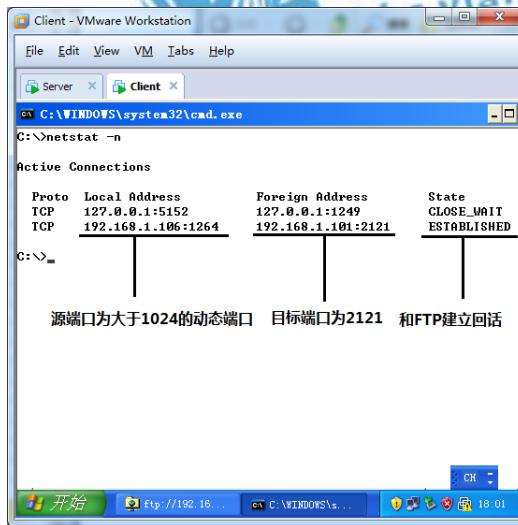
▲ 图 2-38 查看侦听的端口

(15) 如图 2-39 所示, 在 Client 计算机上访问 FTP 站点应在 IP 地址后面添加“2121”来表明不是使用 FTP 默认端口访问 FTP 服务。

(16) 如图 2-40 所示，在命令提示符下输入 netstat-n，可以看到使用 2121 端口和 FTP 建立的会话，注意观察源端口为大于 1024 的动态端口。



▲图 2-39 使用指定端口访问 FTP



▲图 2-40 建立的会话

2.4.3 配置 Web 服务器

Web 服务器使用 HTTP 和客户端通信，默认使用 TCP 的 80 端口侦听客户端的请求。

超文本传输协议（HyperText Transfer Protocol, HTTP）是互联网上应用最为广泛的一种网络协议，所有的 WWW 文件都必须遵守这个标准。设计 HTTP 最初的目的是为了提供一种发布和接收 HTML 页面的方法。

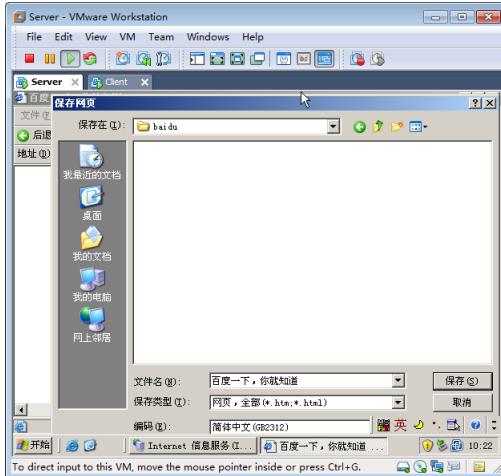
以下步骤将会创建一个 Web 站点，然后在客户端使用默认端口 80 访问 Web 站点，更改 Web 站点端口为 8080，并在客户端使用 8080 访问 Web 站点。

(1) 如图 2-41 所示，在 Server 计算机上访问百度网站，选择“文件”→“另存为”命令。

(2) 如图 2-42 所示，将网页另存到 C 盘根目录下 baidu 文件夹中。



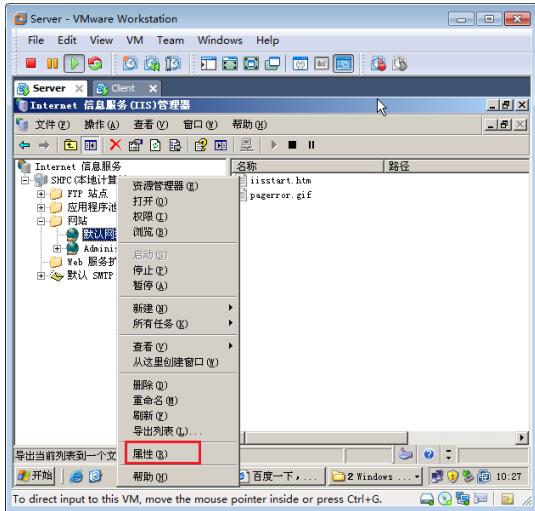
▲图 2-41 选择“另存为”命令



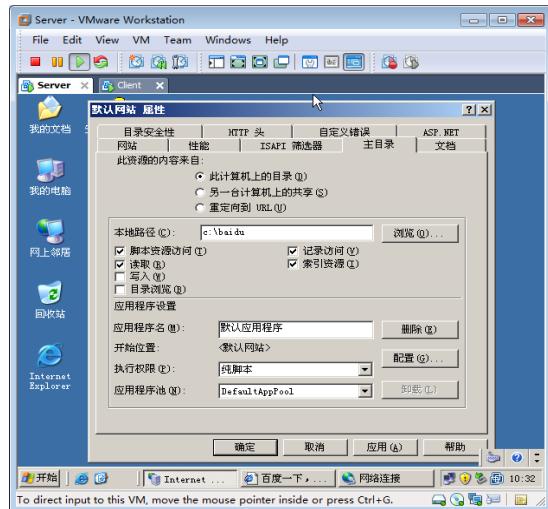
▲图 2-42 保存网页

(3) 如图 2-43 所示，打开“Internet 信息服务 (IIS) 管理器”窗口，右击“默认网站”节点，在弹出的快捷菜单中选择“属性”命令。

(4) 如图 2-44 所示，在弹出的“默认网站 属性”对话框的“主目录”选项卡中，将本地路径更改为“c:/baidu”。这就指定了存放的文件夹。



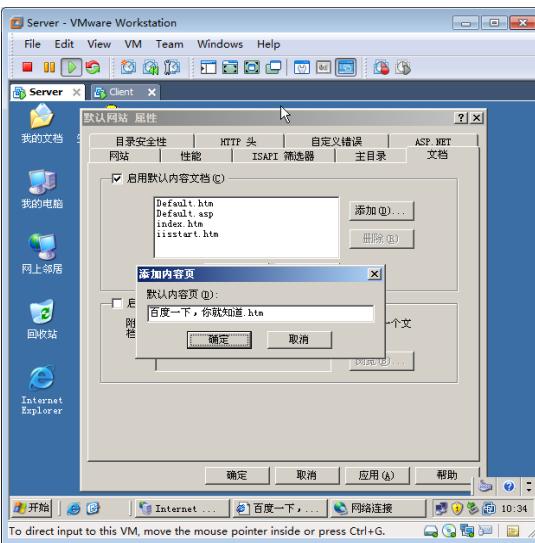
▲图 2-43 打开网站属性



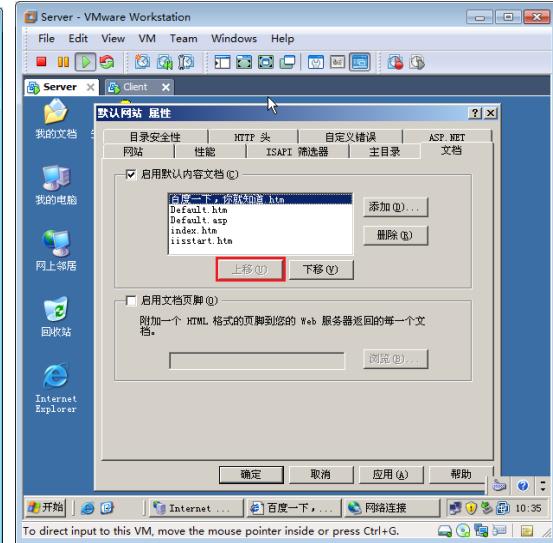
▲图 2-44 查看网站目录

(5) 如图 2-45 所示，在“文档”选项卡中，单击“添加”按钮，在弹出的“添加默认内容页”对话框中，输入“百度一下，你就知道.htm”，单击“确定”按钮。

(6) 如图 2-46 所示，在“启动默认内容文档”选项组中选中“百度一下，你就知道.htm”选项，单击“上移”按钮，使选中的选项移至顶端。单击“确定”按钮。这就指定其为该网站的首页。



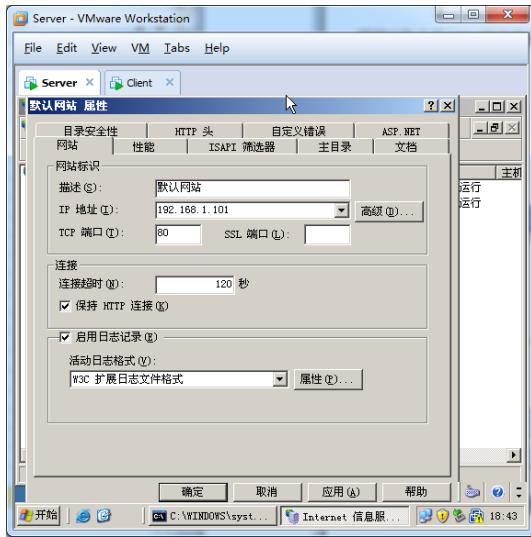
▲图 2-45 指定网站首页



▲图 2-46 上移至顶端

(7) 如图 2-47 所示，在“网站”选项卡中，可以看到该网站使用的是 TCP 的 80 端口。单击“确定”按钮。

(8) 如图 2-48 所示, 在 Client 计算机上打开 IE 浏览器, 输入 Server 网址, 可以访问该网站的首页。



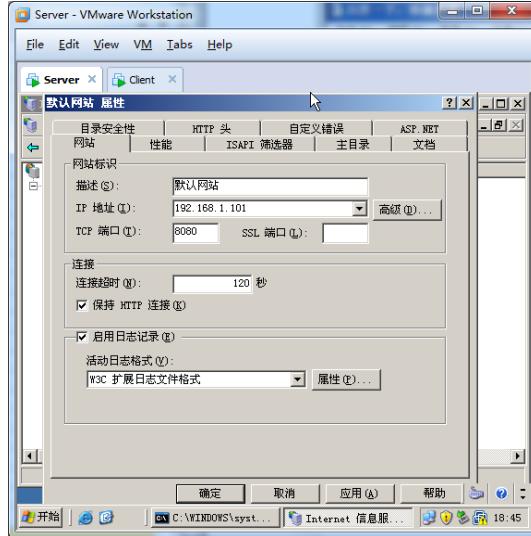
▲图 2-47 查看网站使用的端口



▲图 2-48 访问网站

(9) 如图 2-49 所示, 在 Server 计算机上, 将网站侦听的 TCP 端口更改为 8080, 单击“确定”按钮。

(10) 如图 2-50 所示, 在 Client 计算机上, 打开 IE, 在“地址”栏中输入 <http://10.7.10.239:8080> 指定端口。能够访问该网站。



▲图 2-49 更改 TCP 端口



▲图 2-50 使用指定的端口访问

(11) 在命令提示符下输入 netstat -n 命令可以看到 Client 和 Server 使用 TCP 的 8080 端口建立的会话。

2.4.4 配置 SMTP 服务和 POP3 服务

SMTP (Simple Mail Transfer Protocol) 即简单邮件传输协议, 它是一组用于由源地址到目的地址传送邮件的规则, 由它来控制信件的中转方式。SMTP 协议属于 TCP/IP 协议族, 它帮助每台计算机在发送或中转信件时找到下一个目的地。通过 SMTP 协议所指定的服务器, 就可以把 E-mail 寄到收信人的服务器上, 整个过程只要几分钟。SMTP 服务器则是遵循 SMTP 协议的发送邮件服务器, 用来发送或中转发出的电子邮件。

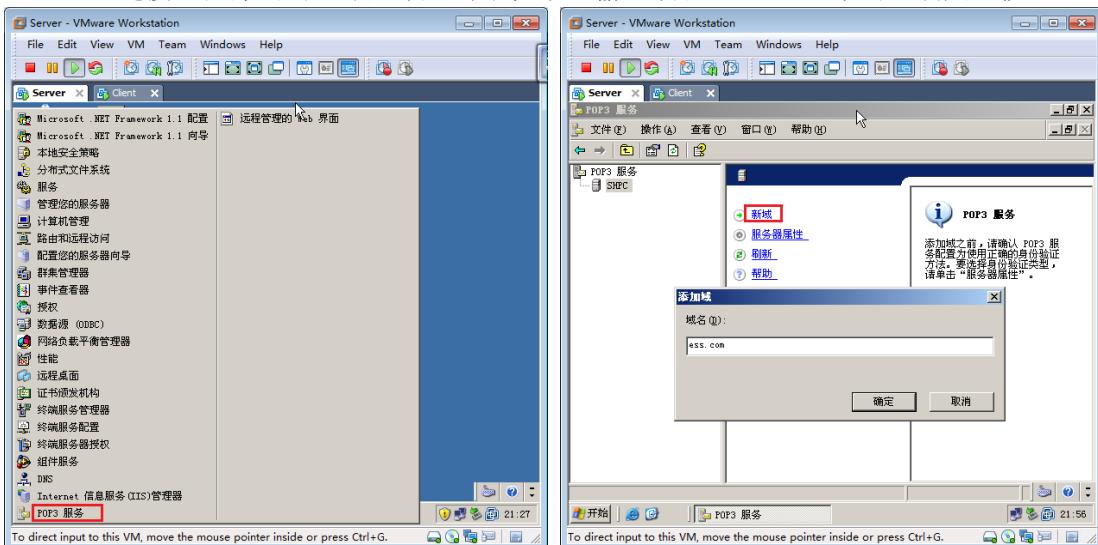
POP3 (Post Office Protocol 3) 即邮局协议的第 3 个版本, 它是规定个人计算机如何连接到互联网上的邮件服务器进行收发邮件的协议。它是因特网电子邮件的第一个离线协议标准, POP3 协议允许用户从服务器上把邮件存储到本地主机 (即自己的计算机) 上, 同时根据客户端的操作删除或保存在邮件服务器上的邮件, 而 POP3 服务器则是遵循 POP3 协议的接收邮件服务器, 用来接收电子邮件的。POP3 协议是 TCP/IP 协议族中的一员, 由 RFC 1939 定义。本协议主要用于支持使用客户端远程管理在服务器上的电子邮件。

以下示例将会配置 Server 上的 SMTP 服务和 POP3 服务, 并且在 Client 计算机上配置邮件服务器客户端 Outlook Express, 收发电子邮件。

- 配置 POP3 服务, 创建邮箱。
- 配置 SMTP 服务, 创建远程域, 允许将电子邮件发送到 Internet。
- 配置服务器和客户端不使用默认的端口收邮件。

操作步骤:

- (1) 如图 2-51 所示, 在 Server 计算机上, 选择“开始”→“程序”→“管理工具”→“POP3 服务”菜单命令。
- (2) 如图 2-52 所示, 在打开的“POP3 服务”窗口中, 选中 SHPC 选项, 单击“新建”链接, 在弹出的“添加域”对话框中, 输入域名 ess.com, 单击“确定”按钮。



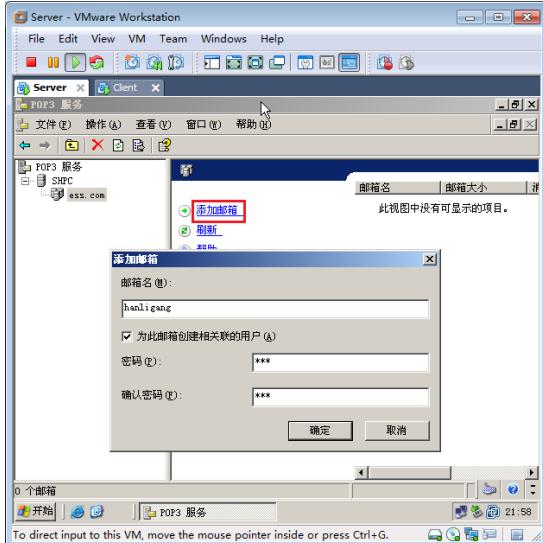
▲图 2-51 选择“POP3 服务”命令

▲图 2-52 创建域

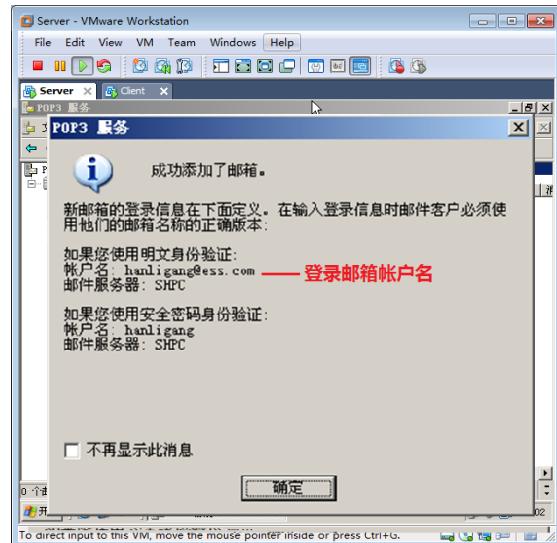
- (3) 如图 2-53 所示, 选中 ess.com 选项, 单击“添加邮箱”链接, 在弹出的“添加邮箱”对话框中, 输入邮箱名称 hanligang, 选中“为此邮箱创建相关联的用户”复

选框，输入密码，单击“确定”按钮。这样，也就同时在该 Server 计算机上创建了一个用户 hanligang。

- (4) 如图 2-54 所示，在弹出的“POP3 服务”对话框中，注意观察登录邮箱账户名，单击“确定”按钮。



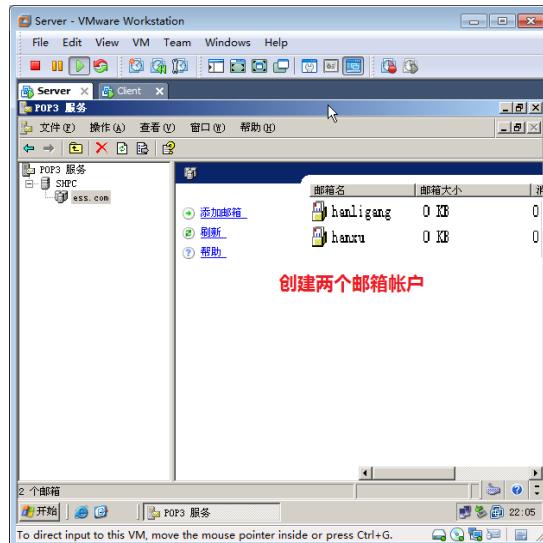
▲图 2-53 添加邮箱



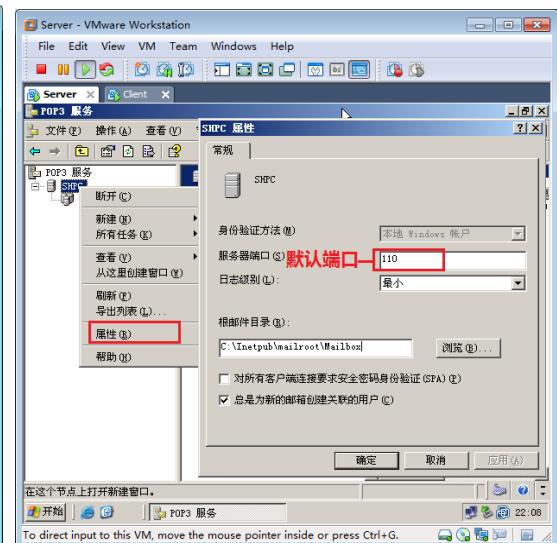
▲图 2-54 “POP3 服务”对话框

- (5) 如图 2-55 所示，在 ess.com 域下创建 hanxu 邮箱和用户。

- (6) 如图 2-56 所示，右击 SHPC 节点，在弹出的快捷菜单中选择“属性”命令，在弹出的“SHPC 属性”对话框中，可以看到 POP3 服务的默认端口为 TCP 的 110。



▲图 2-55 创建两个邮箱

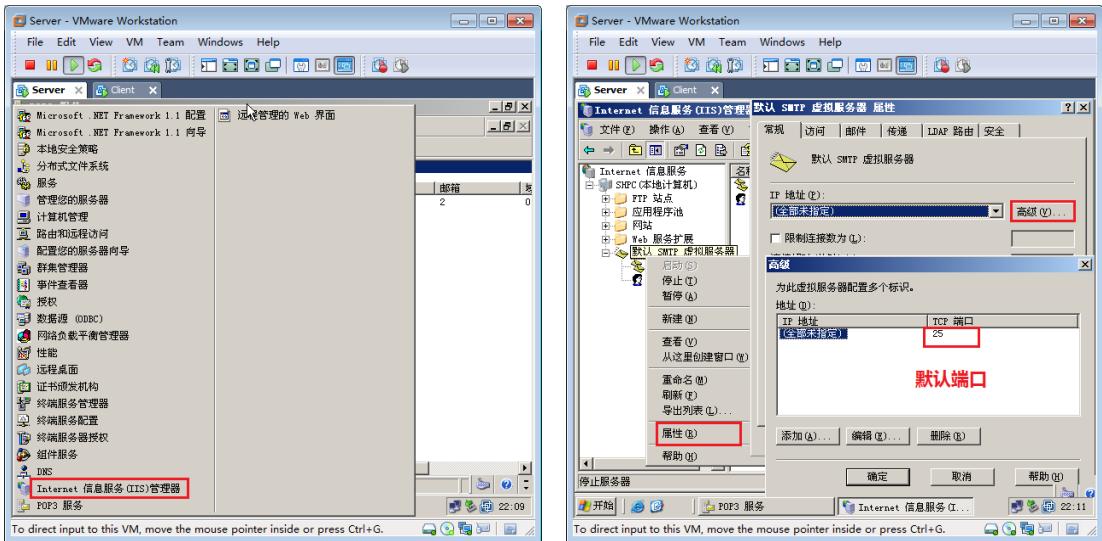


▲图 2-56 查看 POP3 服务的端口

- (7) 如图 2-57 所示，选中“Internet 信息服务 (IIS) 管理器”命令。

- (8) 如图 2-58 所示，在打开的“Internet 信息服务 (IIS) 管理器”窗口中，右击“默认 SMTP 虚拟服务器”节点，在弹出的快捷菜单中选择“属性”命令。

(9) 如图 2-58 所示, 在弹出的“默认 SMTP 虚拟服务器 属性”对话框中, 单击“高级”按钮, 可以在弹出的“高级”对话框中看到默认端口为 TCP 的 25, 单击“确定”按钮。

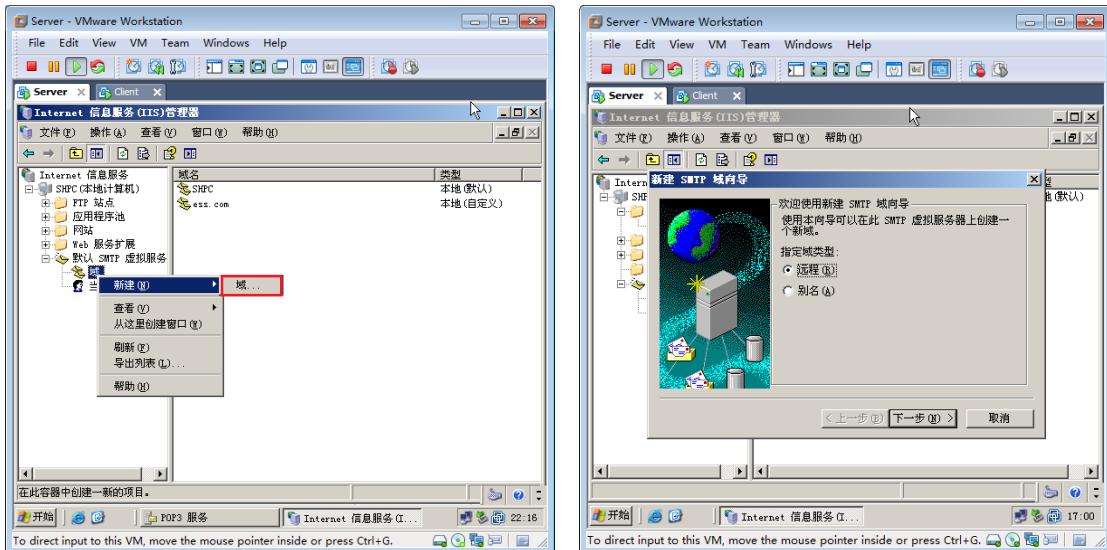


▲图 2-57 选择“Internet 信息服务 (IIS) 管理器”命令

▲图 2-58 查看 SMTP 默认端口

(10) 如图 2-59 所示, 右击“域”节点, 在弹出的快捷菜单中选择“新建”→“域”命令。

(11) 如图 2-60 所示, 在弹出的“新建 SMTP 域向导”对话框中, 选中“远程”单选按钮, 单击“下一步”按钮。

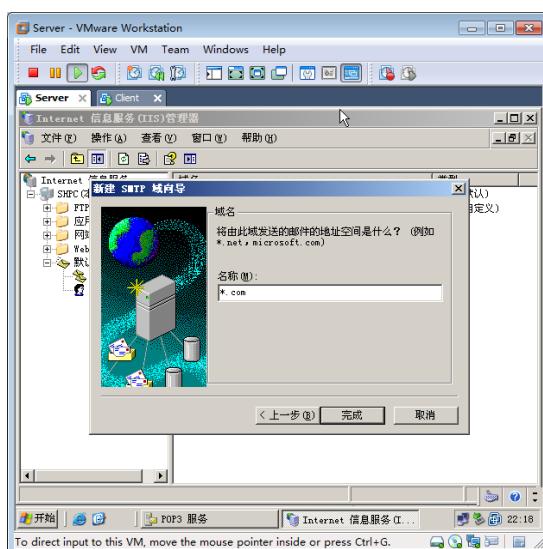


▲图 2-59 新建域

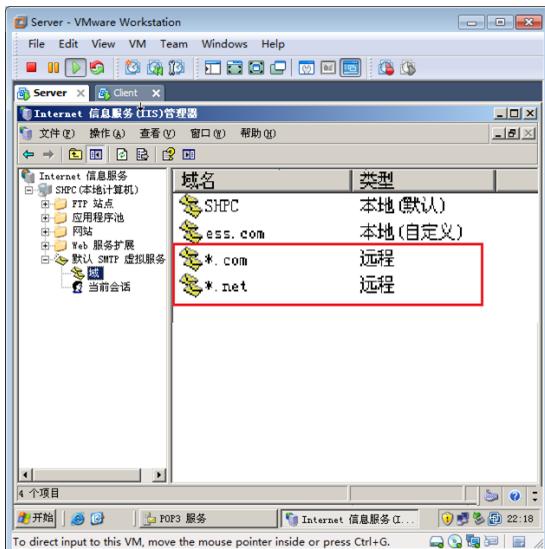
▲图 2-60 指定为远程域

(12) 如图 2-61 所示, 在弹出的“域名”设置界面中, 输入名称*.com, 单击“完成”按钮, 其中, “*”是通配符。

(13) 如图 2-62 所示, 同样创建*.net 远程域, 其中, “*”是通配符。

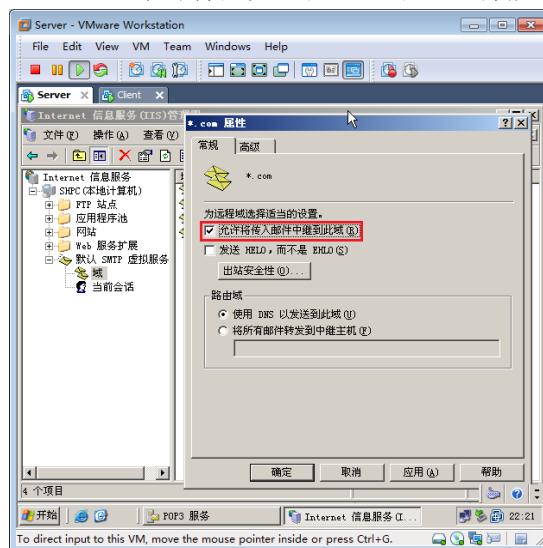


▲图 2-61 输入域名称

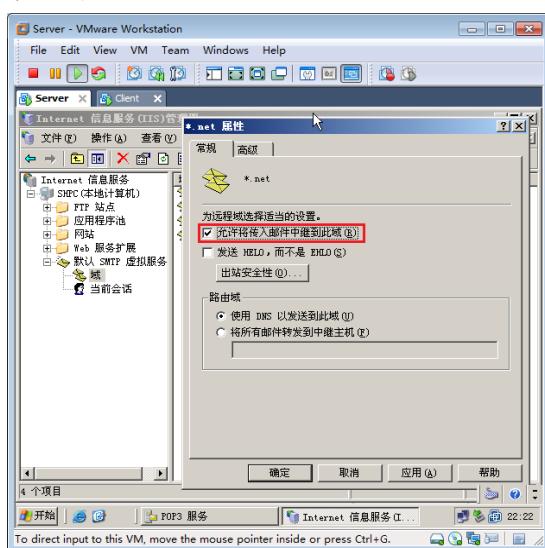


▲图 2-62 创建两个远程域

- (14) 如图 2-63 所示, 双击*.com 选项, 在弹出的“*.com 属性”对话框的“常规”选项卡中, 选中“允许将传入邮件中继到此域”复选框, 单击“确定”按钮。
- (15) 如图 2-64 所示, 同样配置*.net 远程域, 在“*.net 属性”对话框的“常规”选项卡中, 选中“允许将传入邮件中继到此域”复选框, 单击“确定”按钮。这样, SMTP 服务能将 onesthan@hotmail.com, han@inhe.net 邮件转发到这些邮局。电子邮件只要包括.com 和.net 都能够中继出去。

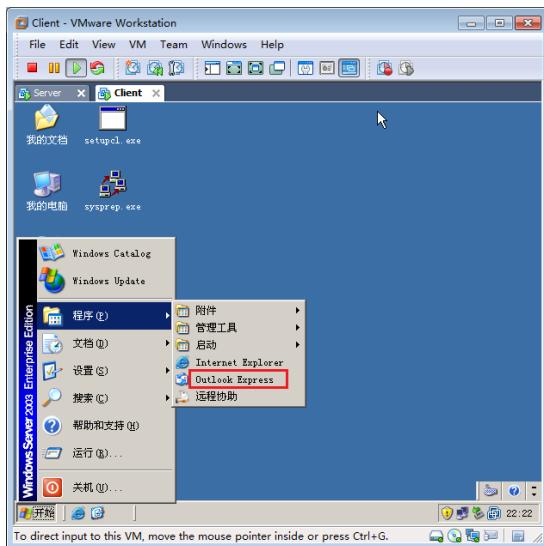


▲图 2-63 允许将传入邮件中继到*.com

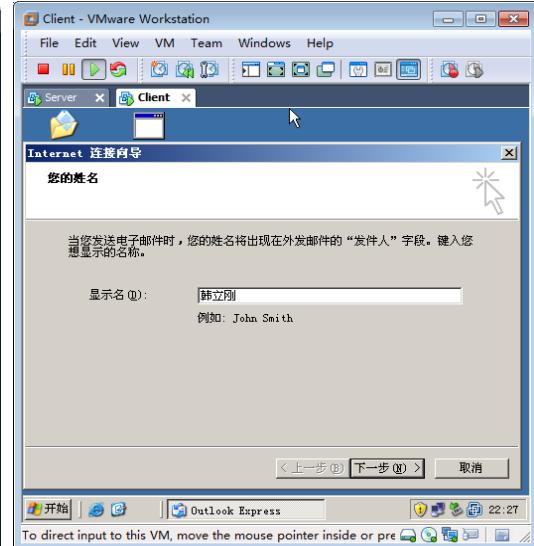


▲图 2-64 允许将传入邮件中继到*.net

- (16) 如图 2-65 所示, 在 Client 计算机上, 选择“开始”→“程序”→Outlook Express 命令。
- (17) 如图 2-66 所示, 在弹出的“您的姓名”设置界面中, 输入显示名, 单击“下一步”按钮。



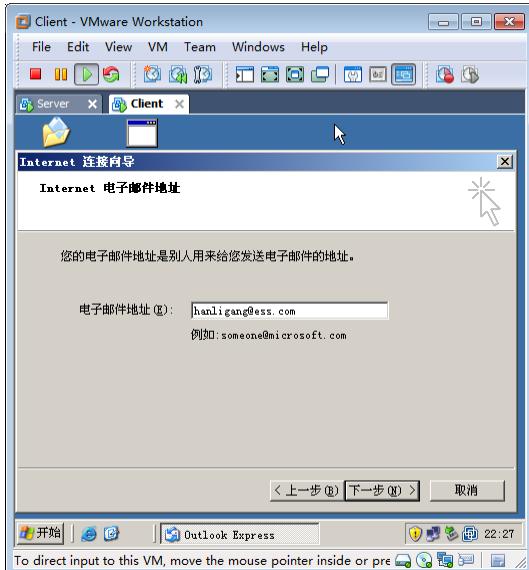
▲图 2-65 选择 Outlook Express



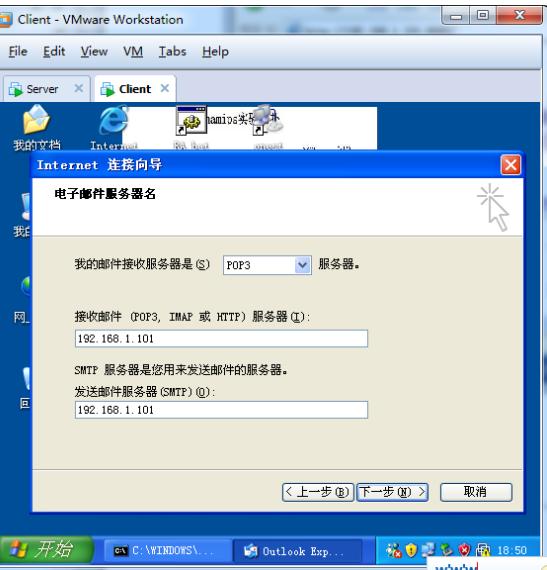
▲图 2-66 输入显示名

(18) 如图 2-67 所示，在弹出的“Internet 电子邮件地址”设置界面中，输入 hanligang@ess.com，单击“下一步”按钮。

(19) 如图 2-68 所示，在弹出的“电子邮件服务器名”设置界面中，选择 POP3 服务器，指定接收邮件服务器的地址和发送邮件服务器的地址，在这里都是 Server 的 IP 地址，单击“下一步”按钮。



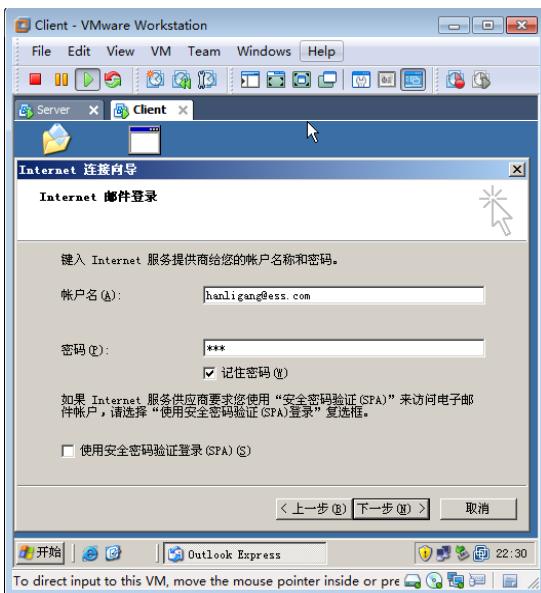
▲图 2-67 配置电子邮件地址



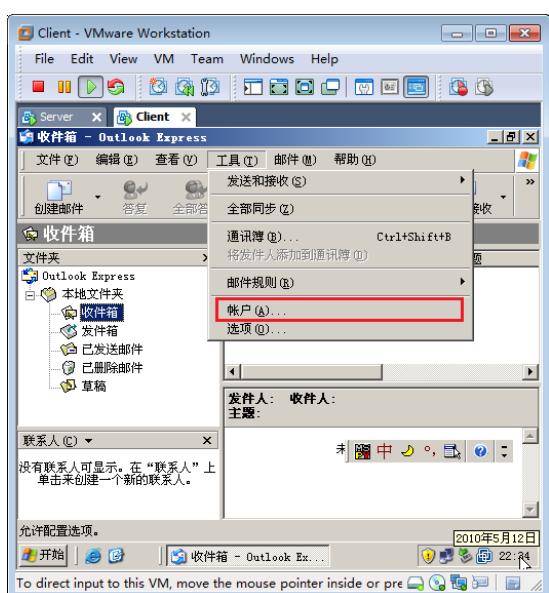
▲图 2-68 输入收发电子邮件服务器的地址

(20) 如图 2-69 所示，在弹出的“Internet 邮件登录”设置界面中，输入账户名 hanligang@ess.com 和密码，选中“记住密码”复选框，单击“下一步”按钮，完成账户的配置。

(21) 如图 2-70 所示，选择“工具”→“账户”菜单命令。

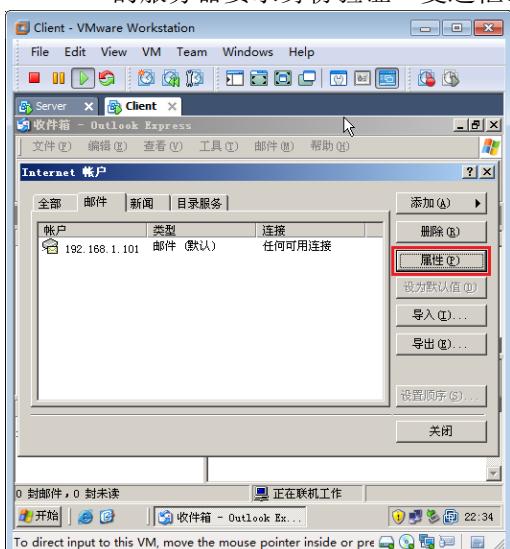


▲图 2-69 输入账户名和密码

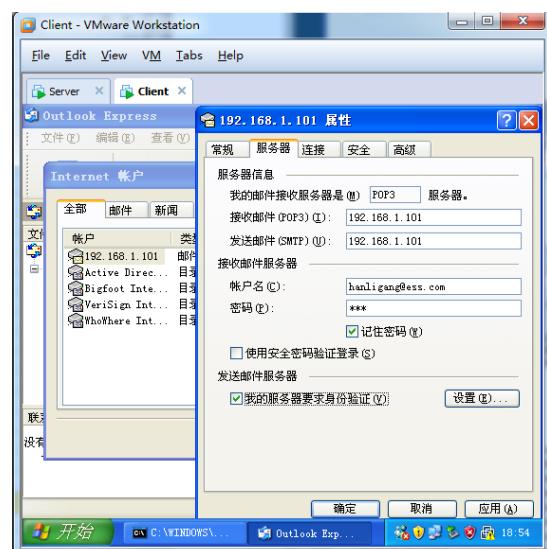


▲图 2-70 选择“账户”命令

- (22) 如图 2-71 所示，在弹出的“Internet 账户”对话框的“邮件”选项卡中，选中刚刚创建的邮件账户，然后单击“属性”按钮。
- (23) 如图 2-72 所示，在出现的邮箱账户属性对话框的“服务器”选项卡中，选中“我的服务器要求身份验证”复选框。

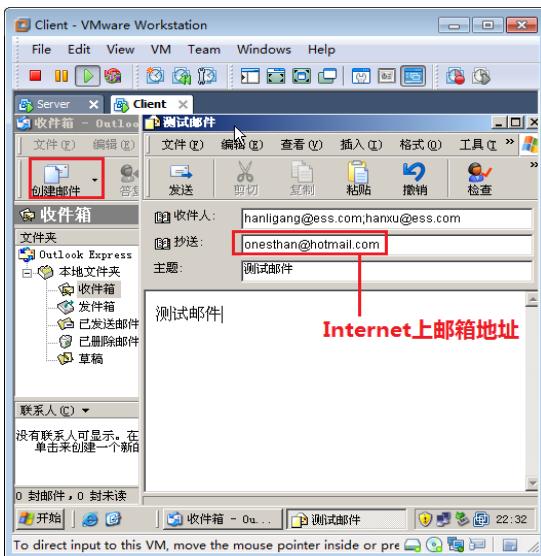


▲图 2-71 “Internet 账户”对话框

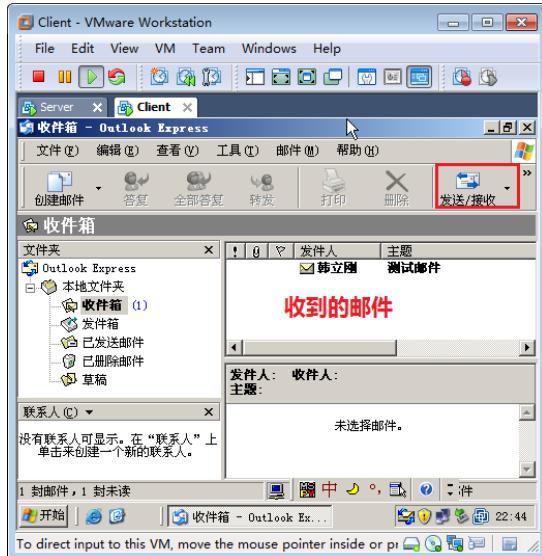


▲图 2-72 配置验证

- (24) 如图 2-73 所示，单击“创建邮件”按钮，在“测试邮件”窗口的“收件人”文本框中输入“hanligang@ess.com”和“hanxu@ess.com”；“抄送”文本框中输入“onesthan@hotmail.com”，单击“发送”按钮。
- (25) 如图 2-74 所示，单击“发送/接收”按钮，可以看到收到自己的邮件。

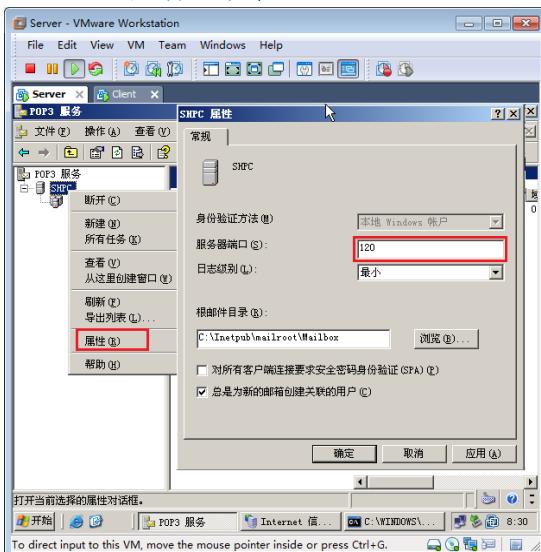


▲图 2-73 创建邮件

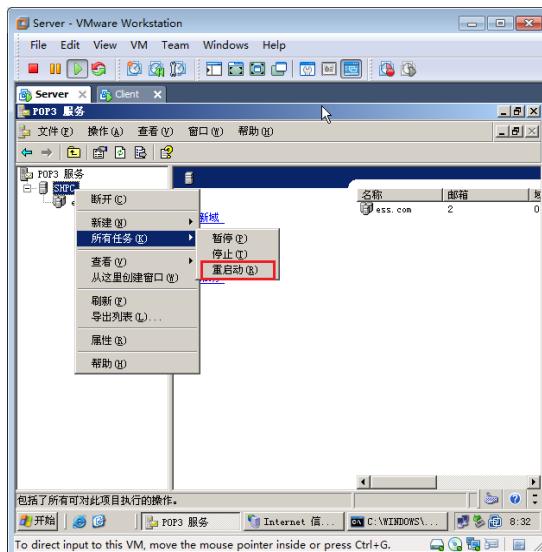


▲图 2-74 发送邮件

- (26) 如图 2-75 所示, 在 Server 计算机上, 打开“POP3 服务”窗口, 右击 SHPC 节点, 在弹出的快捷菜单中选择“属性”命令, 在弹出的“SHPC 属性”对话框中, 将服务器端口更改为 120, 单击“确定”按钮。
- (27) 如图 2-76 所示, 右击 SHPC 节点, 在弹出的快捷菜单中选择“所有任务”→“重启”命令。

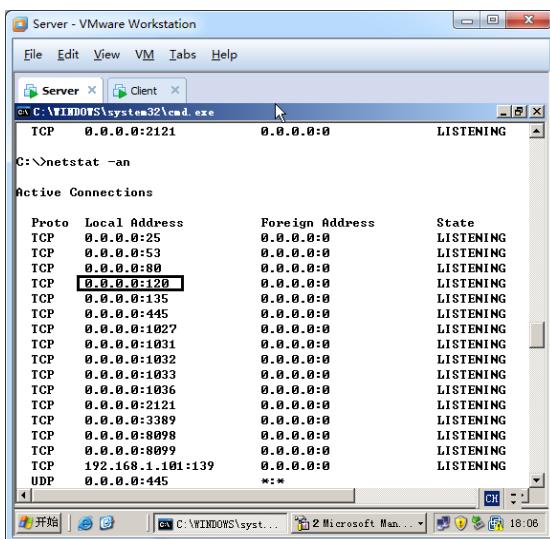


▲图 2-75 更改邮件服务器端口

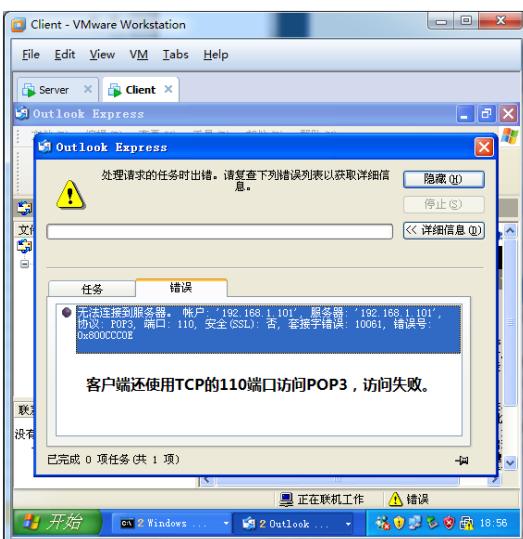


▲图 2-76 重启服务

- (28) 如图 2-77 所示, 在命令提示符下输入 netstat -an 命令, 可以看到出现了在 120 端口侦听。
- (29) 如图 2-78 所示, 在 Client 计算机上, 单击“发送/接收”按钮, 客户端使用默认端口接收电子邮件失败。



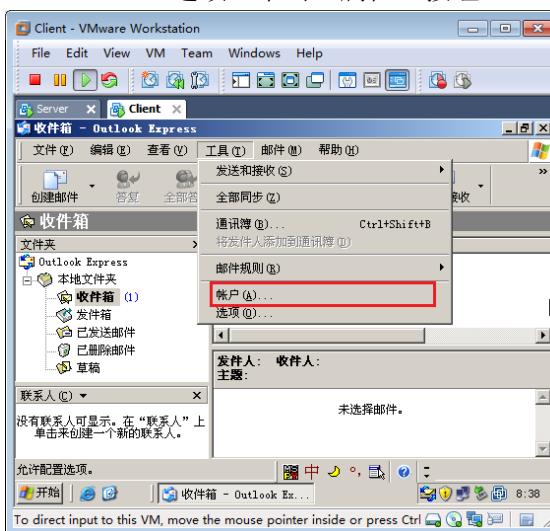
▲图 2-77 查看监听的端口



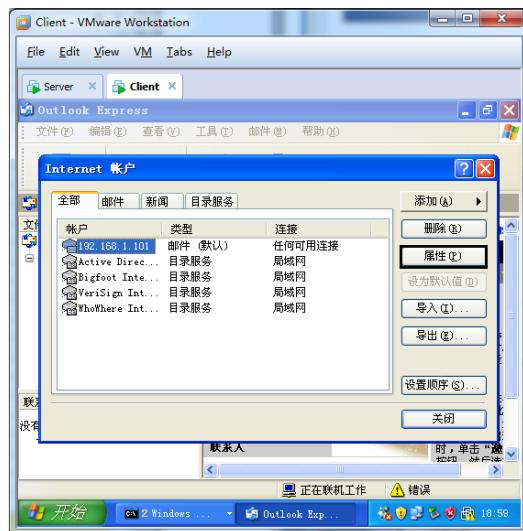
▲图 2-78 客户端访问失败

(30) 如图 2-79 所示, 选择“工具”→“账户”菜单命令。

(31) 如图 2-80 所示, 在弹出的“Internet 账户”对话框的“邮件”选项卡中, 选中 10.7.10.239 选项, 单击“属性”按钮。



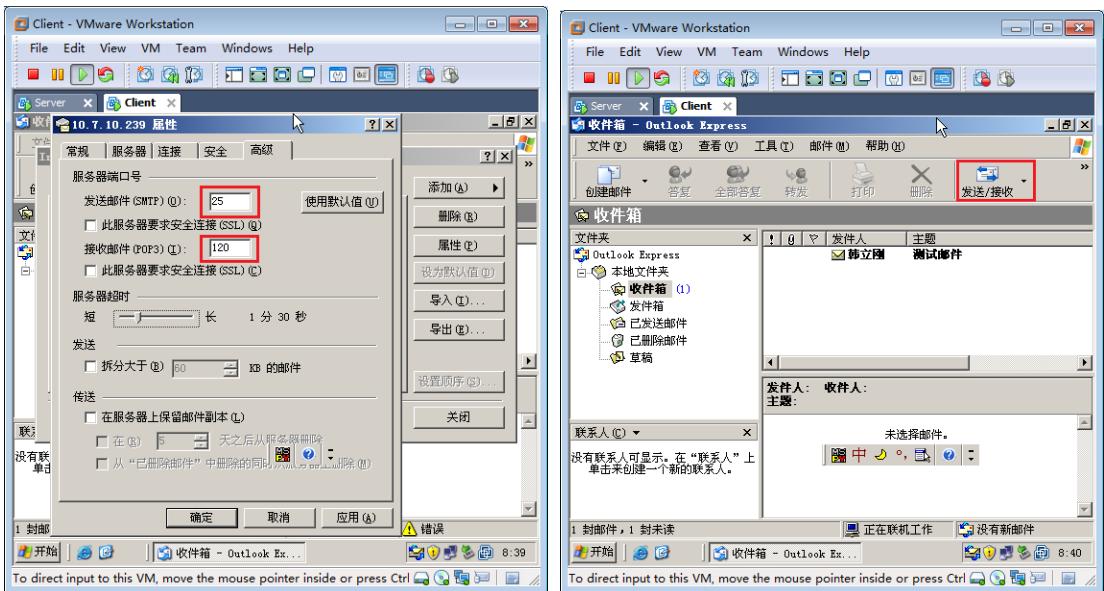
▲图 2-79 配置 Outlook 账户



▲图 2-80 配置属性

(32) 如图 2-81 所示, 在弹出的“10.7.10.239 属性”对话框的“高级”选项卡中, 将接收邮件端口更改为 120, 使之和服务器侦听的端口一致, 单击“确定”按钮。

(33) 如图 2-82 所示, 再次单击“发送/接收”按钮, 成功。



▲图 2-81 更改客户端端口

▲图 2-82 发送接收成功

总结

服务器更改服务端口，客户端也要做相应更改，才能正确请求服务。

2.4.5 启用远程桌面且更改默认端口

无论 Windows XP、Windows 7 还是 Windows Server 2003 或 Windows Server 2008，都提供了远程桌面服务。启用远程桌面后，就可以允许远程计算机通过网络连接到计算机，进行远程管理。下面将演示在 Server 计算机上启用远程桌面，在 Client 计算机上使用 mstsc 连接 Server。

有些服务没有提供更改端口的界面，比如，远程桌面服务就没有提供更改端口的界面，它可以通过注册表更改端口。但是有些系统协议使用固定的端口号，是不能被改变的，比如 139 端口专门用于 NetBIOS 与 TCP/IP 之间的通信，不能手动改变。

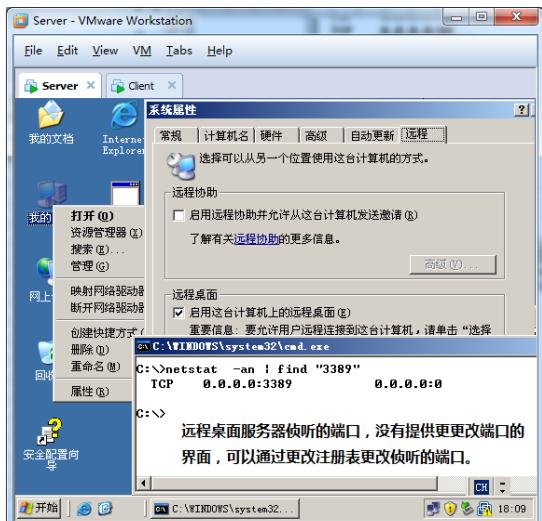
提示

如果你不知道如何更改某个服务的端口，可以访问 <http://www.baidu.com> 进行搜索。

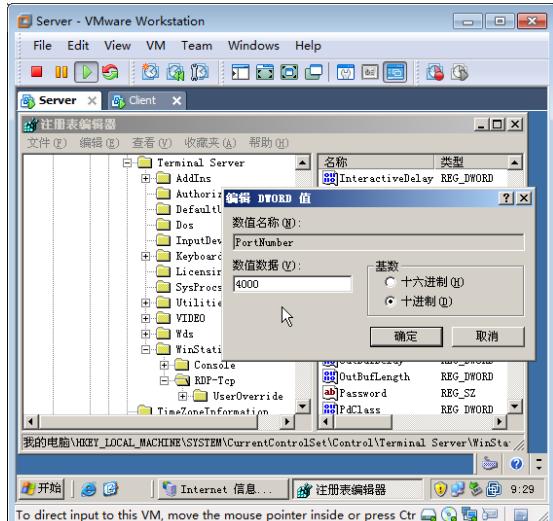
以下示例将远程桌面服务的侦听端口由默认的 3389 更改为 4000。

- (1) 在 Server 计算机上，右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令。
- (2) 如图 2-83 所示，在弹出的“系统属性”对话框的“远程”选项卡中，选中“启用这台计算机上的远程桌面”复选框。
- (3) 如图 2-83 所示，在命令提示符下输入 netstat -an | find " 3389 " 命令，能够看到远程桌面在 3389 端口侦听。
- (4) 单击“运行”→“开始”→“运行”，输入 regedit，单击“确定”按钮，启动注册表编辑器。

- (5) 如图 2-84 所示, 打开注册表编辑器, 展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp\PortNumber 注册表项。
- (6) 如图 2-84 所示, 在“编辑”菜单中, 选择“修改”命令, 然后选中“十进制”单选按钮。

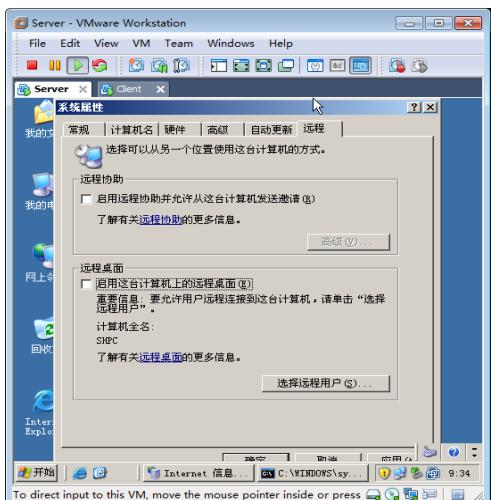


▲图 2-83 启用远程桌面

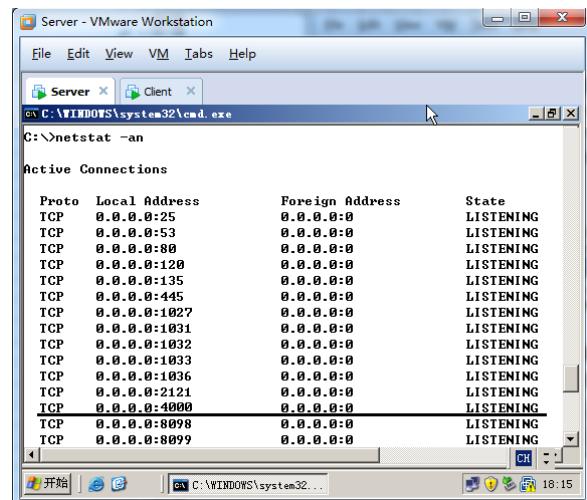


▲图 2-84 更改注册表

- (7) 输入新端口号, 然后单击“确定”按钮。
- (8) 退出注册表编辑器。
- (9) 如图 2-85 所示, 打开“系统属性”对话框, 在“远程”选项卡中, 取消选中“启用这台计算机上的远程桌面”复选框, 单击“应用”按钮, 再选中“启用这台计算机上的远程桌面”复选框, 单击“应用”按钮。相当于重启远程桌面服务。
- (10) 如图 2-86 所示, 在命令提示符下输入 netstat -an 命令, 可以看到侦听的端口被改为 4000。



▲图 2-85 重启远程桌面

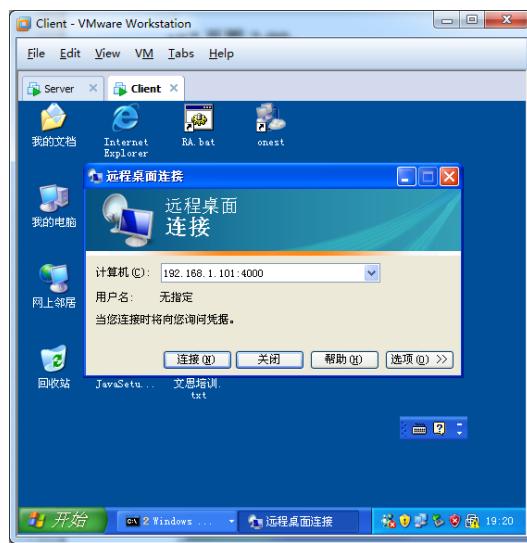


▲图 2-86 查看侦听的端口

- (11) 如图 2-87 所示，在 Client 计算机上，选择“开始”→“运行”，在打开的“运行”对话框中，输入 mstsc，单击“确定”按钮。
- (12) 如图 2-87 所示，在弹出的“远程桌面连接”对话框中，输入 Server 的 IP 地址，单击“连接”按钮。默认是使用 3389 端口连接服务器，出现连接失败提示对话框，单击“确定”按钮。
- (13) 如图 2-88 所示，在“远程桌面连接”对话框中，输入 Server 的 IP 地址后面添加冒号以及端口号 4000，单击“连接”按钮。

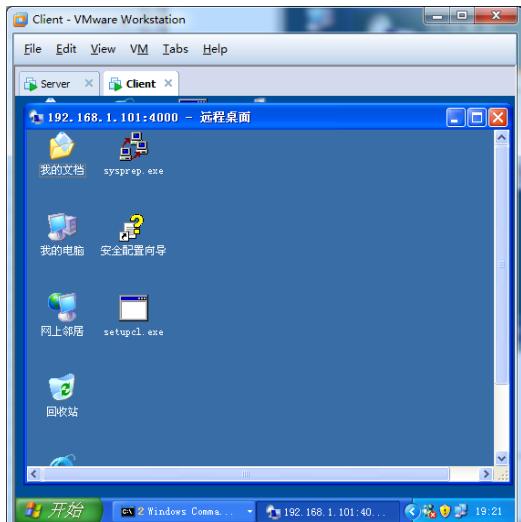


▲图 2-87 客户端使用默认的端口连接失败



▲图 2-88 使用指定端口连接服务器

- (14) 如图 2-89 所示，可以看到使用 4000 端口连接 Server 远程桌面成功。
- (15) 如图 2-90 所示，在命令提示符下输入 netstat -n 命令，可以看到远程桌面建立的会话。



▲图 2-89 使用 4000 端口连接成功



▲图 2-90 查看建立的会话

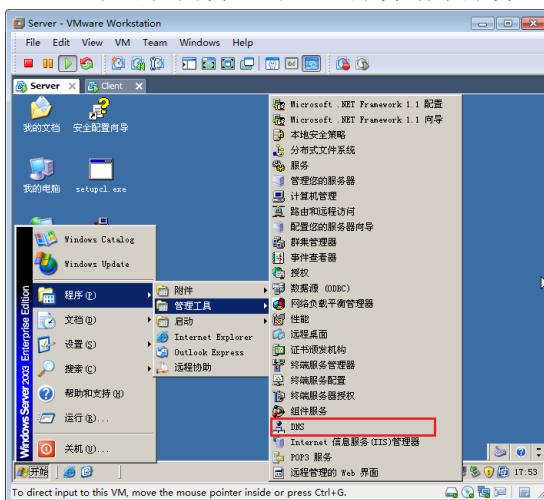
2.4.6 配置 DNS 服务器

DNS 是域名系统 Domain Name System 的缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。在 Internet 上域名与 IP 地址之间是一对一（或者多对一）的关系，域名虽然便于人们记忆，但计算机之间只能互相认识 IP 地址，它们之间的转换工作称为域名解析。域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。DNS 命名用于 Internet 等 TCP/IP 网络中，通过用户友好的名称查找计算机和服务。当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与之相关的其他信息，如 IP 地址。你在上网时输入的网址，是通过域名解析系统解析找到了相对应的 IP 地址，这样才能上网。因此域名的最终指向是 IP。

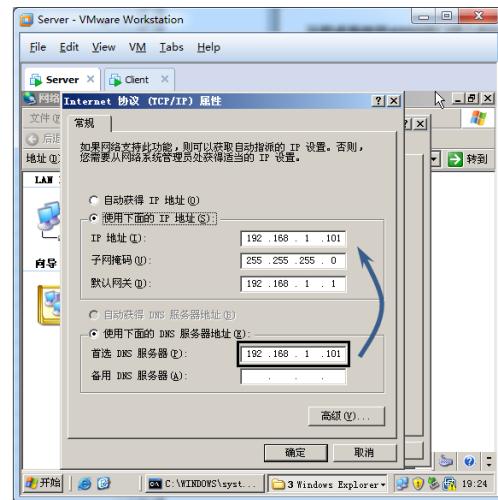
下面将演示配置企业自己的 DNS 服务器负责解析内网服务器的域名 ess.com 和 Internet 域名。内网网站的域名为 www.ess.com，IP 地址为 10.7.1.5。

提示 DNS 服务器默认有根提示，指向 Internet 的根 DNS 服务器，内网的 DNS 服务器只要能够连接 Internet 就能解析 Internet 网站的域名。

- (1) 如图 2-91 所示，在 Server 计算机上，选择“开始”→“程序”→“管理工具”→DNS 命令，打开 DNS 管理工具。
- (2) 如图 2-92 所示，打开 Server 的本地连接，在“Internet 协议 (TCP/IP) 属性”对话框中，将自己的首选 DNS 服务器指向自己的 IP 地址，这样 Server 作为 DNS 客户机就可以向自己的 DNS 服务请求服务。



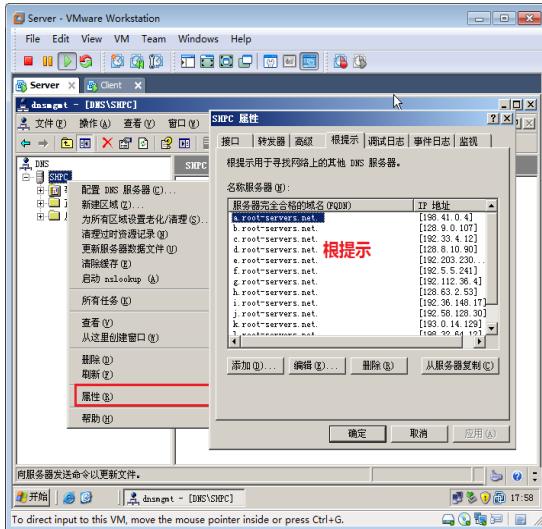
▲图 2-91 选择 DNS 命令



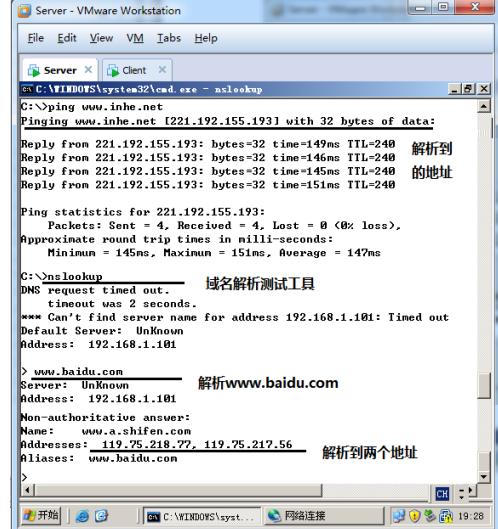
▲图 2-92 配置使用的 DNS 服务器

- (3) 如图 2-93 所示，在打开的 DNS 管理工具中，右击 SHPC 节点，在弹出的快捷菜单中选择“属性”命令。在弹出的“SHPC 属性”对话框的“根提示”选项卡中，可以看到 Internet 的作为根的 DNS 服务器。只要装上 DNS 服务，就能解析 Internet 上的域名，DNS 服务器会向这些根 DNS 转发域名解析请求。
- (4) 如图 2-94 所示，在命令提示符下，输入 ping www.inhe.net 命令可以看到解析到的 IP 地址。

- (5) 如图 2-94 所示，在命令提示符下输入 nslookup 命令，回车，可以看到提供名称解析的 DNS 服务器，输入 www.baidu.com，回车，可以看到解析到的 IP 地址，在这里可以看到解析出两个 IP 地址，可以断定百度网站有镜像站点提供负载均衡。你可以输入 www.sohu.com，查看该域名对应的 IP 地址。



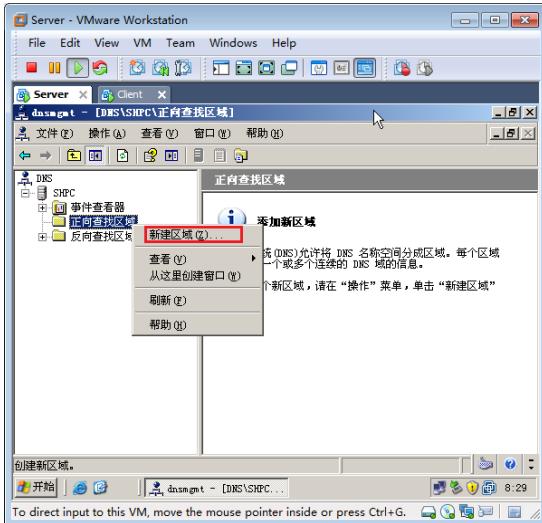
▲图 2-93 查看 DNS 根提示



▲图 2-94 测试名称解析

- (6) 如图 2-95 所示，你公司有一个内网网站，用户使用 www.ess.com 域名访问。你打算内网计算机使用 Server 能够解析内网网站域名。你可以在 DNS 服务器上创建正向查找区域。右击“正向查找区域”节点，在弹出的快捷菜单中选择“新建区域”命令。

- (7) 如图 2-96 所示，在弹出的“欢迎使用新建区域向导”设置界面中，单击“下一步”按钮。

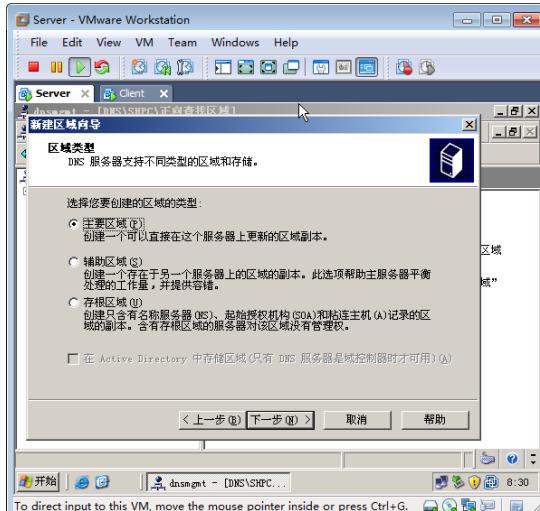


▲图 2-95 创建正向区域

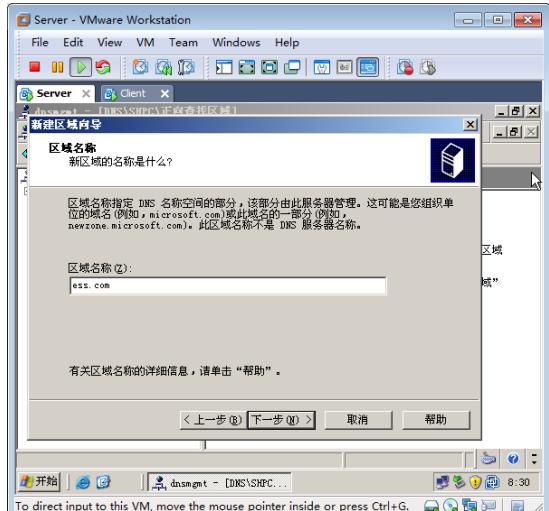


▲图 2-96 DNS 配置向导

- (8) 如图 2-97 所示, 在弹出的“区域类型”设置界面中, 选中“主要区域”单选按钮, 单击“下一步”按钮。
- (9) 如图 2-98 所示, 在弹出的“区域名称”设置界面中, 输入区域名称 ess.com, 单击“下一步”按钮。

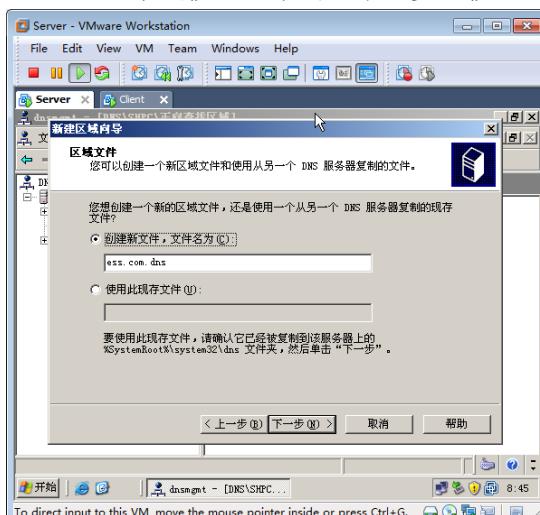


▲图 2-97 选择区域类型



▲图 2-98 输入区域名称

- (10) 如图 2-99 所示, 在弹出的“区域文件”设置界面中, 保持默认, 单击“下一步”按钮。
- (11) 如图 2-100 所示, 在弹出的“动态更新”设置界面中, 选中“不允许动态更新”单选按钮, 单击“下一步”按钮。

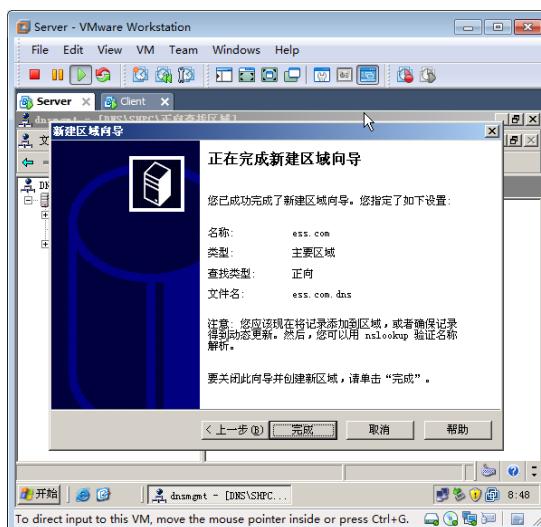


▲图 2-99 创建区域文件

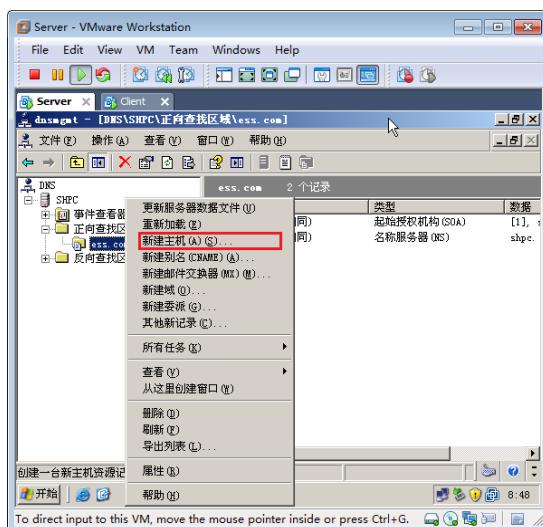


▲图 2-100 不允许动态更新

- (12) 如图 2-101 所示, 在弹出的“正在完成新建区域向导”设置界面中, 单击“完成”按钮。到目前为止该 DNS 服务器负责 ess.com 名称空间的域名解析。
- (13) 如图 2-102 所示, 在 ess.com 区域下添加主机记录, 右击 ess.com 节点, 在弹出的快捷菜单中选择“新建主机”命令。

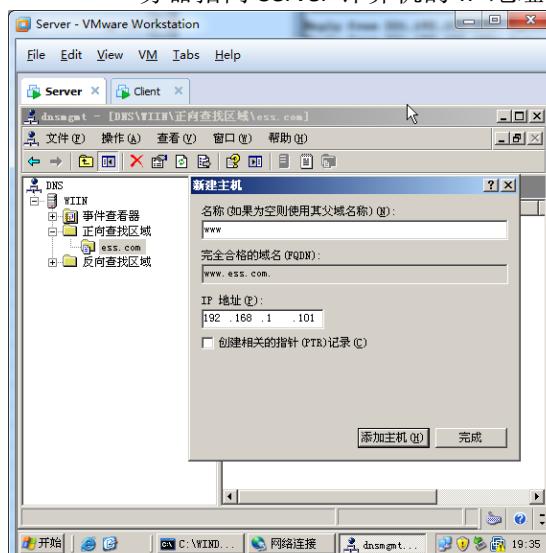


▲图 2-101 完成区域创建

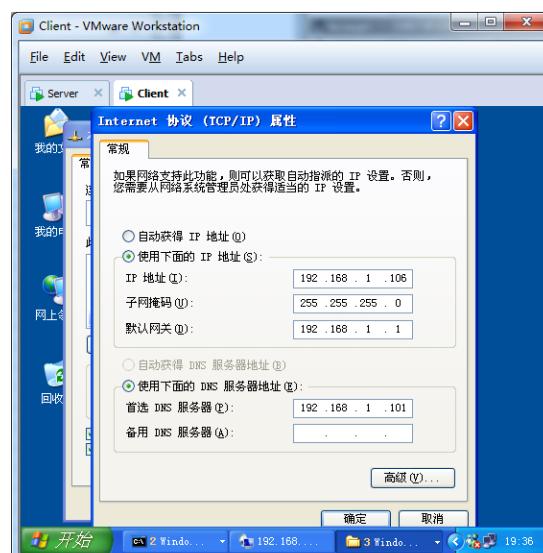


▲图 2-102 添加主机记录

- (14) 如图 2-103 所示，在弹出的“新建主机”对话框中，输入名称和 IP 地址。
- (15) 如图 2-104 所示，在 Client 计算机上，打开本地连接 TCP/IP 属性，将首选 DNS 服务器指向 Server 计算机的 IP 地址。

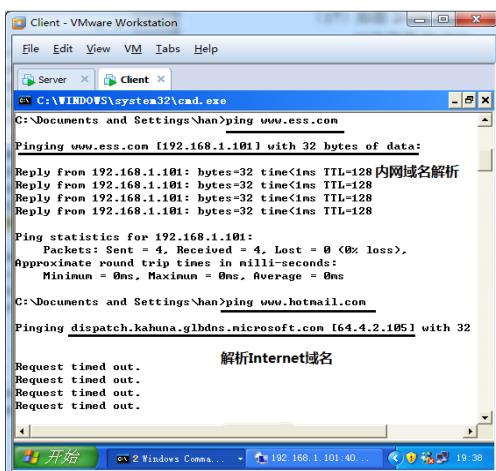


▲图 2-103 输入名称和 IP 地址

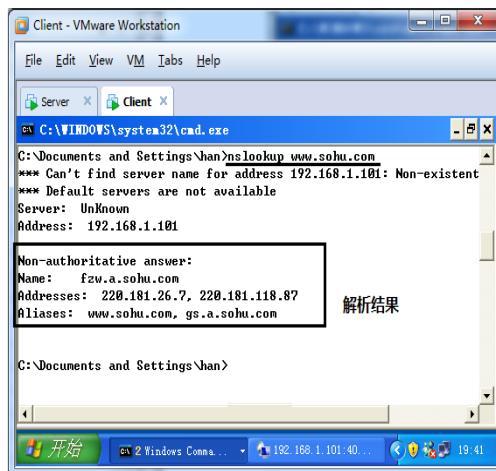


▲图 2-104 配置 DNS 客户端

- (16) 如图 2-105 所示，在命令提示符下输入 ping www.ess.com，能够解析出 IP 地址，输入 ping www.hotmail.com 也能够解析出 IP 地址。注意：出现 Request time out，并不意味着你不能访问该网站。
- (17) 如图 2-106 所示，在命令提示符下输入 nslookup www.sohu.com 能够解析出该网站的所有 IP 地址。



▲图 2-105 域名解析结果 (1)



▲图 2-106 域名解析结果 (2)

2.5 配置服务器网络安全

以上介绍了应用层协议和传输层协议的关系以及应用层协议和服务的关系。现在进一步介绍如何使用这些知识配置服务器安全。

下面将介绍 Windows 防火墙防止主动入侵、配置服务器的 TCP/IP 筛选保护服务器的安全、使用 IPSec 严格控制进出服务器的流量。

2.5.1 端口扫描

黑客打算攻击网络上的服务器，首先使用端口扫描工具，扫描服务器侦听的端口，这样入侵者就能根据扫描到的端口，知道服务器运行的服务，就可以尝试使用专门的攻击工具入侵服务器的某个服务。如果你的服务有漏洞，则入侵成功。

下面演示在 Client 上使用端口扫描工具 ScanPort 扫描服务器 Server 端口。该软件可以在网站 <http://down.51cto.com/> 搜索并下载。

(1) 将 Server 的 Web 服务、FTP 服务、SMTP 服务和 POP3 服务使用的端口改回默认值。

(2) 如图 2-107 所示，在“起始 IP”和“结束 IP”文本框中输入 Server 的 IP 地址，“端口号”文本框中输入“1-1024”，单击“扫描”按钮。

(3) 可以看到扫描到了 21、25、53、80、110、135、139 和 445 端口。没有扫描出 3389



▲图 2-107 端口扫描结果

端口，那是因为你指定的端口范围为 1~1024。

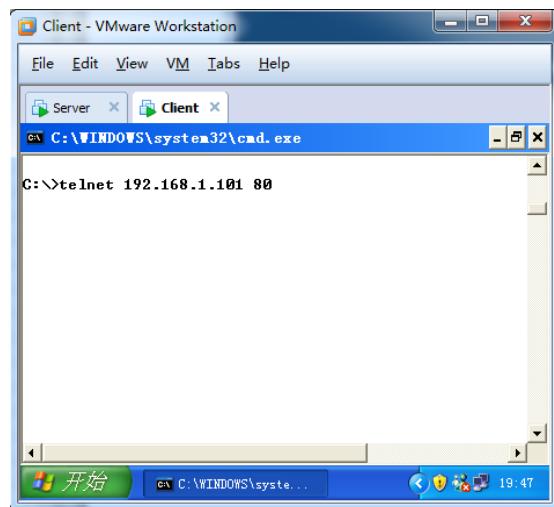
你可以根据端口扫描的结果判定，该服务器运行了 FTP 服务、SMTP 服务，DNS 服务、Web 服务和 POP3 服务，并且能够访问其共享资源，因为扫描到了其在 TCP 的 445 端口侦听。

2.5.2 使用 Telnet 排除网络故障

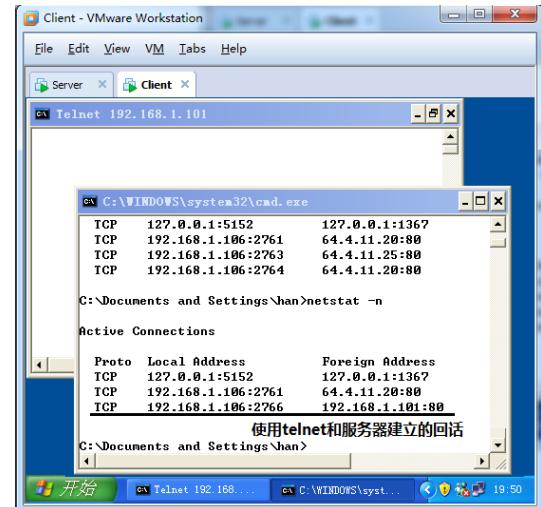
如果员工告诉你，他的计算机不能访问网站。你需要断定是他的计算机系统出了问题还是 IE 浏览器中了恶意插件，或者是网络层面的问题。

如图 2-108 所示，通过 Telnet 服务器的某个端口，就能断定是否访问该服务器的某个服务。如果你没有端口扫描工具，可以使用 Telnet 测试远程服务器侦听的端口。在命令提示符下输入 telnet 10.7.10.239 80。

如图 2-109 所示，如果 Telnet 成功，将会和服务器在该端口建立会话。再打开命令提示符，输入 netstat -n，可以看到建立的会话。

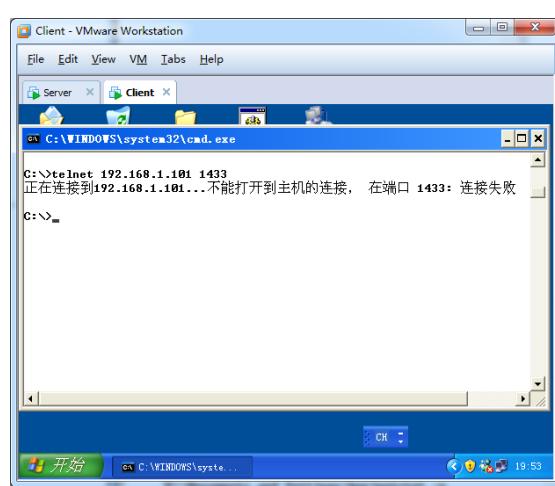


▲图 2-108 Telnet 测试



▲图 2-109 查看 Telnet 建立的会话

如图 2-110 所示，是 Telnet 端口失败的例子，失败的原因可能是远程计算机防火墙没有打开相应的端口，或远程服务器没有启动该端口对应的服务，或服务器和客户机之间的路由器拦截了到服务器特定端口的数据包。不管什么原因，Telnet 特定端口失败，就意味着不能访问远程服务器上的那个服务。如果 Telnet www.51cto.com 80 能够成功，而你的 IE 浏览器打不开该网址，说明是你的 IE 浏览器或计算机出现问题，即应用层出现问题，而非网络问题。



▲图 2-110 Telnet 失败的例子

2.5.3 Windows 防火墙保护客户端安全

Windows XP、Vista 和 Windows 7 都属于工作站操作系统，即安装在用户工作或娱乐用的计算机操作系统。对于普通使用者来说，要想从网络层面保护计算机安全，最好启用 Windows 防火墙。Windows 防火墙只阻截所有传入的未经请求的流量，对主动请求传出的流量不做理会。

如果在网络层不做任何防护，入侵者只要知道了你的计算机的管理员账号和密码，就能主动入侵你的系统。

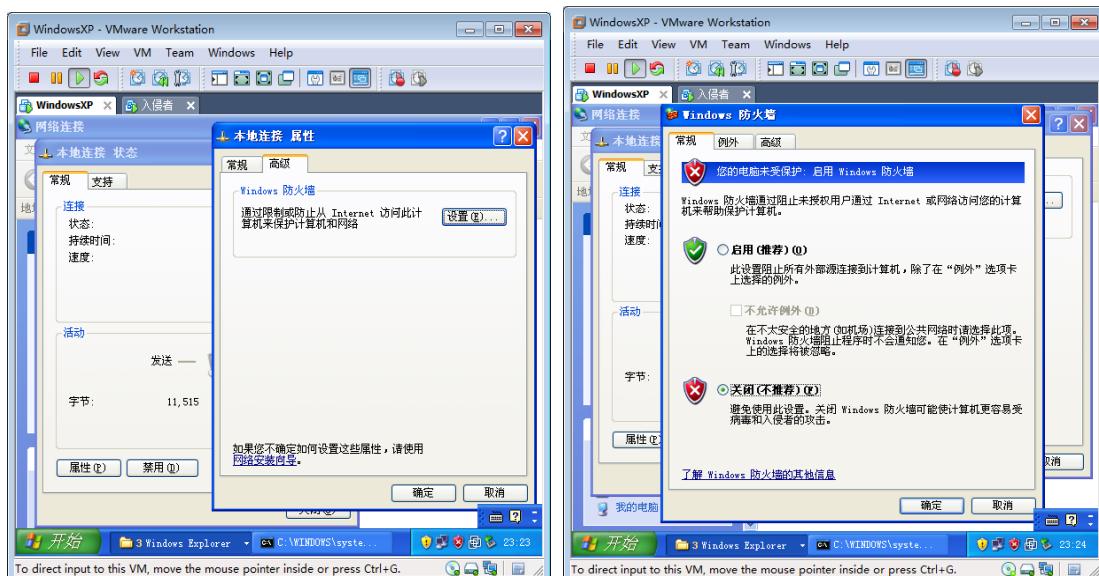
现在介绍一款能够主动入侵计算机，并且能够远程监视和控制计算机的软件“DameWare 迷你远程控制”，用以验证 Windows 防火墙的作用。该软件可以在 <http://down.51cto.com> 网站搜索 DameWare 并下载。

1. 任务

- 关闭 Windows XP 的防火墙
- 入侵者使用 DameWare 迷你远程控制入侵 Windows XP
- 启用 Windows XP 防火墙
- 入侵者入侵失败

2. 操作步骤

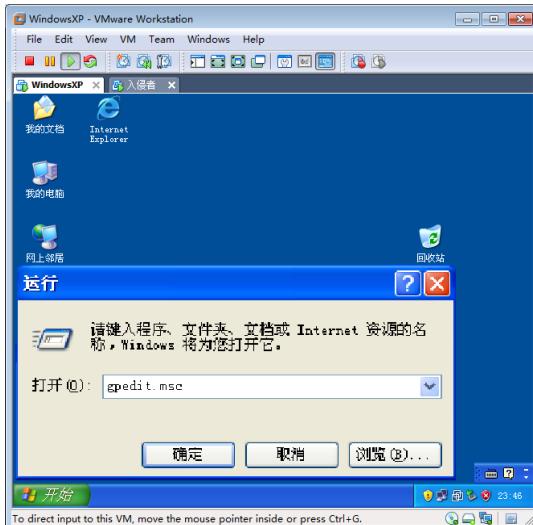
- (1) 在 Windows XP 中，选择“开始”→“设置”→“网络连接”命令。
- (2) 双击“本地连接”，弹出“本地连接状态”对话框，单击“属性”按钮。
- (3) 如图 2-111 所示，在弹出的“本地连接属性”对话框的“高级”选项卡中，单击“设置”按钮。
- (4) 如图 2-112 所示，在弹出的“Windows 防火墙”对话框的“常规”选项卡中，选中“关闭”单选按钮。



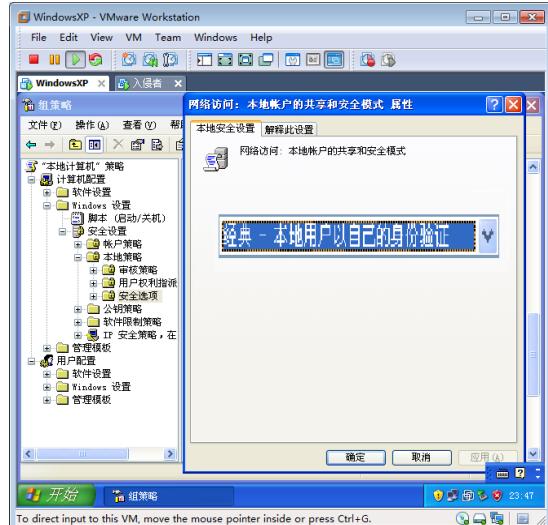
▲图 2-111 “本地连接 属性”对话框

▲图 2-112 “Windows 防火墙”对话框

- (5) 如图 2-113 所示, 选择“开始”→“运行”命令, 在弹出的对话框中输入 gpedit.msc, 单击“确定”按钮。
- (6) 如图 2-114 所示, 打开组策略编辑工具, 展开“计算机配置”\“Windows 设置”\“安全设置”\“本地策略”\“安全选项”节点, 在详细栏, 双击“网络访问: 本地账户的共享和安全模式”, 在出现的对话框中, 选中“经典-本地用户以自己的身份验证”按钮。如果不这样设置, Windows XP 默认只允许 guest 用户访问共享资源。

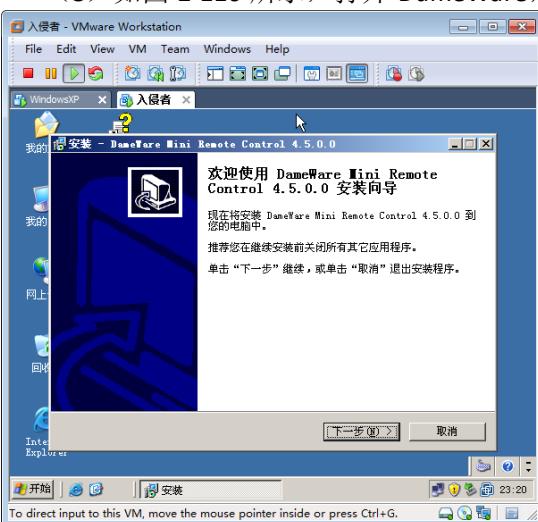


▲图 2-113 “运行”对话框

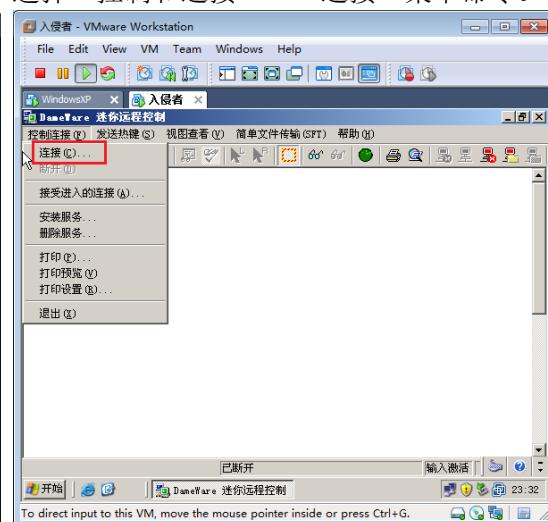


▲图 2-114 配置本地安全设置

- (7) 如图 2-115 所示, 在入侵者的计算机上安装“DameWare 迷你远程控制”软件, 单击“下一步”按钮, 完成安装。
- (8) 如图 2-116 所示, 打开 DameWare, 选择“控制和连接”→“连接”菜单命令。



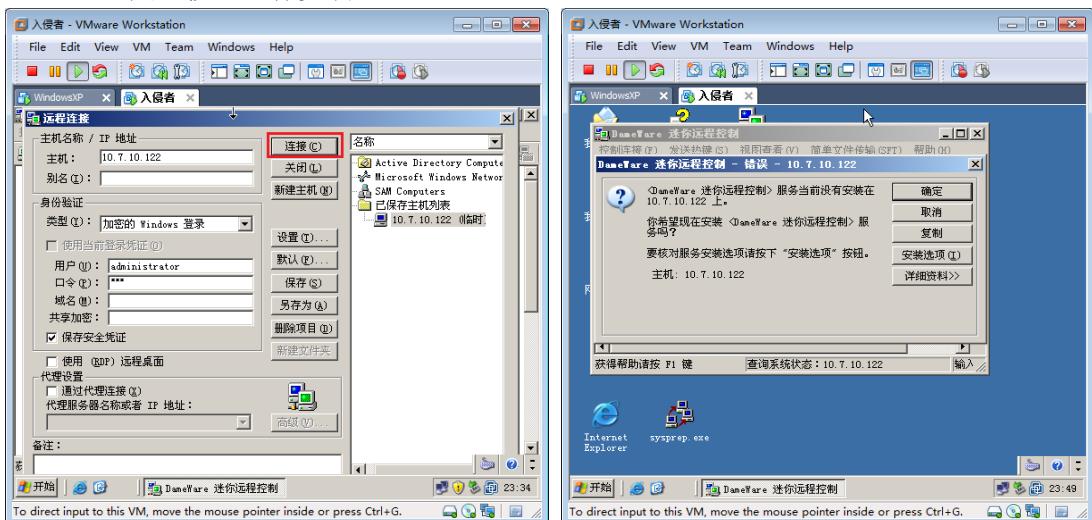
▲图 2-115 安装 DameWare



▲图 2-116 入侵他人计算机

(9) 如图 2-217 所示，在出现的“远程连接”对话框中的“主机”文本框中输入 Windows XP 的地址，在“用户”和“口令”文本框中分别输入连接 Windows XP 的用户和口令，该用户必须是 Windows XP 的 administrators 组的成员。单击“连接”按钮。

(10) 如图 2-218 所示，出现提示对话框，提示在 Windows XP 上没有安装服务。单击“确定”按钮进行安装。

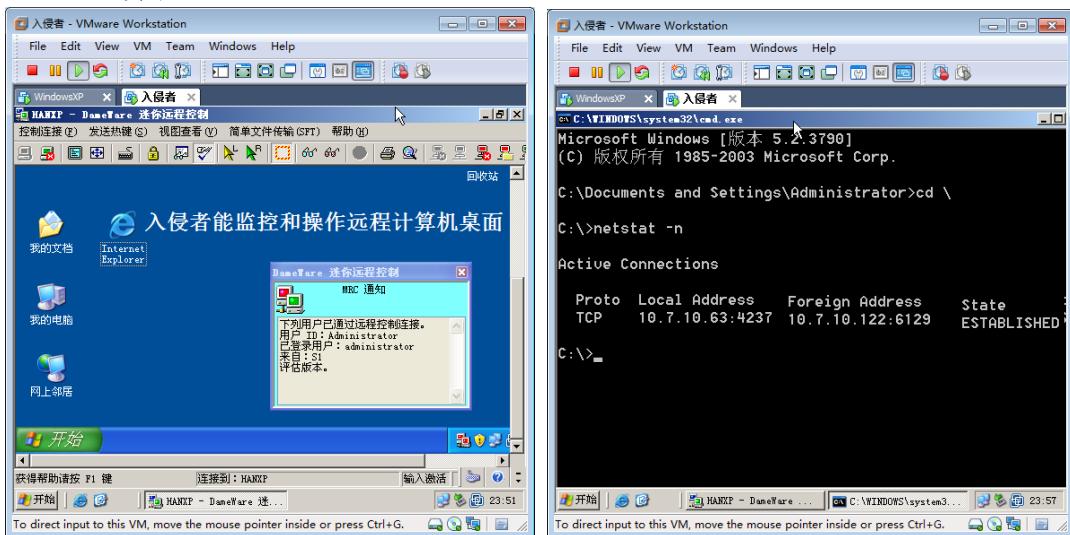


▲图 2-217 连接远程计算机

▲图 2-218 安装被控制端

(11) 如图 2-119 所示，该程序会自动将安装文件拷贝到 Windows XP，并自动安装服务，即可远程监控和操作 Windows XP 了。不过，在桌面上会出现提示，该软件不算是黑客工具。

(12) 如图 2-120 所示，在命令提示符下输入 netstat -n，可以看到远程监控软件建立的会话。



▲图 2-119 入侵成功

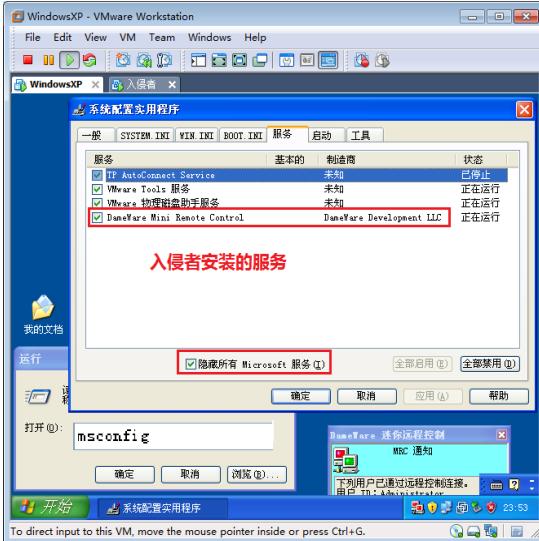
▲图 2-120 查看建立的会话

(13) 在 Windows XP 上，选择“开始”→“运行”命令，在弹出的“运行”对话框中

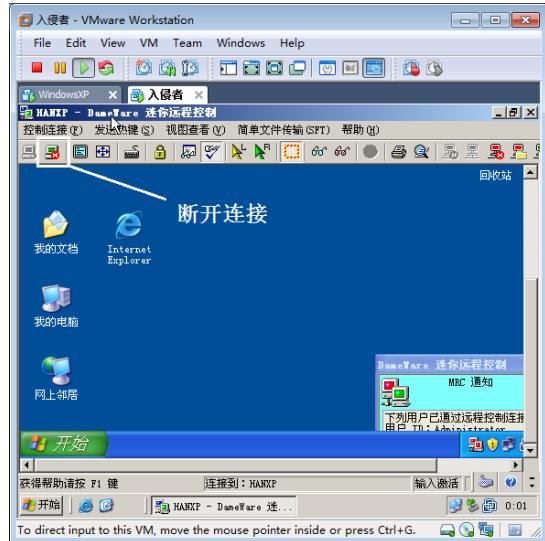
输入 msconfig，单击“确定”按钮。打开“系统配置实用程序”对话框。

(14) 如图 2-121 所示，在“服务”选项卡中，选中“隐藏所有 Microsoft 服务”复选框，可以看到在 Windows XP 上安装的服务。

(15) 如图 2-122 所示，在入侵者计算机上，单击 ，断开 Windows XP 的连接。



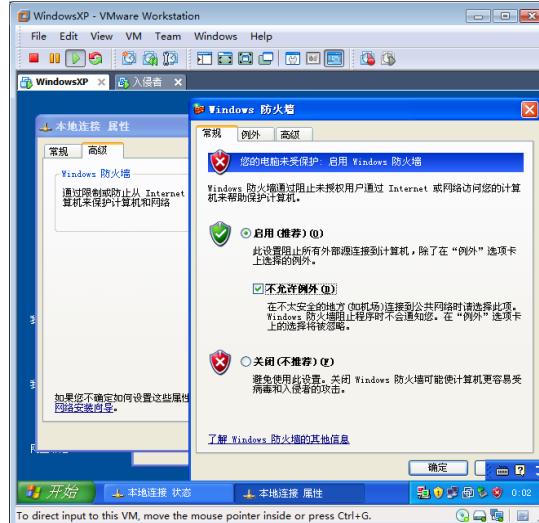
▲图 2-121 安装的服务



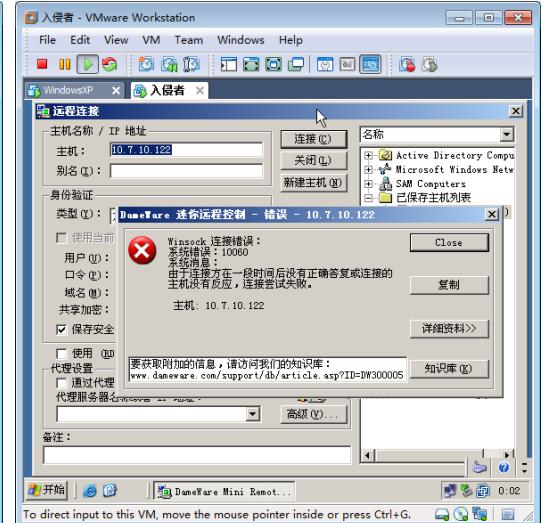
▲图 2-122 断开连接

(16) 如图 2-123 所示，在 Windows XP 上，启用 Windows 防火墙，且选中“不允许例外”复选框，单击“确定”按钮。

(17) 如图 2-124 所示，在入侵者计算机上，再次连接 Windows XP 失败。



▲图 2-123 启用防火墙

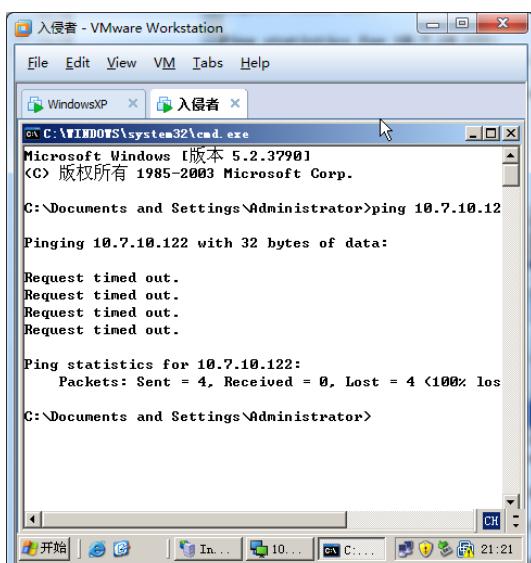


▲图 2-124 入侵失败

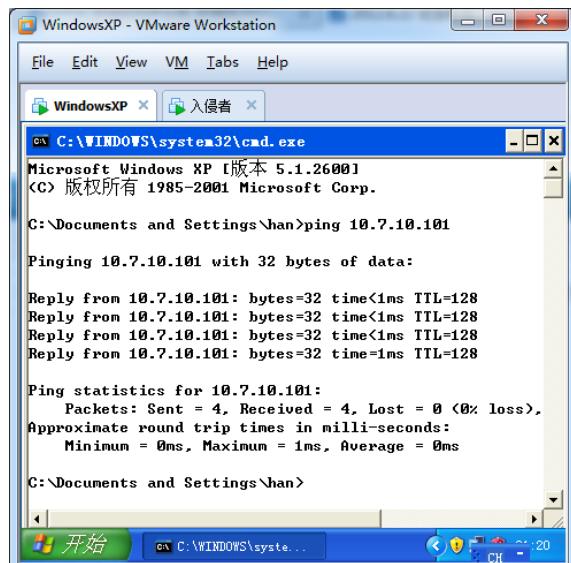
(18) 如图 2-125 所示，在命令提示符下，ping Windows XP 的地址，发现不通。

(19) 如图 2-126 所示，在 Windows XP 上 ping 入侵者计算机的 IP 地址，能够 ping 通。

(20) 这足以证明 Windows 防火墙的作用，能够防止主动的入侵，不拦截出去的流量。



▲图 2-125 不通

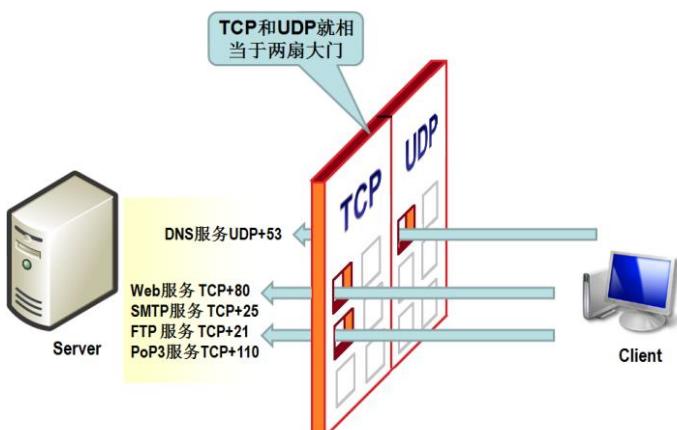


▲图 2-126 通

2.5.4 使用 TCP/IP 筛选保护服务器安全

对于部署在 Internet 的服务器，安全是必须要考虑的事情。为了降低服务器受攻击的危险，停止不必要的服务或在本地连接的 TCP/IP 属性中只打开必要的端口。

如图 2-127 所示，实验环境为 Server 的 IP 地址 192.168.1.200，运行着 Web 服务、SMTP 服务、POP3 服务、FTP 服务和 DNS 服务。Client 的 IP 地址为 192.168.1.121。只允许 Client 计算机访问 Server 计算机的 Web 服务、FTP 服务和 DNS 服务。以下演示配置 Server 计算机的 TCP/IP 筛选只允许 TCP 目标端口为 80 和 21 的数据包进入，以及只允许 UDP 目标端口为 53 的数据包进入。



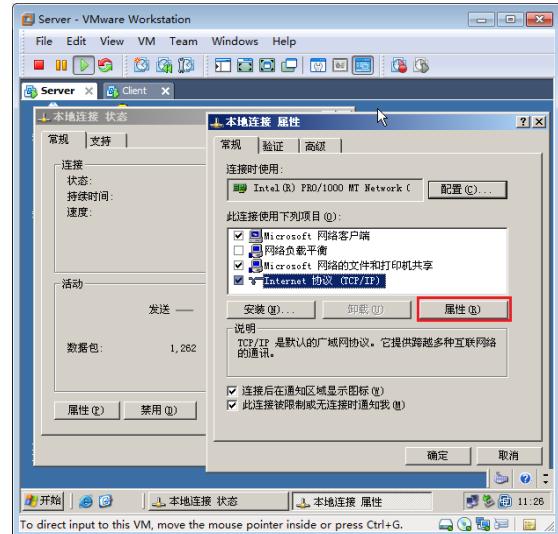
▲图 2-127 TCP/IP 筛选示意图

- (1) 如图 2-128 所示，在 Client 计算机上安装 ScanPort 软件，输入起始地址和结束地址都为 Server 计算机的 IP 地址 192.168.1.200，并输入端口号的范围，单击“扫描”按钮。
- (2) 如图 2-128 所示，可以看到扫描结果。通过扫描结果，可以断定该服务器运行着 FTP 服务、SMTP 服务、DNS 服务、Web 服务和 POP3 服务等。
- (3) 如图 2-129 所示，在 Server 上，打开“本地连接 属性”对话框，选中“Internet

协议（TCP/IP）”复选框，单击“属性”按钮。

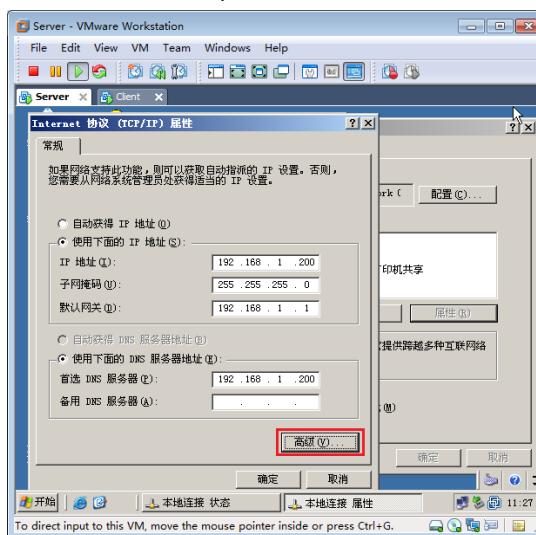


▲图 2-128 端口扫描

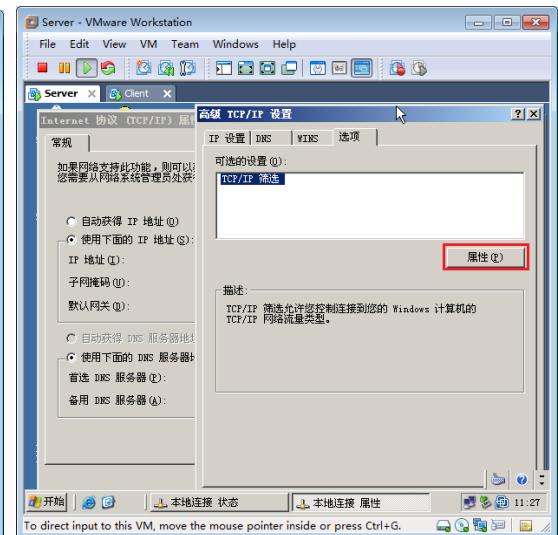


▲图 2-129 “本地连接 属性”对话框

- (4) 如图 2-130 所示，在打开的“Internet 协议（TCP/IP）属性”对话框中，单击“高级”按钮。
- (5) 如图 2-131 所示，在出现的“高级 TCP/IP 设置”对话框的“选项”选项卡中，选中“TCP/IP 筛选”选项，单击“属性”按钮。

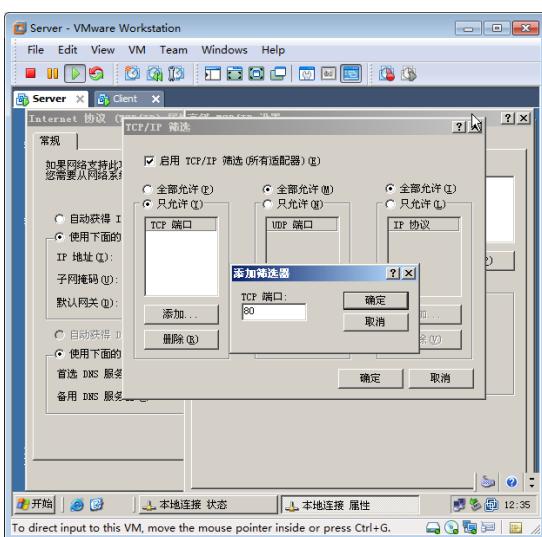


▲图 2-130 “Internet 协议（TCP/IP）属性”对话框

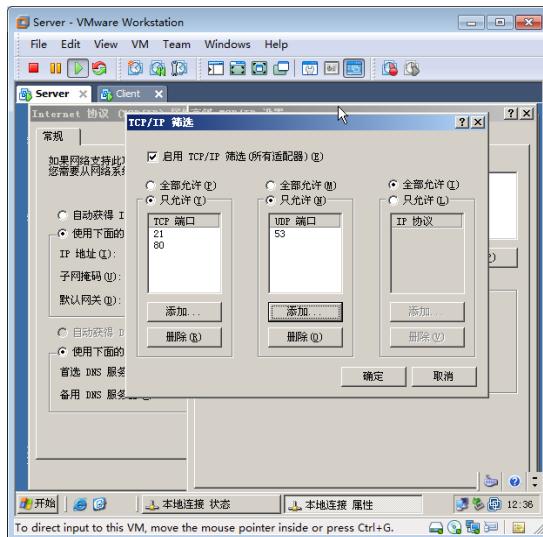


▲图 2-131 “高级 TCP/IP 设置”对话框

- (6) 如图 2-132 所示，在出现的“TCP/IP 筛选”对话框中，选中“启用 TCP/IP 筛选”复选框，TCP 端口选中“只允许”单选按钮，单击“添加”按钮。
- (7) 如图 2-132 所示，在出现的“添加筛选器”对话框中，输入 80，单击“确定”按钮。
- (8) 如图 2-133 所示，同样添加 TCP 的 21 端口。
- (9) 如图 2-133 所示，UDP 端口选中“只允许”单选按钮，添加端口 53，单击“确定”按钮。

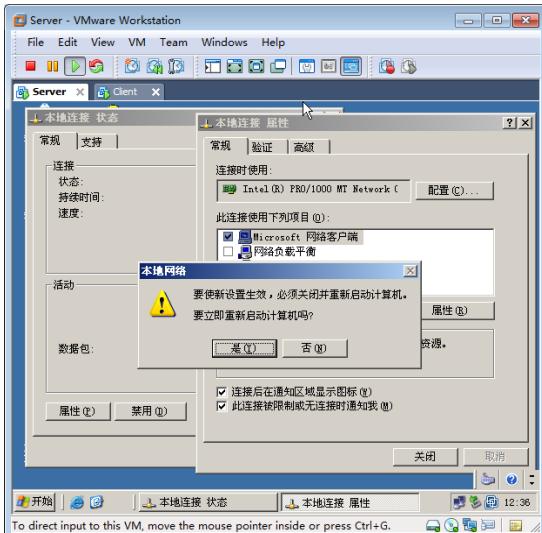


▲图 2-132 添加允许的 TCP 端口

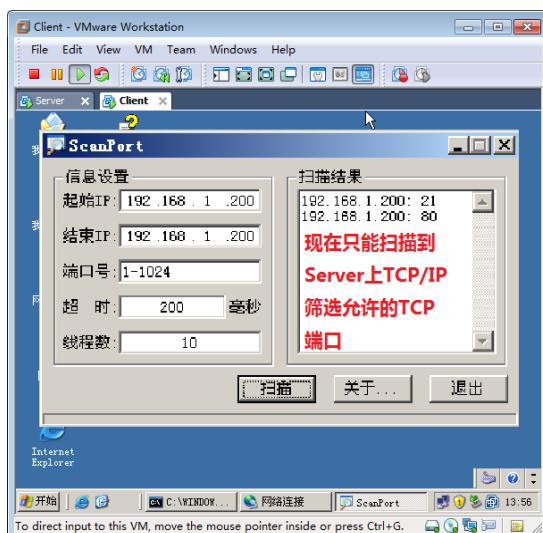


▲图 2-133 添加允许的 UDP 端口

- (10) 如图 2-134 所示, 提示需要重启计算机, 单击“是”按钮, 重启计算机。
- (11) 如图 2-135 所示, 在 Client 上, 发现只能扫描到 21 和 80 端口, 端口扫描只是扫描 TCP 的端口, 不扫描 UDP 端口。这样 Client 计算机只能访问 Server FTP 服务和 Web 服务。

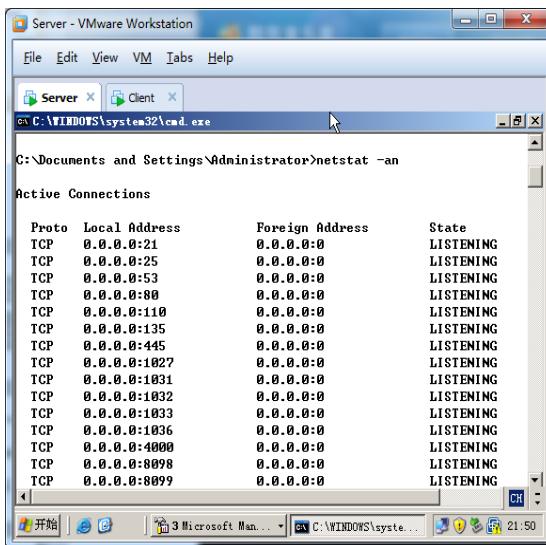


▲图 2-134 需要重启计算机

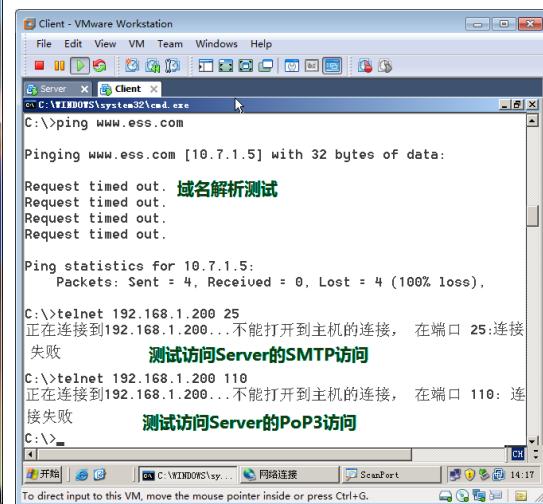


▲图 2-135 扫描端口

- (12) 如图 2-136 所示, 在 Server 上, 在命令提示符下输入 netstat -an 查看侦听的端口。可以看到该服务器在 TCP 的 25、110 端口侦听。这说明 TCP/IP 筛选并不控制服务器侦听的端口。
- (13) 如图 2-137 所示, 在 Client 上, 运行 ping www.ess.com, 可以看到 Client 计算机可以通过 Server 进行域名解析。
- (14) 如图 2-137 所示, telnet Server 的 25 端口和 110 端口失败。说明 TCP/IP 筛选没有允许这些端口。



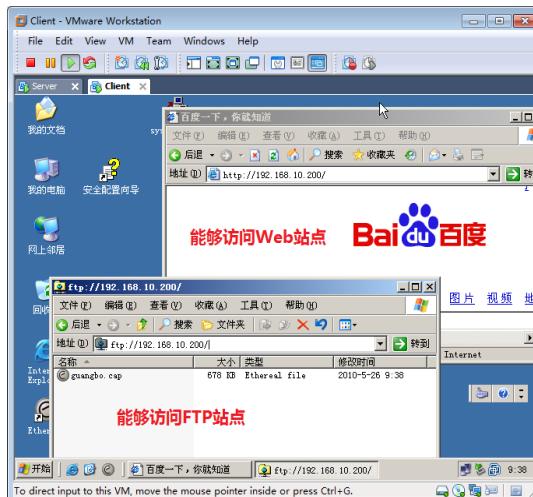
▲图 2-136 查看侦听的端口



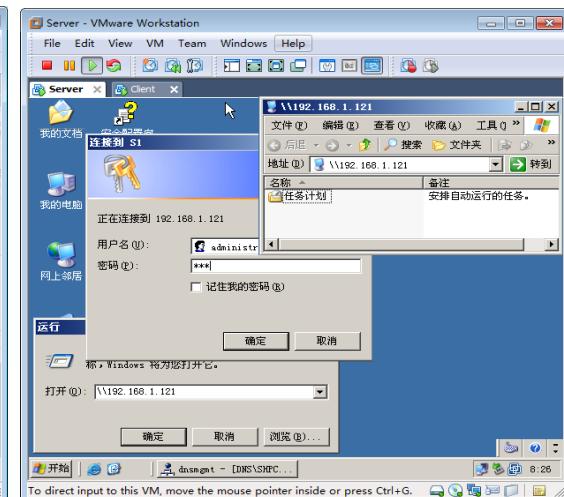
▲图 2-137 测试域名解析

(15) 如图 2-138 所示，在 Client 上可以访问 Server 的 Web 服务，也能够访问 FTP 服务。

(16) 如图 2-139 所示，在 Server 上访问 Client 计算机的共享文件夹，输入 Client 计算机的用户名和密码，能够访问成功。



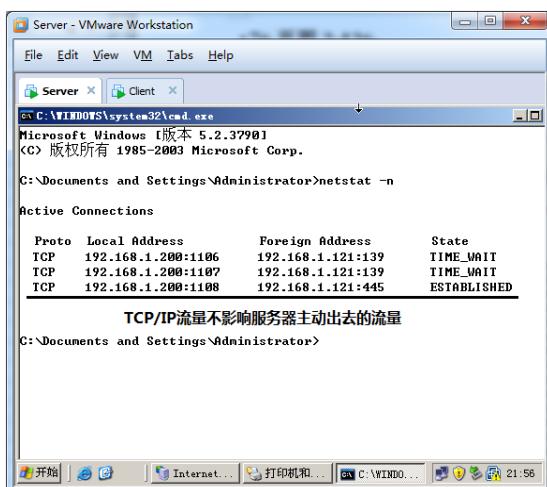
▲图 2-138 能够访问 Web 和 FTP 站点



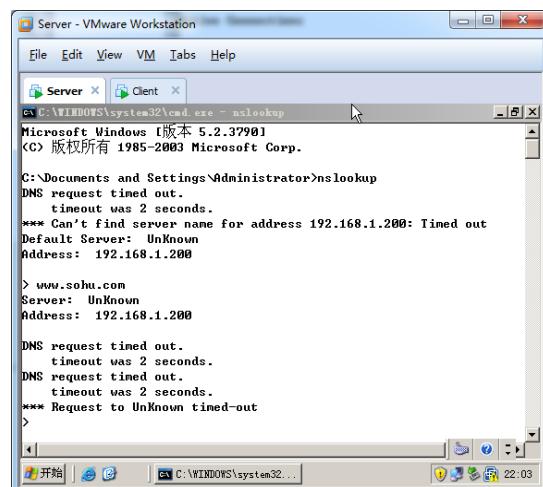
▲图 2-139 TCP/IP 筛选不影响出去的流量

(17) 如图 2-140 所示，在命令提示符下输入 netstat -n，可以看到建立的会话，说明 TCP/IP 筛选并不控制出去的流量。

(18) 如图 2-141 所示，在 Server 上 ping www.sohu.com，发现不能域名解析，输入 nslookup 后，输入 www.sohu.com，可以看到解析失败。为什么 Server 不能将域名解析呢？



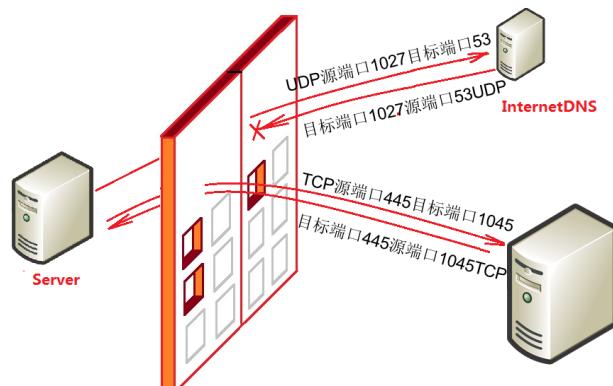
▲图 2-140 查看建立的会话



▲图 2-141 域名解析

Server 为什么不能解析 Internet DNS 服务器的域名？举例说明：Server 向 Internet DNS 发送域名解析的请求，协议是 UDP，目标端口为 53，源端口为 1027，当数据包发出去后，由于 UDP 不建立会话，发出去的数据包或请求就忘记了，在域名解析结果返回来的时候，由于 TCP/IP 筛选 UDP 只打开了 53 端口，而没有打开 1027 端口，因此被 TCP/IP 筛选拦截。因此域名解析失败。

为什么 Server 的 TCP/IP 筛选访问 Client 的共享文件夹？举例说明：如图 2-142 所示，Server 访问 Client 的共享文件夹，Server 向 Client 发送访问共享文件夹的请求数据包，使用 TCP 协议，目标端口为 445，源端口为 1045，因为 TCP 是建立会话的，所以 Server 会临时打开端口 1045，这样 Client 返回的数据包，能够进入 Server。



▲图 2-142 UDP 不建立会话

2.5.5 使用 IPSec 保护服务器安全

不管是在 Windows XP 上启用防火墙还是 Windows Server 上配置 TCP/IP 筛选，都不能严格控制出去的流量。因此如果你的服务器中了木马程序（比如中了灰鸽子木马程序），该程序会主动连接入侵者建立会话，入侵者就能监控和控制你的服务器了。

最大化配置服务器网络安全，你可以严格控制进出服务器的流量，比如你的服务器是 Web 服务器，你可以配置只允许 TCP 目标端口 80 的数据包进入服务器，TCP 源端口为 80 的数据包离开服务器。这样即便你的服务器中了灰鸽子木马程序，也不能主动连接入侵者。这种控制方式可以通过配置服务器 IPSec 来实现，Windows XP, Windows Server 2003 和 Windows Server 2008 都支持 IPSec。

下面就以通过 IPSec 配置 Web 服务器安全，防止灰鸽子木马程序为例。演示入侵者制作木马程序，在 Server 上启用 Windows 防火墙，安装木马程序，在入侵者远程控制服务器。配置 IPSec，如图 2-143 所示，只允许 TCP 的目标端口为 80 数据包进入服务器，只允许 TCP 的源端口为 80 的数据包离开服务器。验证木马程序不能连接到入侵者。

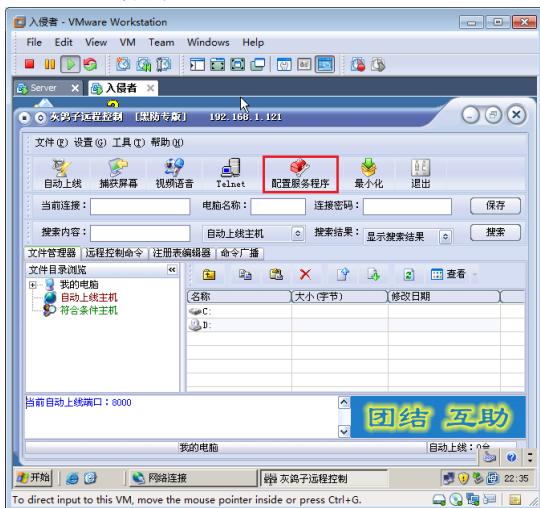
入侵者的 IP 地址为 192.168.1.121，服务器 Server 的 IP 地址为 192.168.1.200。

1. 制作木马程序

灰鸽子木马程序，可以在 <http://down.51cto.com/> 搜索“灰鸽子”，可以找到并下载。

中了灰鸽子木马程序，会主动连接到入侵者，入侵者就可以远程监控和操控中了木马的服务器。这就要求木马程序能够连接到入侵者，因此生成的木马程序必须指定入侵者的 IP 地址。

- (1) 如图 2-144 所示，在入侵者的计算机上安装并运行灰鸽子木马程序，单击“配置服务程序”按钮。提示木马程序在中了招的计算机上是以服务的方式存在的。
- (2) 如图 2-145 所示，在出现的“服务器配置”对话框的“自动上线设置”中输入入侵者的 IP 地址。



▲图 2-144 运行灰鸽子木马程序



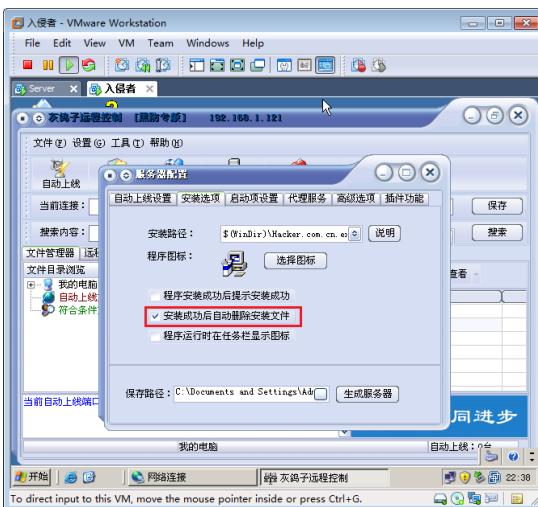
▲图 2-145 “服务器配置”对话框

- (3) 如图 2-146 所示，在“安装选项”选项卡中，选中“安装成功后自动删除安装文件”复选框。木马程序一般都是在后台偷偷运行的，取消选中“程序安装成功后提示安装成功”和“程序运行时在任务栏显示图标”复选框。
- (4) 如图 2-147 所示，在“启动设置”选项卡中，选中“Win2000/XP 下优先安装成服务启动”复选框，然后单击“生成服务器”按钮，这样就制作好了木马程序。

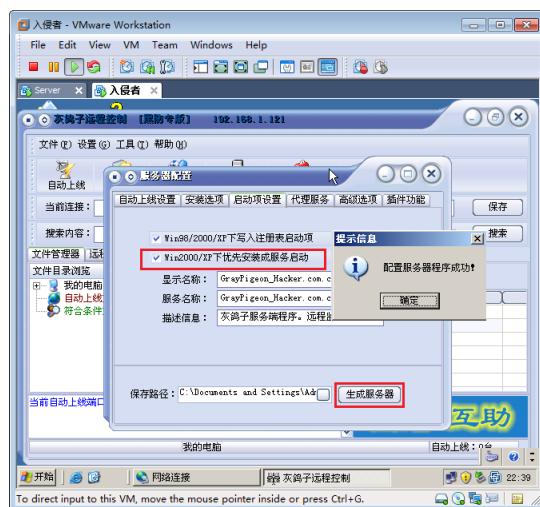
IPSec控制进出流量



▲图 2-143 访问 Web 服务器的流量



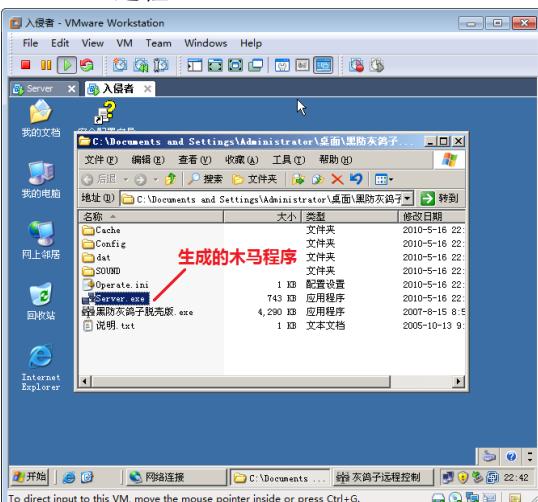
▲图 2-146 “安装选项”选项卡



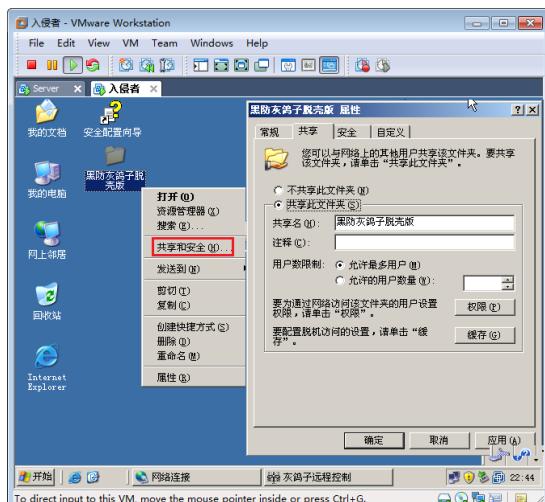
▲图 2-147 “服务器配置”对话框

(5) 如图 2-148 所示，可以看到生成的木马程序“Server.exe”。

(6) 如图 2-149 所示，将有木马程序的文件夹共享。以方便 Server 访问，模拟中木马的过程。



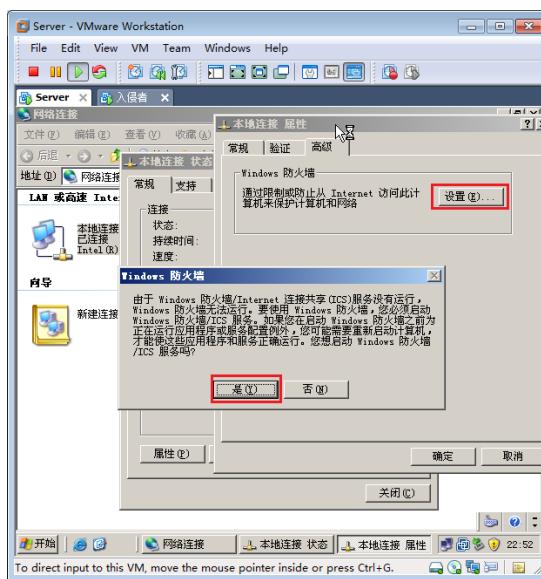
▲图 2-148 生成的木马程序



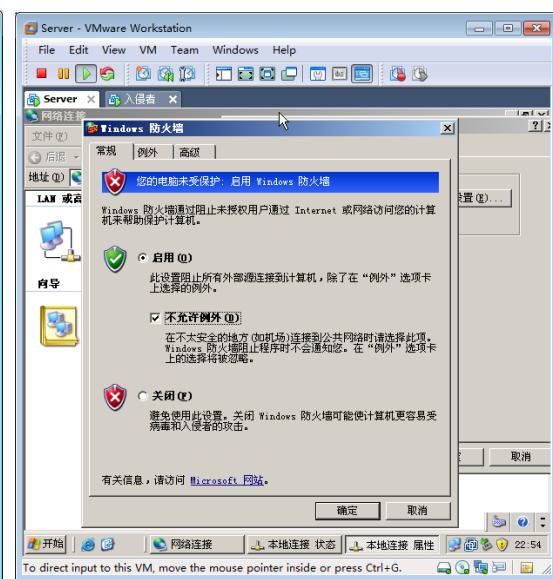
▲图 2-149 共享存放木马的文件夹

2. 中木马的过程

- (1) 如图 2-150 所示，在 Server 上，打开“本地连接 属性”对话框，单击“设置”按钮，在出现的“Windows 防火墙”提示对话框中，单击“是”按钮，启用 Windows 防火墙服务。
- (2) 如图 2-151 所示，在出现的“Windows 防火墙”对话框的“常规”选项卡中，选中“启用”单选按钮和“不允许例外”复选框。



▲图 2-150 “本地连接 属性”对话框

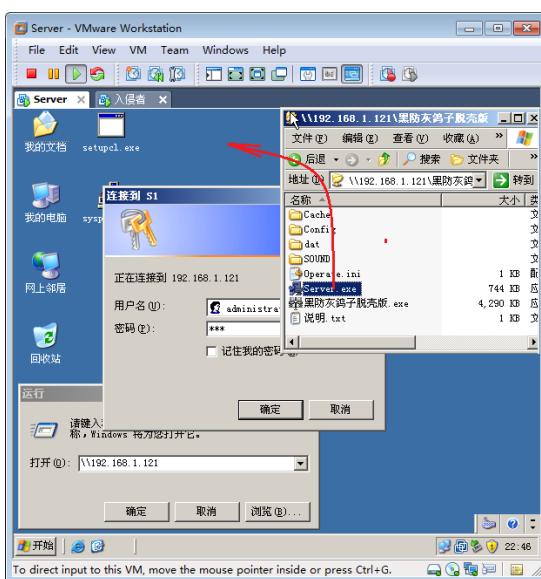


▲图 2-151 “Windows 防火墙”对话框

- (3) 如图 2-152 所示, 可以看到本地连接启用了 Windows 防火墙的图标, 加了一把锁。
- (4) 如图 2-153 所示, 在 Server 上访问入侵者的共享文件夹, 将木马程序拷贝到桌面, 双击, 安装木马程序。



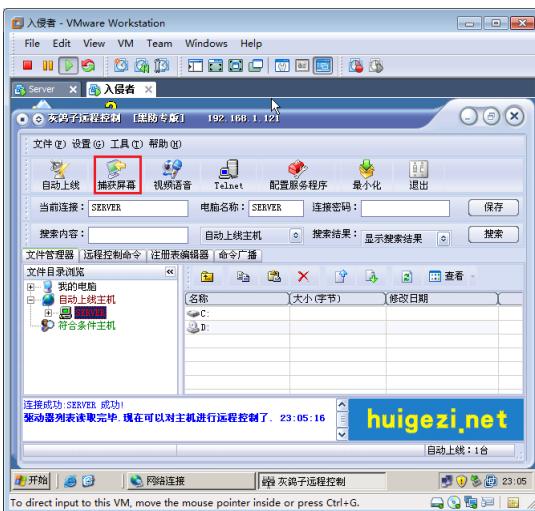
▲图 2-152 启用 Windows 防火墙



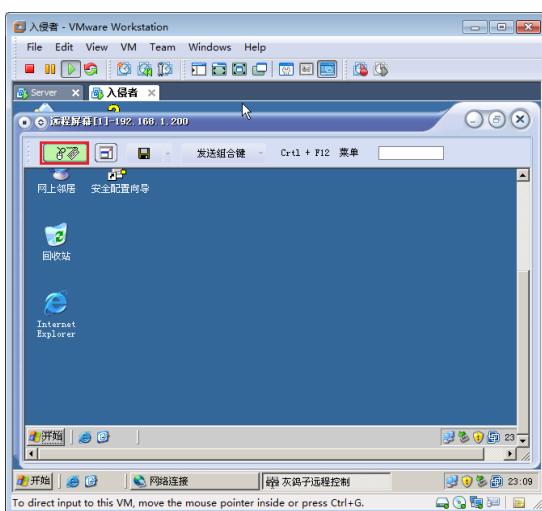
▲图 2-153 将木马拷贝到本地并安装

3. 远程监控和控制

- (1) 如图 2-154 所示, 在入侵者计算机上, 可以看到中了木马的计算机自动上线, 选中上线的服务器, 单击“捕获屏幕”按钮。可以远程监控 Server 桌面。
- (2) 如图 2-155 所示, 单击图中框起的鼠标和键盘图标, 还可以控制远程计算机。

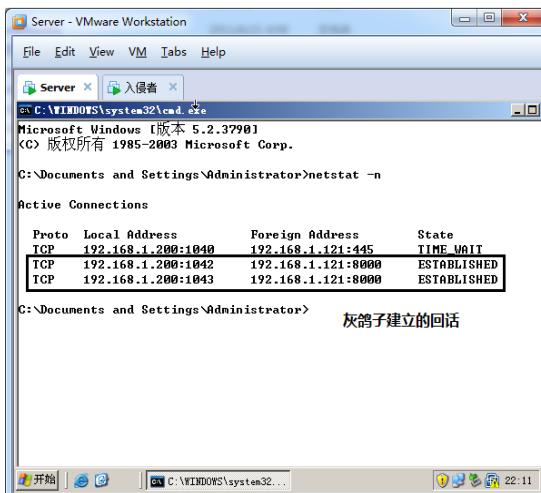


▲图 2-154 捕获屏幕

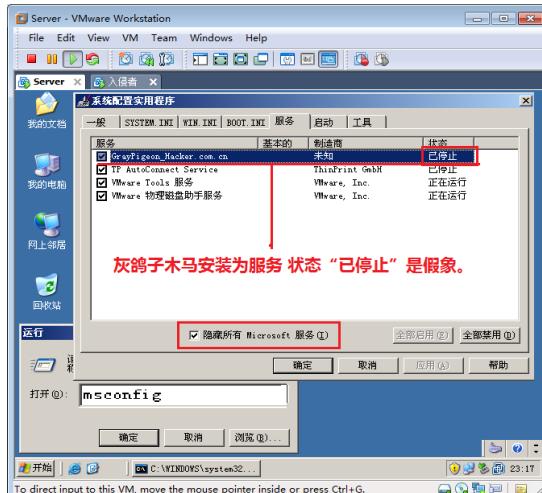


▲图 2-155 远程控制

- (3) 如图 2-156 所示, 在 Server 上的命令提示符下输入 netstat -n, 可以看到木马建立的会话。
- (4) 如图 2-157 所示, 在 Server 上, 运行 msconfig, 打开“系统配置实用程序”对话框, 选中“隐藏所有 Microsoft 服务”复选框, 可以看到灰鸽子木马安装的服务。



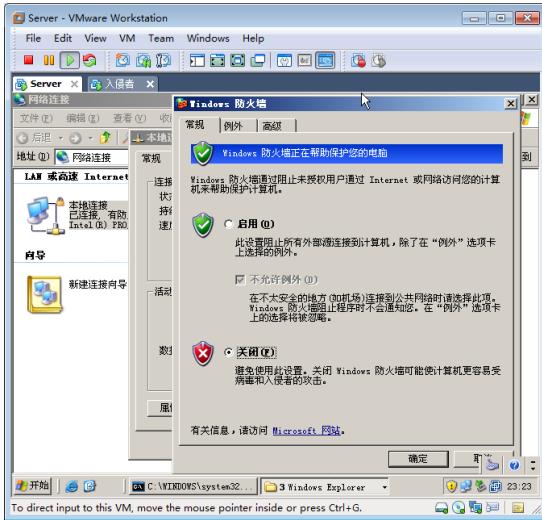
▲图 2-156 灰鸽子建立的会话



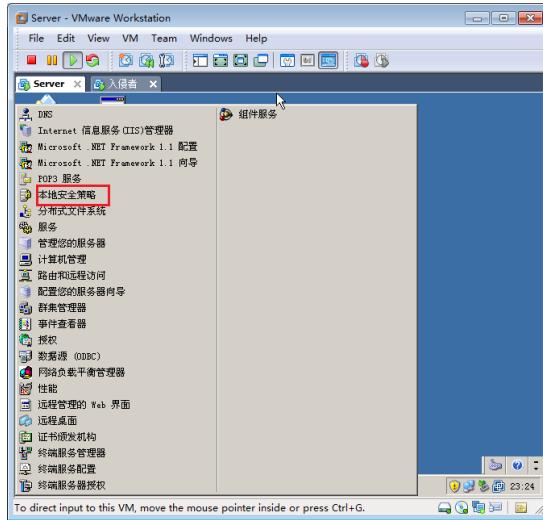
▲图 2-157 安装的灰鸽子木马

4. 配置 IPSec 保护 Web 服务器

- (1) 如图 2-158 所示, 在 Server 上禁用 Windows 防火墙。现在使用 IPSec 严格控制出入流量。
- (2) 如图 2-159 所示, 选择“开始”→“程序”→“管理工具”→“本地安全策略”命令。

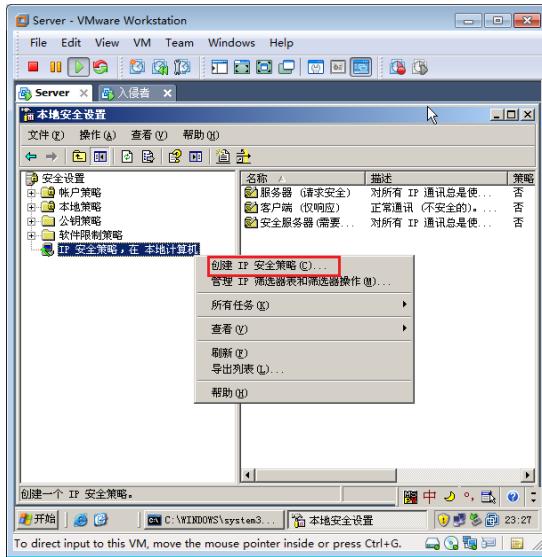


▲图 2-158 关闭 Windows 防火墙

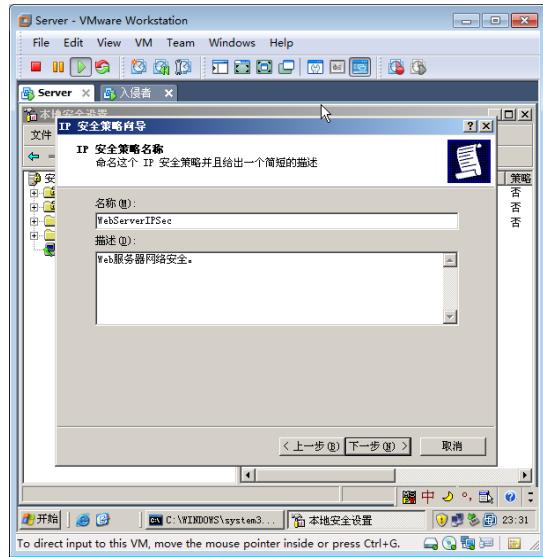


▲图 2-159 选择“本地安全策略”命令

- (3) 如图 2-160 所示，在打开的“本地安全设置”窗口中，右击“IP 安全策略”，在本地计算机”节点，在弹出的快捷菜单中选择“创建 IP 安全策略”命令。
- (4) 在出现的“欢迎使用 IP 安全策略向导”对话框中，单击“下一步”按钮。
- (5) 如图 2-161 所示，在出现的“IP 安全策略名称”设置界面中，输入名称和描述信息，单击“下一步”按钮。

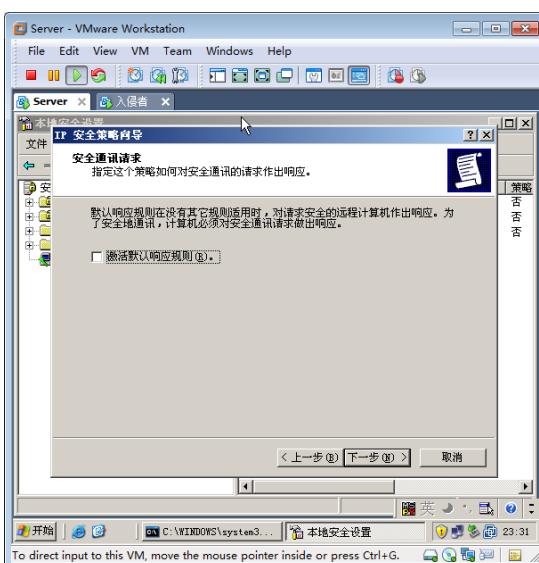


▲图 2-160 “本地安全设置”窗口

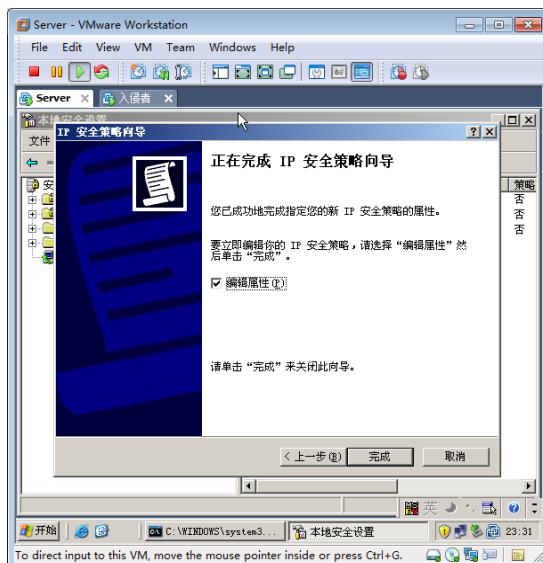


▲图 2-161 “IP 安全策略名称”设置界面

- (6) 如图 2-162 所示，在出现的“安全通讯请求”设置界面中，取消选中“激活默认响应规则”复选框，单击“下一步”按钮。
- (7) 如图 2-163 所示，在出现的“正在完成 IP 安全策略向导”设置界面中，单击“完成”按钮。

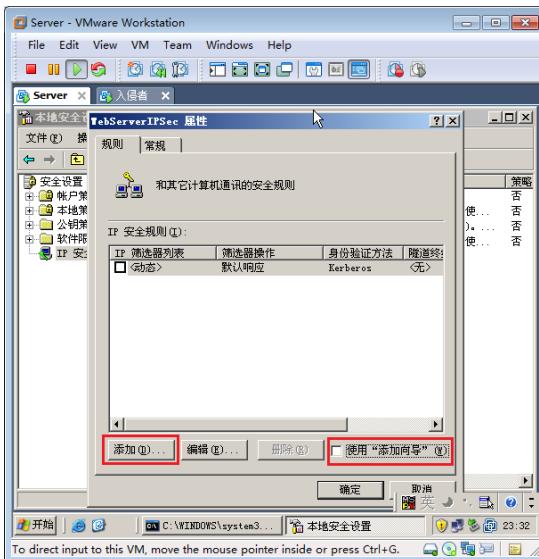


▲图 2-162 “安全通讯请求”设置界面

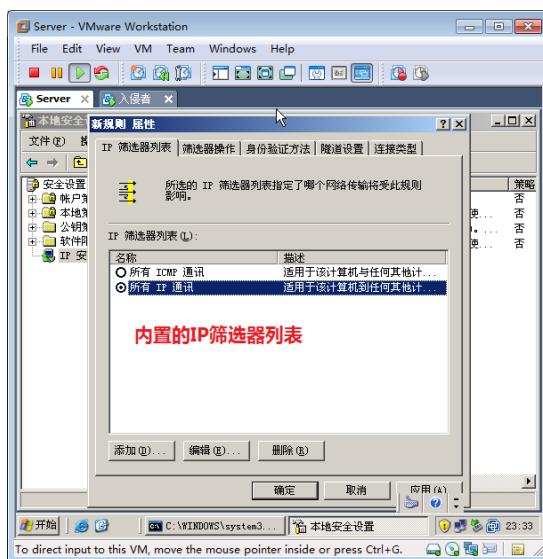


▲图 2-163 “正在完成 IP 安全策略向导”设置界面

- (8) 如图 2-164 所示，在出现的“WebServerIPSec 属性”对话框中，取消选中“使用‘添加向导’”复选框，单击“添加”按钮。
- (9) 如图 2-165 所示，在出现的“新规则 属性”对话框中，选中“所有 IP 通讯”单选按钮，单击“筛选器操作”标签。

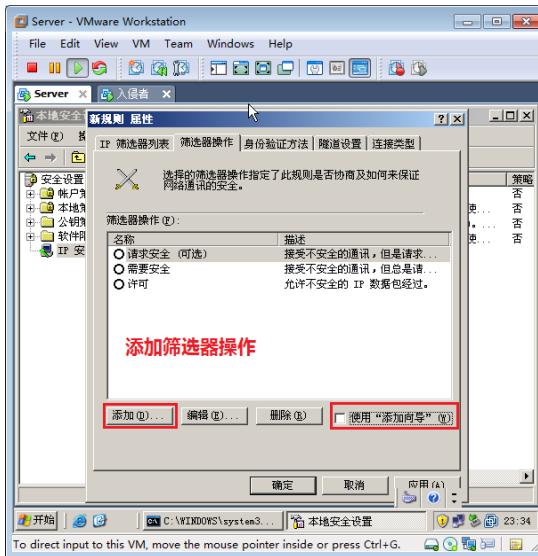


▲图 2-164 “WebServerIPSec 属性”对话框

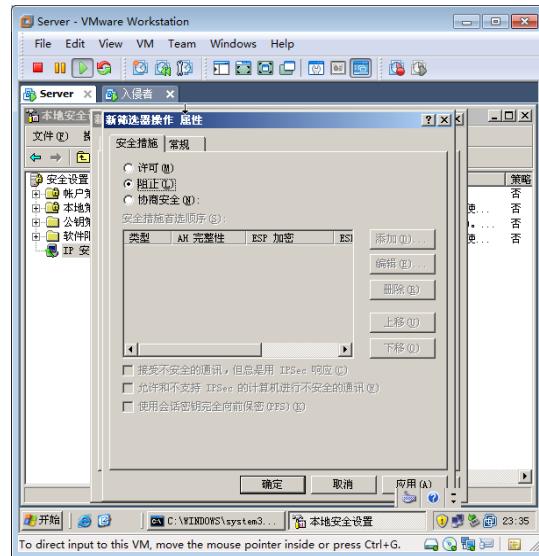


▲图 2-165 “新规则 属性”对话框

- (10) 如图 2-166 所示，在“筛选器操作”选项卡中，没有拒绝的动作，取消选中“使用‘添加向导’”复选框，单击“添加”按钮。
- (11) 如图 2-167 所示，在出现的“新筛选器操作 属性”对话框的“安全措施”选项卡中，选中“阻止”单选按钮，单击“常规”标签。

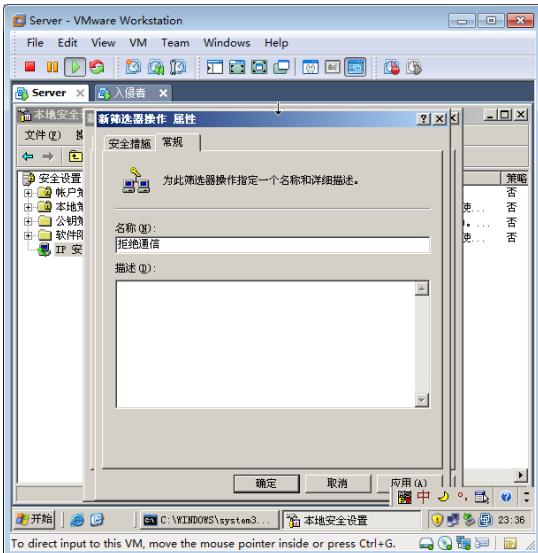


▲图 2-166 添加筛选器的操作

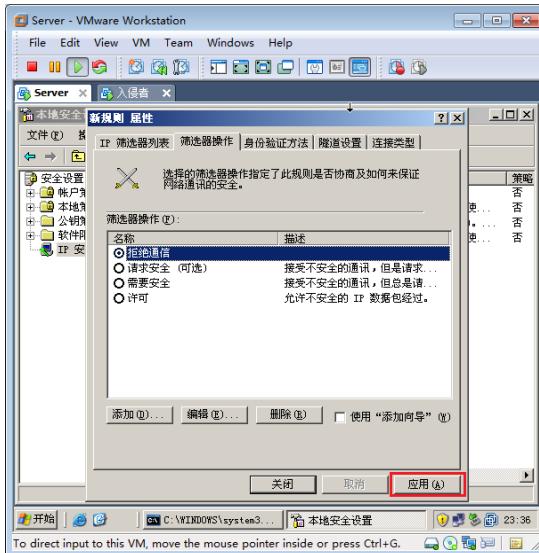


▲图 2-167 选择阻止

- (12) 如图 2-168 所示, 在“常规”选项卡中, 输入名称, 单击“确定”按钮。
 (13) 如图 2-169 所示, 在“新规则 属性”对话框中, 选择刚刚创建的操作“拒绝通信”, 单击“应用”按钮。

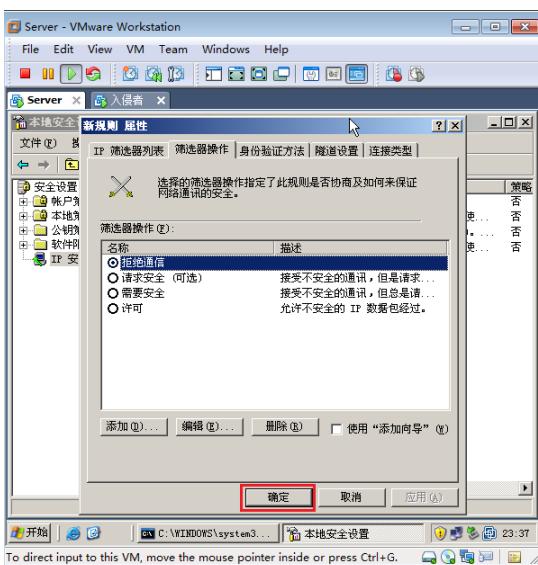


▲图 2-168 指定操作名称

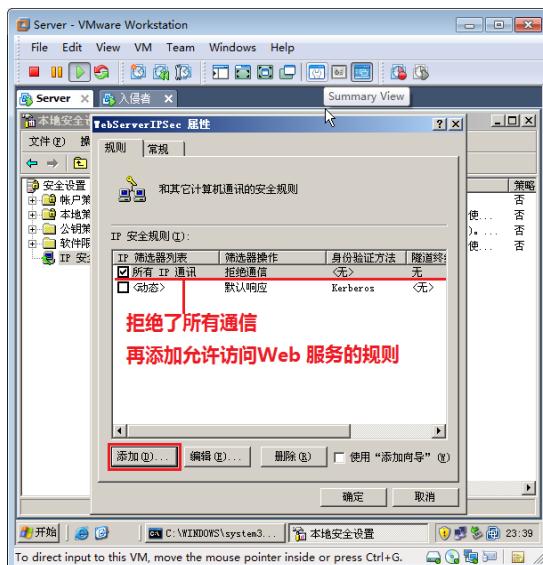


▲图 2-169 选择操作

- (14) 如图 2-170 所示, 单击“确定”按钮。
 (15) 如图 2-171 所示, 这样就添加了拒绝所有通信, 相当于拔了网线。然后添加规则允许访问 Web 站点的流量出入。



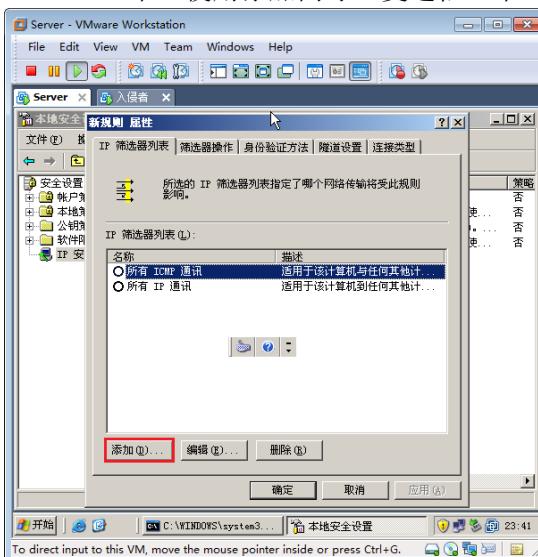
▲图 2-170 完成添加规则



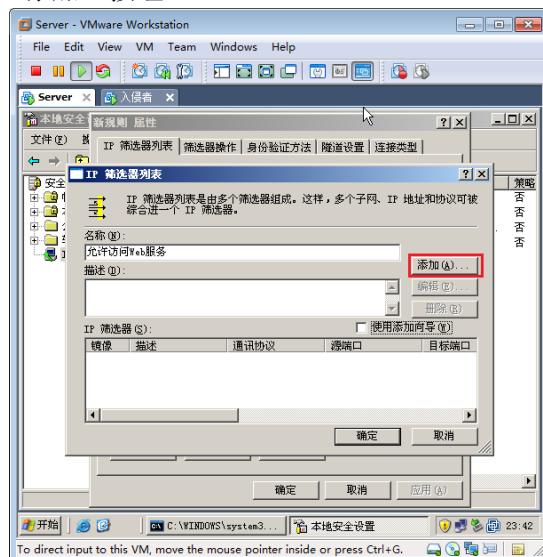
▲图 2-171 添加允许访问 Web 服务的规则

(16) 如图 2-172 所示, 在“新规则 属性”对话框中, 单击“添加”按钮。

(17) 如图 2-173 所示, 在出现的“IP 筛选器列表”对话框中, 输入规则名称, 取消选中“使用添加向导”复选框, 单击“添加”按钮。



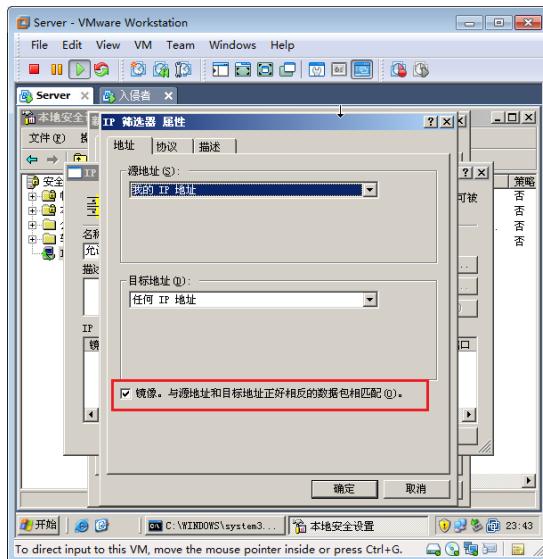
▲图 2-172 添加筛选器列表



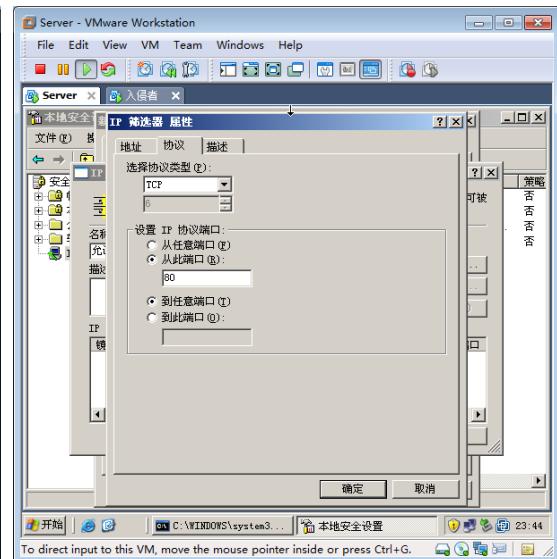
▲图 2-173 添加筛选器

(18) 如图 2-174 所示, 在出现的“IP 筛选器 属性”对话框中, 可以看到源地址和目标地址, 一定要选中“镜像, 与源地址和目标地址正好相反的数据包相匹配”复选框。

(19) 如图 2-175 所示, 在“协议”选项卡中, 协议选择 TCP, “设置 IP 协议端口”选项组中, 选中“从此端口”和“到任意端口”单选按钮, 单击“确定”按钮。

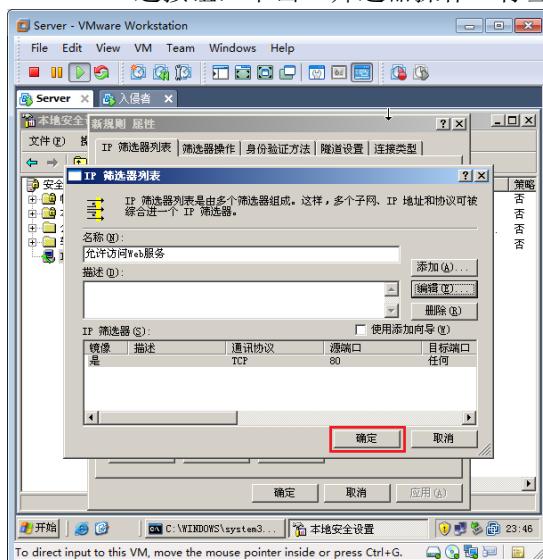


▲图 2-174 配置筛选器

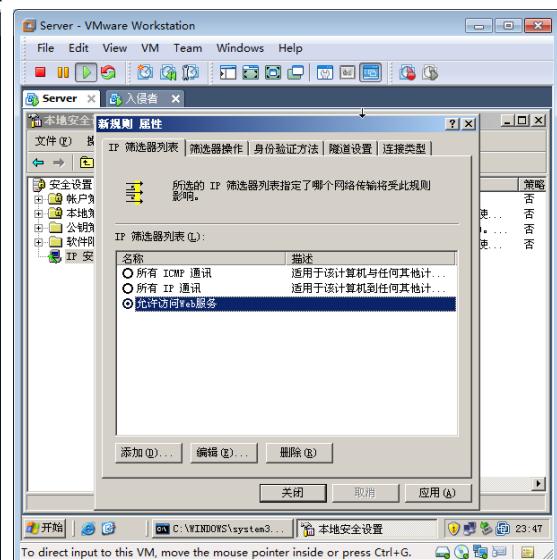


▲图 2-175 指定协议和端口

- (20) 如图 2-176 所示，单击“确定”按钮。当然，如果还希望别人访问 FTP 站点，你还可以继续单击“添加”按钮，添加相应的筛选器。筛选器列表中可以包括多个筛选器。
- (21) 如图 2-177 所示，在“新规则属性”对话框中，选中“允许访问 Web 服务”单选按钮，单击“筛选器操作”标签。

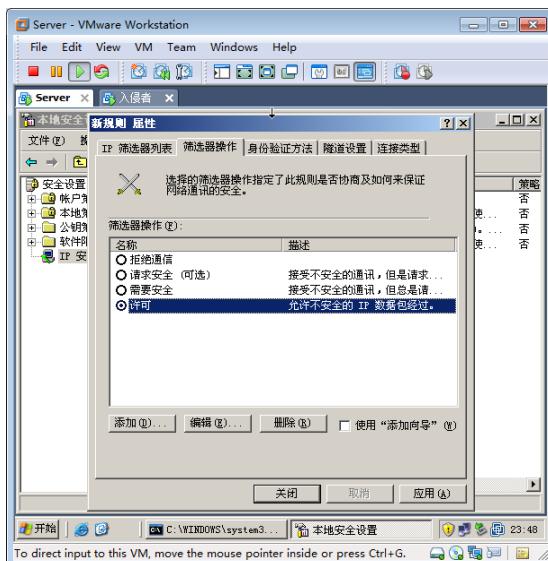


▲图 2-176 完成筛选器列表

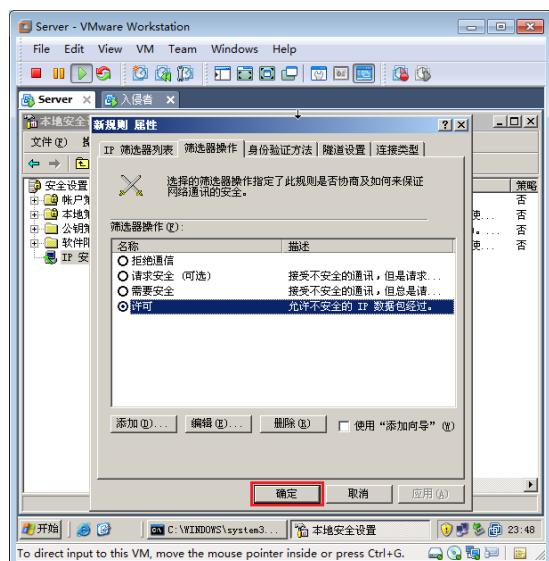


▲图 2-177 选择筛选器规则

- (22) 如图 2-178 所示，在“筛选器操作”选项卡中，选中“许可”单选按钮，单击“应用”按钮。
- (23) 如图 2-179 所示，单击“确定”按钮。

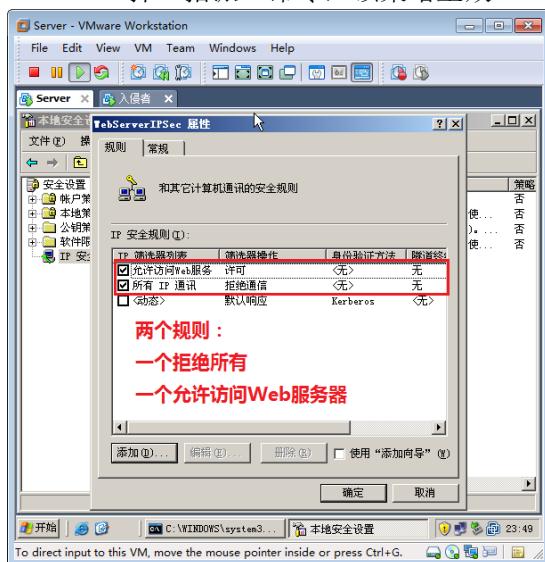


▲图 2-178 “筛选器操作”选项卡

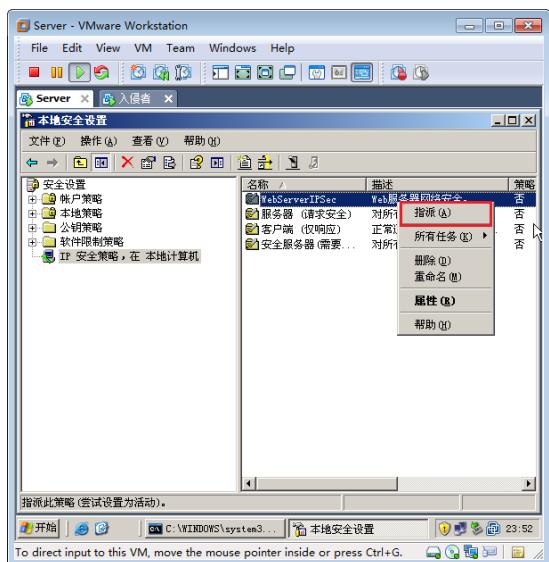


▲图 2-179 单击“确定”按钮

- (24) 如图 2-180 所示, 到目前为止已经创建了两个规则, 一个是拒绝所有通信, 一个 是允许访问 Web 服务器的流量, 多个规则以最佳匹配为准。也就意味着不是访问 Web 站点的流量就应用所有 IP 通信的规则。
- (25) 如图 2-181 所示, 右击刚才创建的 WebServerIPSec 策略, 在弹出的快捷菜单中选择“指派”命令, 该策略生效。



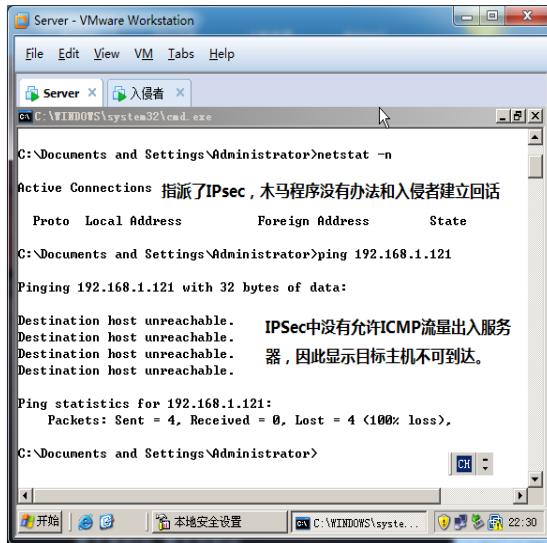
▲图 2-180 创建的两个规则



▲图 2-181 指派 IP 策略

- (26) 如图 2-182 所示, 在 Server 上运行 netstat -n 命令, 可以看到木马程序不能和入侵者的计算机建立会话, 这样木马就成了“卧槽马”, 不会为你的 Server 造成多大危害。
- (27) 如图 2-182 所示, ping 入侵者的 IP 地址, 出现 Destination host unreachable。因为 IPSec 没有允许此类通信出入。

(28) 如图 2-183 所示，在入侵者计算机上，你也看不到自动上线的主机，就没办法监控和控制中了木马的服务器。



▲图 2-182 查看会话测试网络

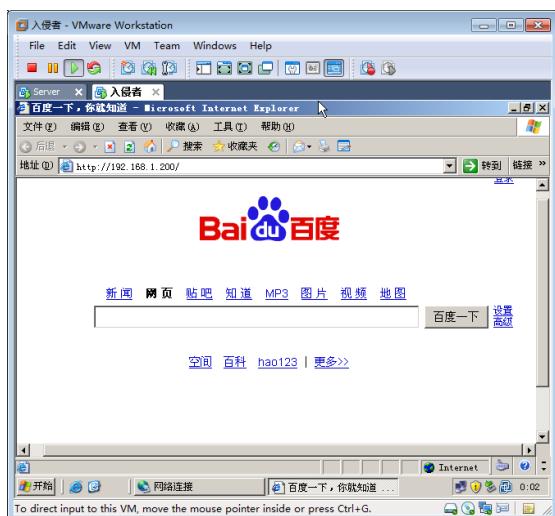
(29) 如图 2-184 所示，可以看到，在入侵者计算机访问 Server 的 Web 站点还是可以的。

结论

Windows 防火墙能够禁止主动入侵，但是对木马没有防护作用。Windows 的 TCP/IP 筛选和 Windows 防火墙类似，能够禁止主动入侵，但是对木马没有防护作用。要想使用严格控制出入服务器的流量策略，可以使用 IPSec 实现。



▲图 2-183 灰鸽子不能上线了



▲图 2-184 能够访问 Web 站点

2. 6 网络层协议

在 TCP/IP 协议栈中网络层有四个协议 IP、IGMP、ICMP 和 ARP 协议。

在下面的小节中，我们将描述在因特网层上的协议：

- 因特网协议（IP）
- 因特网控制报文协议（ICMP）
- 地址解析协议（ARP）

- 逆向地址解析协议 (RARP)
- 代理 ARP

下面逐一介绍各个协议的功能。

2.6.1 IP协议

1. IP协议

IP是英文Internet Protocol（网络之间互联的协议）的缩写，也就是为计算机网络相互连接进行通信而设计的协议。在因特网中，它是能使连接到网上的所有计算机网络实现相互通信的一套规则，规定了计算机在因特网上进行通信时应当遵守的规则。任何厂家生产的计算机系统，只要遵守IP协议就可以与因特网互连互通。

因特网协议(IP)其实质就是因特网层，如图2-185所示。其他的协议仅仅是建立在其基础之上用于支持IP协议的。相互通信的计算机和网络设备必须统一规划网络层地址，即IP地址。IP关注每个数据包的地址，网络层设备通过使用路由表，IP可以决定一个数据包将发送给哪一个被选择好的后续最佳路径，那些动态路由协议(RIP、EIGRP和OSPF协议都是IP协议)。处于DoD模型底部的网络接口层协议不会关心IP在整个网络上的工作，它们只处理(本地网络的)物理链接。

如图2-186所示，网络为三个网段 $10.0.0.0/8$ 、 $11.0.0.0/8$ 和 $12.0.0.0/8$ ，计算机A的MAC地址为M1，IP地址为10.0.0.2，网关为10.0.0.1，路由器Router1连接交换机SW1的接口的MAC地址为M2，其他路由器设备和计算机设备的MAC地址和IP地址如图2-186所示。

下面介绍一下计算机A和计算机B通信的过程。

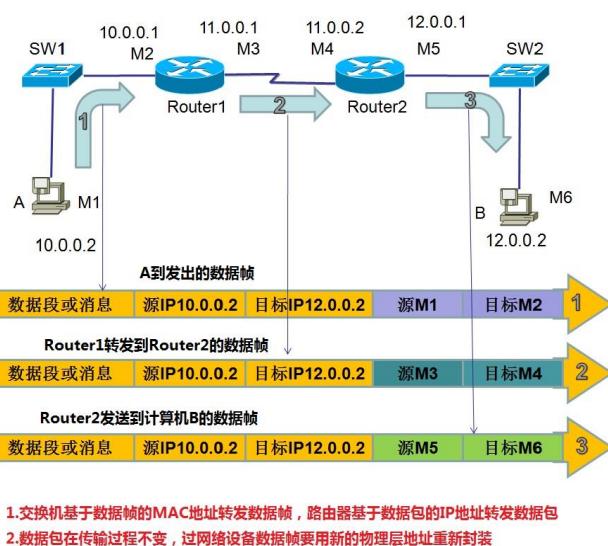
(1) A计算机首先判断B计算机的IP地址和自己的IP地址是否在一个网段，即网络部分是否相同。如果发现不在一个网段，数据包应该发送给路由器Router1，再由路由器Router1转发。

(2) 计算机A配置了网关10.0.0.1，A计算机发出去的数据帧源IP地址为10.0.0.2，目标IP地址为12.0.0.2；源MAC地址为M1，目标MAC地址为M2。这样，交换机SW1

IP协议两个层面意思



▲图2-185 IP协议内涵



▲图2-186 数据转发的过程

将会根据 MAC 地址表将数据帧转发到路由器 Router 1 的接口。

路由器 Router 1 查看数据包的目标 IP 地址，根据路由表，决定数据包下一跳应该发往何处。本示例 Router 1 将数据包转发到 Router 2。Router 1 将数据帧的目标 MAC 地址更改为 M4，源 MAC 地址更改为 M3，这样，Router 2 就能接收该数据帧。

- (3) 同样，路由器 Router 2 接收到数据帧后，查看数据包的目标 IP 地址，根据路由表转发，数据帧的源 MAC 地址更改为 M5，目标 MAC 地址更改为 M6。这样数据帧就能够被交换机 SW2 转发到计算机 B。

2. 数据包的传输过程

总结图 2-184 中计算机 A 和计算机 B 的通信过程，如图 2-187 所示。计算机 A 在和计算机 B 通信的过程中，A 计算机需要为数据在网络层添加源 IP 地址和目标 IP 地址；然后为数据包在数据链路层添加源 MAC 地址和目标 MAC 地址。在传输过程中需要通过交换机和路由器这样的设备，交换机基于目标 MAC 地址转发数据帧，工作在数据链路层；路由器基于目标 IP 地址转发数据包，工作在网络层。计算机 B

接收到数据帧后，在数据链路层去掉 MAC 地址，在网络层去掉 IP 地址，一直到应用层。

3. IP 数据包的格式

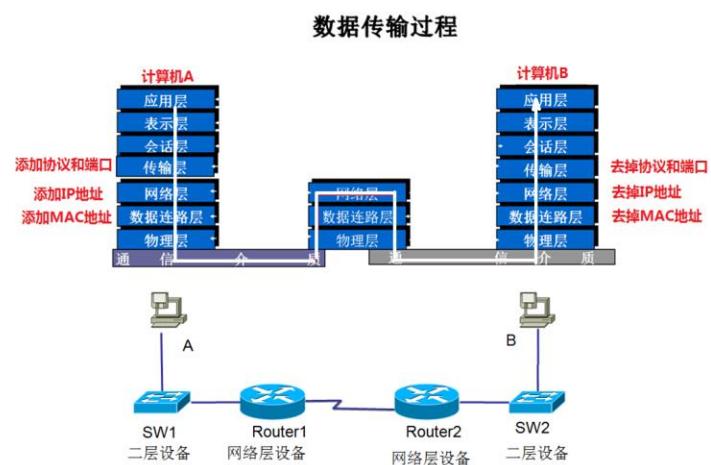
一个 IP 数据包由首部和数据两部分组成。

如图 2-188 所示，首部的前一部分是固定长度，共 20 字节，是所有 IP 数据包必须具有的。

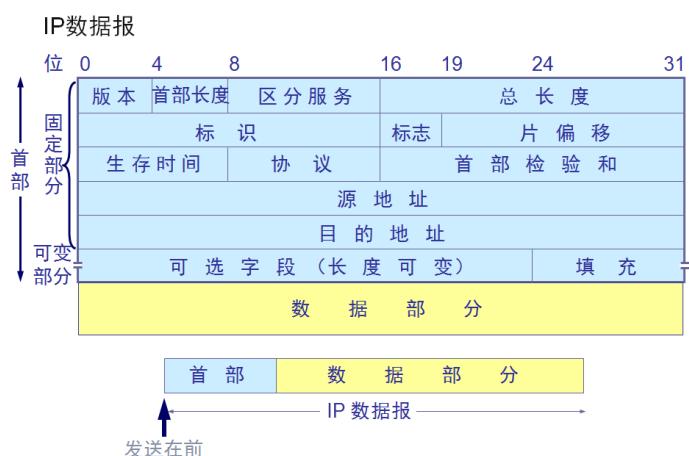
在首部固定部分的后面是一些可选字段，其长度是可变的。

构成 IP 包头的字段如下。

- 版本：IP 版本号。
- 首部长度：32 位字的包头长度（HLEN）。
- 区分服务：服务类型描述数据包将如何被处理。前 3 位表示优先级位。



▲图 2-187 数据传输过程对应的 OSI 参考模型中的层



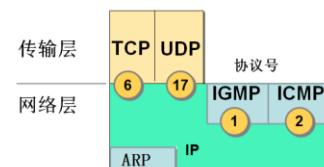
▲图 2-188 IP 数据包格式

- 总长度：包括包头和数据的数据包长度。
- 标识：唯一的 IP 数据包值。
- 标志：说明是否有数据被分段。
- 片偏移：如果数据包在装入帧时太大，则需要进行分段和重组。分段功能允许在因特网上存在大小不同的最大传输单元（MTU）。
- 生存时间（TTL）：存活期是在数据包产生时建立在其内部的一个设置。如果这个数据包在该 TTL 到期时仍没有到达它要去的目的地，那么它将被丢弃。这个设置将防止 IP 包在寻找目的地的时候在网络中不断循环。
- 协议：上层协议的端口（TCP 是端口 6，UDP 是端口 17（十六进制地址））。同样也支持网络层协议，如 ARP 和 ICMP。在某些分析器中被称为类型字段。
- 包头校验和：只针对包头的循环冗余校验（CRC）。
- 源 IP 地址：发送站的 32 位 IP 地址。
- 目的 IP 地址：数据包目的方站点的 32 位 IP 地址。
- 选项：用于网络检测、调试、安全以及更多的内容。
- 数据：在 IP 选项字段后面的就是上层数据。

类型字段是很重要的，它实际上是一个协议字段，在这里，分析仪将它视为 IP 类型字段。如果在数据包的包头中没有为下一层载有这个协议信息，IP 将不知道在本数据包中被装载的数据是用来做什么的。

如图 2-189 所示，展示了网络层协议和传输层协议的关系，即网络层协议+协议号标识传输层协议，如表 2-1 所示。

在这个示例中，协议字段的内容告诉 IP 将此数据发送给 TCP 的端口 6 或 UDP 的端口 17（两个都是十六进制地址）。但是，如果数据是一个前往上层服务或应用程序数据流中的一部分，则这个数据就只是一个 UDP 或 TCP 段。这个数据也可以简单地被指定为因特网控制报文协议（ICMP）、地址解析协议（ARP），或一些其他类型的网络层协议。



▲图 2-189 网络层和传输层的关系

表 2-1 协议和协议号

协议	协议号
ICMP	1
IGMP	2
IPinIP（隧道）	4
EIGRP	88
OSPF	89
IPv6	41
L2TP	115

2.6.2 ICMP 协议

ICMP (Internet Control Message Protocol) 是 Internet 控制报文协议。它是 TCP/IP 协议族的一个子协议，用于在 IP 主机和路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用网络本身的消息。当遇到 IP 数据无法访问目标、IP 路由器无法按当前的传输速率转发数据包等情况时，会自动返回相应的 ICMP 消息。

在计算机上检测网络层故障经常用到的 ping 和 pathping 命令就是使用 ICMP 协议。下面介绍 ping 和 pathping 的使用。

1. ping 命令诊断网络故障

ping (Packet Internet Grope)，因特网包探索器，用于测试网络连接量的程序。ping 发送一个 ICMP 回声请求消息给目的地并报告是否收到所希望的 ICMP 回声应答。

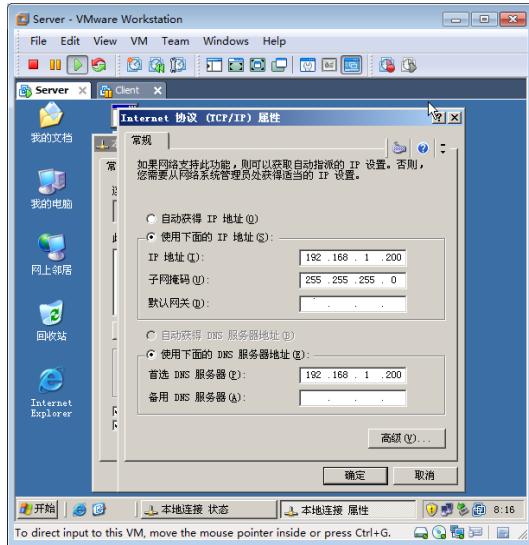
ping 指的是端对端连通，通常用来作为可用性的检查，但是某些病毒木马会强行大量远程执行 ping 命令抢占你的网络资源，导致系统和网速变慢。严禁 ping 入侵作为大多数防火墙的一个基本功能给用户提供选择。

如果你打开 IE 浏览器访问网站失败，你可以通过 ping 命令测试到 Internet 的网络连通，可以为你排除网络故障提供线索。下面展示 ping 命令返回的信息以及其原因分析。

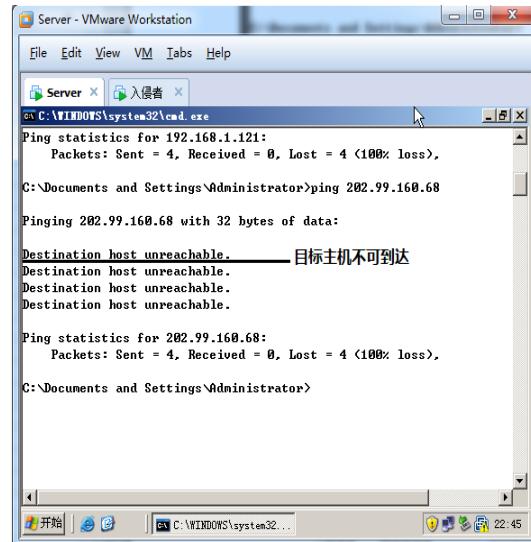
1) 目标主机不可到达

如图 2-190 所示，不设置计算机的网关。

如图 2-191 所示，ping 其他网段的地址，会出现“Destination host unreachable”提示，也就是计算机不知道到该地址下一跳转发给谁。



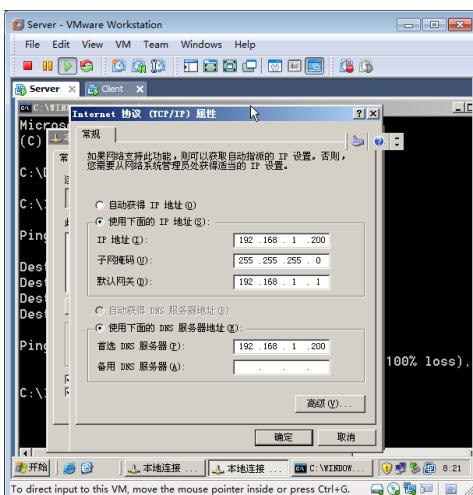
▲图 2-190 去掉网关



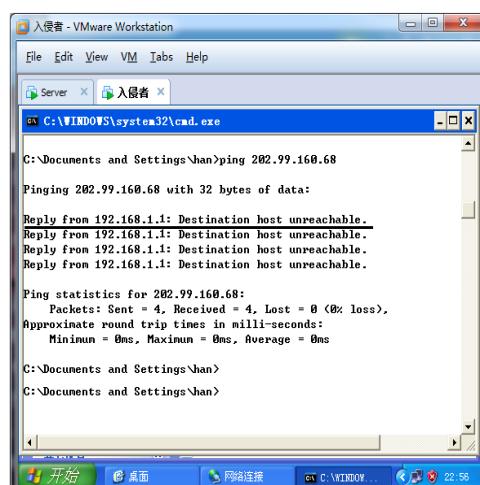
▲图 2-191 目标主机不可到达

如图 2-192 所示，为计算机配置网关。如果路由器没有到目标网段的路由，也就是路由器不知道数据包的目标地址如何转发，

如图 2-193 所示，就会从网关返回“Destination net unreachable”(目标网络不可到达)的信息。



▲图 2-192 添加网关



▲图 2-193 路由器返回目标主机不可到达

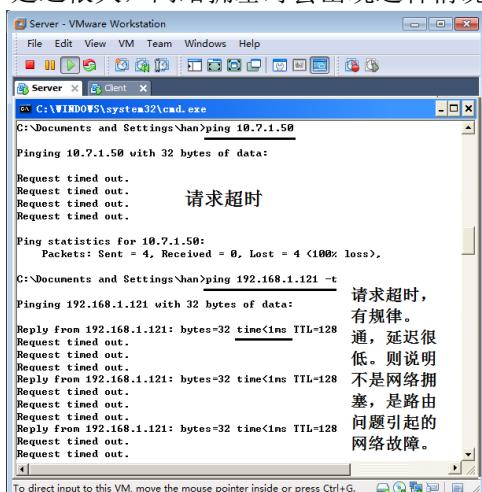
2) 请求超时

如图 2-194 所示, Server 计算机上 ping 10.7.1.50, 返回“Request timed out”提示。以下几种情况均会出现这种信息。

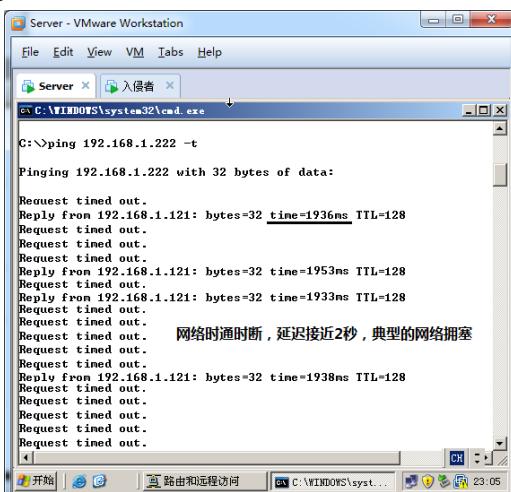
- 对方计算机关机或目标计算机 IP 地址不存在。
- 对方计算机启用了 Windows 防火墙或其他防火墙。
- 数据包到达目的地, 但是返回时失败。
- 网络堵塞。
- 沿途路由器禁止了 ICMP 数据包通过。

如图 2-194 所示, ping 192.168.1.121 -t, 第一个通, 且延迟 1ms, 后面出现 3 个请求超时, 出现一个通、又出现一个请求超时, 这类故障不是网络拥塞, 而是到 192.168.1.121 这个地址有多个路径, 有些路径不通, 是路由器上路由表引起的问题。

如图 2-195 所示, ping 192.168.1.222 -t, 出现时通时断现象。其中 time 是延迟, 接近 2 秒, 延迟很大, 网络拥塞时会出现这种情况。



▲图 2-194 请求超时



▲图 2-195 网络拥塞

3) 通过延迟评估网络带宽

在 Server 计算机上 ping Client 计算机的 IP 地址，在命令提示符下输入 ping 192.168.1.63 -t，(其中，t 参数是一直 ping，否则 ping 4 个数据包就停止了)。按 Ctrl+C 组合键结束 ping。

如图 2-196 所示，10M 以太网和 100M 以太网网速很快，延迟在 1ms 左右。如果大于这个值，则局域网有可能有点堵。

如图 2-197 所示，ping www.inhe.net，可以看到最大延迟、最小延迟以及平均延迟都比局域网大得多。如果你访问国外的一些网站，延迟一般会比国内的网站大。

```
C:\>ping 192.168.1.63

Pinging 192.168.1.63 with 32 bytes of data:

Reply from 192.168.1.63: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.63:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>= 局域网通信延迟一般在1ms左右
```

▲图 2-196 ping 192.168.1.63 -t

```
C:\>ping www.inhe.net [221.192.155.193] with 32 bytes of data:

Reply from 221.192.155.193: bytes=32 time=192ms TTL=240
Reply from 221.192.155.193: bytes=32 time=193ms TTL=240
Reply from 221.192.155.193: bytes=32 time=192ms TTL=240
Reply from 221.192.155.193: bytes=32 time=191ms TTL=240

Ping statistics for 221.192.155.193:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 191ms, Maximum = 193ms, Average = 192ms

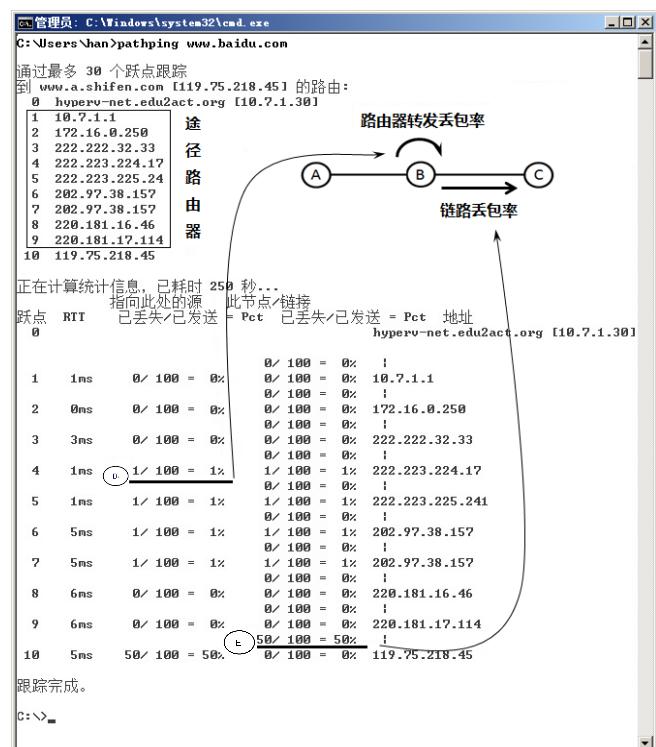
C:\>= 最小延迟 最大延迟 平均延迟
```

▲图 2-197 ping www.inhe.net

2. pathping 跟踪数据包的路径

使用 ping 能够判断网络通还是不通，比如请求超时，但不能判断是哪个位置出现的网络故障造成请求超时。使用 pathping 命令就能跟踪数据包的路径，查出故障点，并计算路由器转发丢包率、链路丢包率以及延迟，据此可以判断出网络的拥塞情况。

如图 2-198 所示，在命令行下输入 pathping www.baidu.com，可以看到数据包到达目的地途经的路由器、计算的延迟和丢包率。丢包率有路由器转发丢包率，如图 2-198 中 D 处所示丢包率是路由器接收到数据包后，路径选择转发时的丢包率。转发丢包率高则表明这些路由器已经超载，说明路由器的处理能力不够；丢包率还有链路丢包率，如图 2-198 中 E 处所



▲图 2-198 pathping 的结果

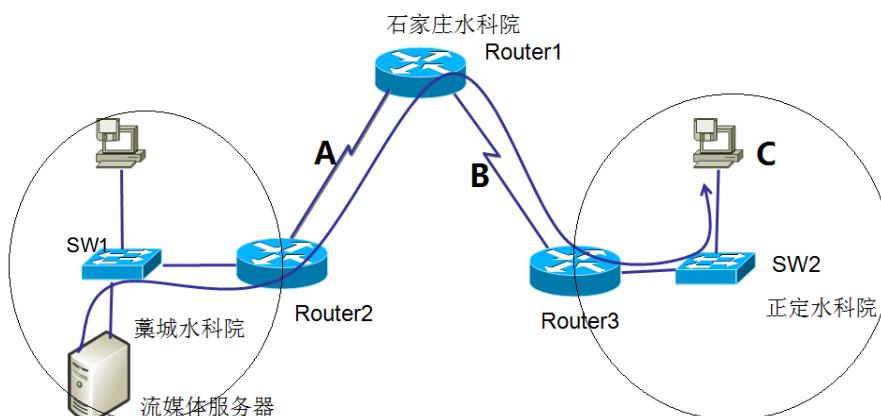
示，是指路由器 B 到路由器 C 链路上的丢包率，链路上的丢包率反映的是造成路径上转发数据包丢失的链路的拥挤状态。

3. 使用 pathping 判断网络故障点

藁城水科院和正定水科院都与石家庄水科院连接，如图 2-199 所示。在藁城水科院部署了一台流媒体服务器，一天，正定水科院的人反映访问藁城的流媒体服务器点播视频非常不连贯。如果你是藁城水科院的网络管理员，如何断定是网络出现了拥塞还是流媒体服务器过载？

出现问题的网络无外乎是藁城水科院局域网、连接石家庄的 A 广域网、连接石家庄和正定的 B 广域网，以及正定水科院局域网。

断定网络是否拥塞的办法就是，在正定水科院的计算机 C 上 ping 藁城水科院的流媒体服务器的 IP 地址，如果响应时间很短，则网络没问题，有可能是流媒体服务器的性能差造成响应客户端请求慢，从而造成视频播放不连贯。如果有请求超时的数据包或响应延迟超长，比如大于 500ms，则有可能是网络拥塞造成的问题。然后使用 pathping 服务器的 IP 地址，根据 pathping 的结果查看哪段网络丢包严重。就能断定哪段网络拥塞。



▲图 2-199 pathping 排错

4. 根据 TTL 判断对方是什么操作系统

TTL (Time To Live, 生存时间)，是 IP 协议包中的一个值，指定数据包被路由器丢弃之前允许通过的网段数量，数据包每经过路由器转发一次都至少要把 TTL 减一，TTL 通常表示包在被丢弃前最多能经过的路由器个数。当记数到 0 时，路由器决定丢弃该包，并发送一个 ICMP 报文给最初的发送者。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。

TTL 是由发送主机设置的，TTL 字段值可以帮助我们识别操作系统类型。下面是默认操作系统 TTL。

- | | |
|-------------------|-----|
| ▪ Linux | 64 |
| ▪ Windows 2000/NT | 128 |
| ▪ Windows 系列 | 32 |
| ▪ Unix 系列 | 255 |

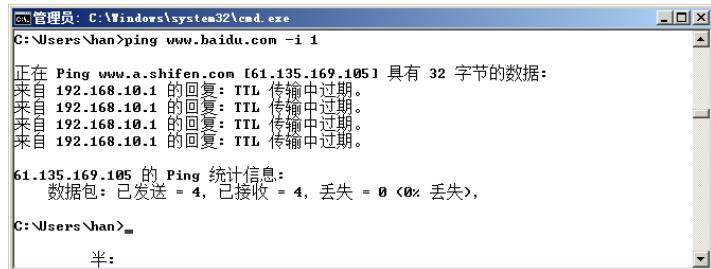
我们可以更改注册表设置 TTL 的值，可以修改，但不能大于十进制的 255，使用 ping 发现的 TTL 可以粗略判断对方是什么操作系统，中间经过了多少个路由器。



▲图 2-200 通过查看 TTL 值判断一些信息

下面使用 ping 返回来的 TTL 值判断百度的操作系统以及途经的路由器。如图 2-200 所示。可以看到返回来的数据包 TTL 值为 54，接近 64，可以初步断定其是 Linux 操作系统，中间经过 10 个路由器到达本机因此 TTL 变为 54。

使用 ping 后面添加 i 参数，可以更改计算机发送 ICMP 数据包的 TTL 值，如下所示，数据包-i 后面添加了 1，从网关（也就是第一个路由器）就返回 TTL 在传输中过期。如果是 2，就会从第二个路由器返回 TTL 在传输过程中过期，如果输入 3，我们就可以不用使用 pathping，也能判断数据包经过的路由器。如图 2-201 所示。



▲图 2-201 ping 后面添加 i 参数

2.6.3 IGMP 协议

Internet 组管理协议 IGMP (The Internet Group Management Protocol) 是因特网协议家族中的一个组播协议，用于 IP 主机向任意一个直接相邻的路由器报告它们的组成员情况。IGMP 信息封装在 IP 报文中，其 IP 协议号为 2。

IGMP 用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。IGMP 不包括组播路由器之间的组成员关系信息的传播与维护，这部分工作由各组播路由协议完成。所有参与组播的主机必须实现 IGMP。

参与 IP 组播的主机可以在任意位置、任意时间、成员总数不受限制地加入或退出组播组。组播路由器不需要也不可能保存所有主机的成员关系，它只是通过 IGMP 协议了解每个接口连接的网段上是否存在某个组播组的接收者，即组成员。而主机方只需要保存自己加入了哪些组播组。

2.6.4 ARP协议

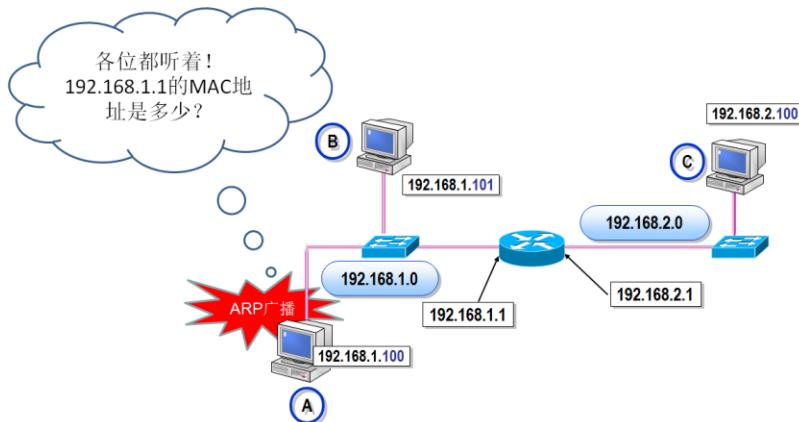
地址解析协议 ARP (Address Resolution Protocol) 可以由已知主机的 IP 地址在网络上查找到它的硬件地址。其工作过程如下。

(1) 同网段通信。

如图 2-200 所示, 当计算机 A 和计算机 B 通信, 计算机 A 需要获得计算机 B 的 MAC 地址, 计算机 A 根据自己的 IP 地址以及子网掩码判断出和目标 IP 地址在同一个网段, 计算机 A 就直接在网上发送一个 ARP 广播包解析目标 B 计算机 IP 地址对应的 MAC 地址, 该数据帧目标 MAC 地址为 FF-FF-FF-FF-FF-FF, 该网段的计算机都能收到该广播包, 计算机 B 返回计算机自己的 MAC 地址, 计算机 A 缓存该结果。后续的通信都用该 MAC 地址封装。

(2) 不同网段通信。

如图 2-202 所示, 计算机 A 和计算机 C 通信, 计算机 A 根据自己的 IP 地址以及子网掩码判断出和目标 IP 地址不在同一个网段, 因此计算机 A 发送 ARP 广播包解析网关的 MAC 地址, 也就是路由器的接口地址 192.168.1.1 的 MAC 地址。路由器返回自己的 MAC 地址, 计算机 A 缓存解析的结果。



▲图 2-202 ARP 解析过程

从以上描述可以看出, ARP 解析 MAC 地址时, 不进行任何验证, 缓存的结果还可以被其他计算机重新修改, 这就是一个很严重的安全漏洞。下面将会介绍利用 ARP 漏洞的一款局域网流量控制软件“P2P 终结者”。

逆向 ARP 即 RARP, 就是已知 MAC 地址得到 IP 地址, 如果计算机的 IP 地址配置为自动获得, 将会使用 RARP, 即请求 IP 地址过程用到的协议为逆向 RAP (RARP)。

1. 局域网流量控制软件

P2P 终结者按正常来说是个很好的网管软件, 但是好多人却拿它来恶意地限制他人的流量, 使他人不能正常上网。下面我们对 P2P 终结者的功能以及原理还有突破方法进行详细的介绍。

我们先来看看来自网上 P2P 的资料: P2P 终结者是由 Net.Soft 工作室开发的一套专门用来控制企业网络 P2P 下载流量的网络管理软件。该软件针对目前 P2P 软件过多占用带宽的问题, 提供了一个非常简单的解决方案。P2P 终结者基于底层协议分析处理实现, 具有良好的透明性。它可以适应绝大多数网络环境, 包括代理服务器、ADSL 路由器共享上网、LAN 专

线等网络接入环境。

P2P 终结者彻底解决了交换机连接网络环境的问题，做到真正只需要在任意一台主机安装即可控制整个网络的 P2P 流量，对于网络中的主机来说具有良好的控制透明性，从而有效地解决了这一目前令许多网络管理员都极为头痛的问题，具有较好的应用价值。

P2P 终结者功能可以说是非常强大的，作者开发它是为网络管理者所使用，但是由于现在 P2P 终结者的破解版在网上广为流传（P2P 是一款收费软件），如果被网络管理者正当地使用也罢了，但是却有很多人利用它来恶意控制别人的网速，使得我们平时的正常使用都出现问题。尤其 P2P 终结者比另外的一些网管软件多出很多功能，最为突出的是控制目前比较流行的多种 P2P 协议，像 BitTorrent 协议、Baidu 下吧协议、Poco 协议、Kamun 协议等。该软件可以控制基于上述协议的绝大部分客户端软件，如 BitComet（比特彗星）、Bitspirit（比特精灵）、贪婪 BT、卡盟、百度下吧、Poco、PP 点点通等软件；而且还有 HTTP 下载自定义文件后缀控制功能，FTP 下载限制功能，QQ、MSN、POPO、UC 聊天工具控制功能等等。

那么它到底是怎样实现这些功能的呢？要想突破它，就得对它的原理有比较清楚的了解。

P2P 终结者对这些软件下载的限制最基本的原理也和其他的网管软件相同，像网络执法人员一样，都用的是 ARP 欺骗原理。

正常情况下，当计算机 A 要发送数据给 B 的时候，就会先去查询本地的 ARP 缓存表，找到计算机 B 的 IP 地址对应的 MAC 地址，然后进行数据传输。如果没有找到，则广播一个 ARP 请求报文（携带计算机 A 的 IP 地址 IA 和物理地址 MA），请求 IP 地址为 IB 的 MAC 地址。网上所有计算机包括计算机 B 都收到 ARP 请求，但只有计算机 B 能识别自己的 IP 地址，于是向计算机 A 发回一个 ARP 响应报文，其中就包含有计算机 B 的 MAC 地址。计算机 A 接收到计算机 B 的应答后，就会更新本地的 ARP 缓存，接着使用这个 MAC 地址发送数据。因此，本地高速缓存的这个 ARP 表是本地网络流通的基础，而且这个缓存是动态的。ARP 协议并不只在发送了 ARP 请求后才接收 ARP 应答，当计算机接收到 ARP 应答数据包的时候，就会对本地的 ARP 缓存进行更新，将应答中的 IP 和 MAC 地址存储在 ARP 缓存中。

如果计算机 A 解析计算机 B 的 MAC 地址时，网络中的计算机 C 向计算机 A 发送一个应答，冒充计算机 B 伪造 ARP 响应，即 IP 地址为计算机 B 的 IP，而 MAC 地址是计算机 C 的 MAC 地址，则当计算机 A 接收到计算机 C 伪造的 ARP 应答后，就会更新本地的 ARP 缓存。这样在计算机 A 看来，计算机 B 的 IP 地址没有变化，而其 MAC 地址已不是原来的那个了。由于局域网的交换机转发数据不是根据 IP 地址进行，而是按照 MAC 地址进行转发。这样计算机 A 发给计算机 B 的通信，将通过交换机转发到计算机 C，然后再由计算机 C 转发给计算机 B，这样就能够捕获计算机 A 和计算机 B 之间的通信，当然计算机 C 也能够控制通信的带宽。

如果那个伪造出来的 MAC 地址在计算机 A 上被修改成一个不存在的 MAC 地址，则会造成网络不通，导致计算机 A 不能 ping 通计算机 B。这就是一个简单的 ARP 欺骗。

看到这些内容，想必大家也就会明白为什么 P2P 可以对网络中的计算机进行流量控制。其实在这儿，它充当了一个网关的角色。如图 2-201 所示，把一网段内的所有计算机的数据欺骗过来，然后再进行二次转发。所有被控制计算机的数据以后都会先经过这台 P2P 主机，然后再转到网关。

基本原理就是这样，下面针对它的工作原理进行突破。

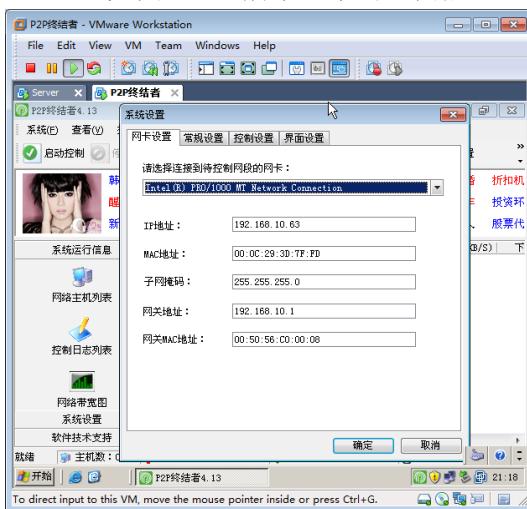
使用双向 IP/MAC 绑定，在 PC 上绑定你的出口路由器的 MAC 地址，P2P 终结者软件不能对你进行 ARP 欺骗，自然也没法管你，不过只是 PC 绑定路由的 MAC 还不安全。因为 P2P 终结者软件可以欺骗路由，所以最好的解决办法是使用 PC、路由上双向 IP/MAC 绑定。也就是说，在 PC 上绑定路由的 MAC 地址，在路由上绑定 PC 的 IP 和 MAC 地址。这就要求路由要支持 IP/MAC 绑定。

2. 使用 P2P 终结者控制流量

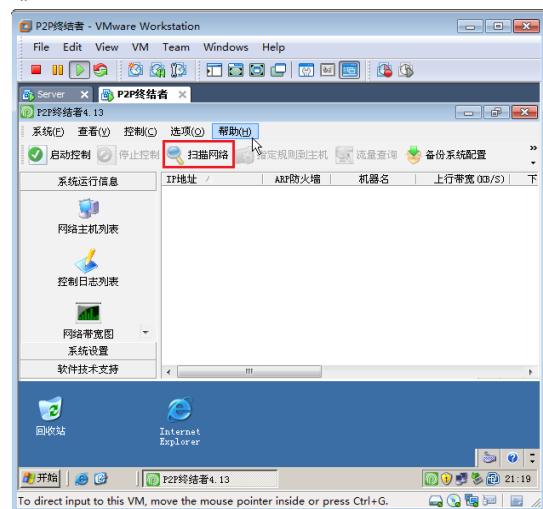
下面就以同一个网段的两个计算机演示 P2P 终结者流量控制软件是如何控制网络流量的。P2P 终结者可以在 <http://down.51cto.com/> 网站搜索“P2P 终结者”并下载。

现在演示使用“P2P 终结者”控制 Server 上网带宽，展示 MAC 地址欺骗的过程。

- (1) 在“P2P 终结者”计算机上安装 P2P 终结者软件，单击运行该软件。
- (2) 如图 2-204 所示，出现“系统设置”对话框，在“网卡设置”选项卡中，选中网卡，单击“确定”按钮。
- (3) 如图 2-205 所示，单击“扫描网络”按钮。

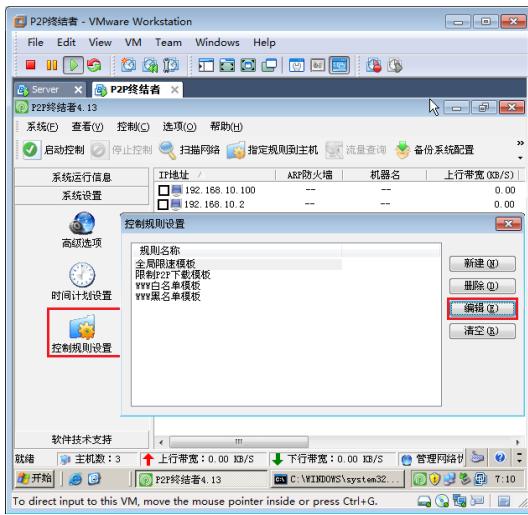


▲图 2-204 选择网卡

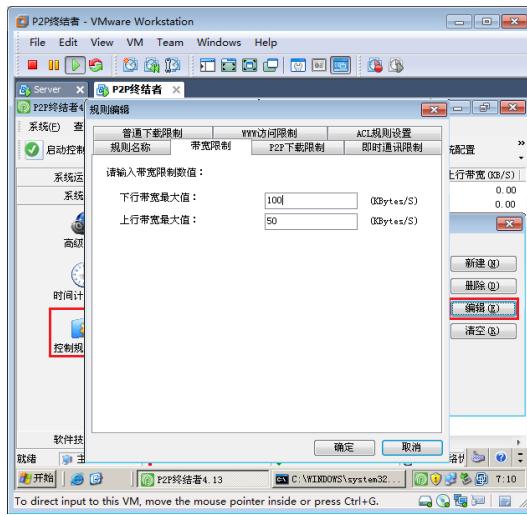


▲图 2-205 扫描网络

- (4) 如图 2-206 所示，单击“控制规则”按钮，在出现的“控制规则设置”对话框中，选中“全局限速模板”选项，单击“编辑”按钮。
- (5) 如图 2-207 所示，在“带宽限制”选项卡中，指定下行和上行的最大带宽，单击“确定”按钮。

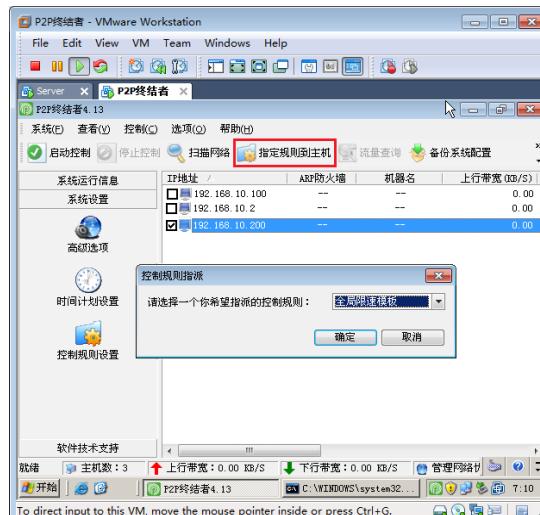


▲图 2-206 编辑控制规则

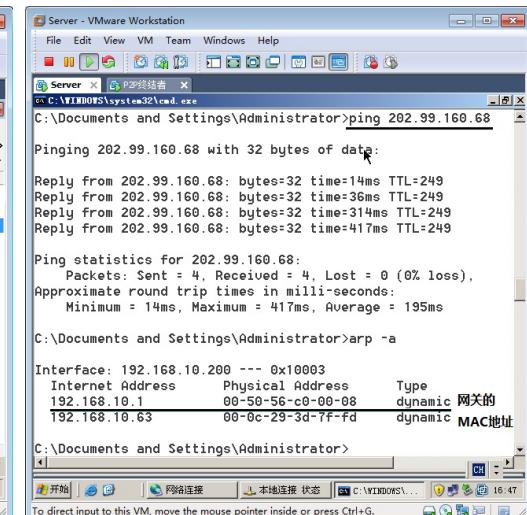


▲图 2-207 指定上、下行带宽

- (6) 如图 2-208 所示，选中 Server 的 IP 地址，单击“指定规则到主机”按钮，在出现的“控制规则指派”对话框中，选择“全局限速模板”选项，单击“确定”按钮。
- (7) 如图 2-209 所示，在 Server 上，ping 202.99.160.68 地址，这是 Internet 的 DNS 服务器的地址，然后运行 arp -a 命令查看网关的 MAC 地址。注意，现在查看的地址是真正的网关的 MAC 地址。

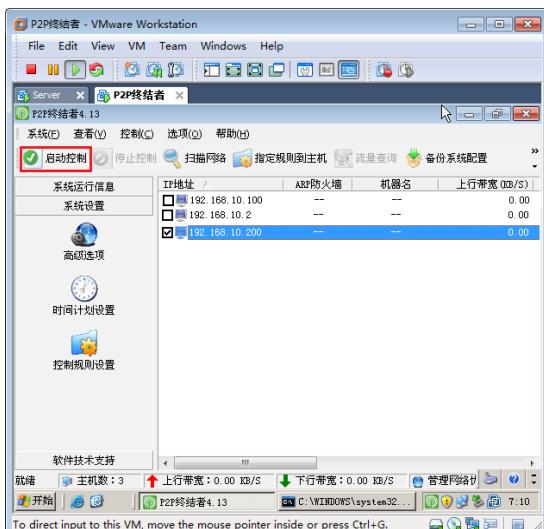


▲图 2-208 应用规则到主机

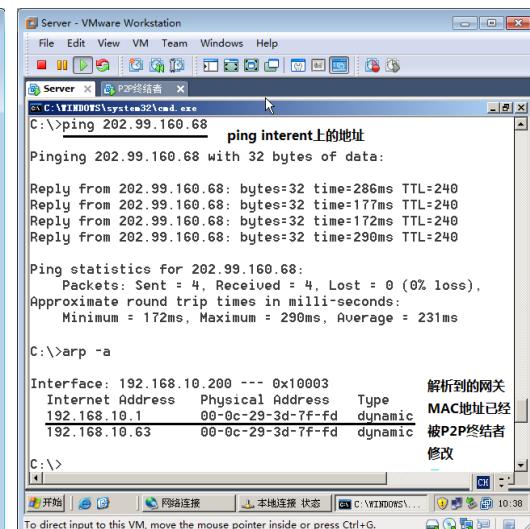


▲图 2-209 查看网关的 MAC 地址

- (8) 如图 2-210 所示，在“P2P 终结者”计算机上，单击“启动控制”按钮。
- (9) 如图 2-211 所示，再在 Server 上 ping 202.99.160.68，然后运行 arp -a 命令查看缓存的 MAC 地址，发现和上面看到的不一样了。



▲图 2-210 启用控制



▲图 2-211 查看网关的 MAC 地址

- (10) 如图 2-212 所示，在“P2P 终结者”计算机上，在命令提示符下输入 ipconfig /all 可以看到其 MAC 地址，对比 Server 上缓存的网关的 MAC 地址，发现 Server 上缓存的网关的 MAC 地址是“P2P 终结者”计算机上的 MAC 地址。这样，Server 访问 Internet 流量都会转发到“P2P 终结者”计算机上，然后即可进行带宽控制，这就是 ARP 欺骗。
- (11) 如何避免 ARP 欺骗呢？如图 2-213 所示，你可以在 Server 上运行 arp -s 192.168.1.1 00-50-56-c0-00-08 添加网关和 MAC 地址绑定。运行 arp -a 命令，可以看到添加的静态的 IP 地址和 MAC 地址映射，这样，Server 就不会发送 ARP 广播包解析网关的 MAC 地址了。

```
C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration

Host Name . . . . . : $1
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter 本地连接:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT
Physical Address. . . . . : 00-0c-29-3d-7f-fd
DHCP Enabled. . . . . : No
IP Address . . . . . : 192.168.10.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
DNS Servers . . . . . : 202.99.160.68

C:\Documents and Settings\Administrator>_
```

▲图 2-212 查看本机 MAC 地址

```
C:\Documents and Settings\Administrator>cd \
C:\>arp -s 192.168.1.1 00-50-56-c0-00-08 将网关的IP和MAC绑定
C:\>arp -a

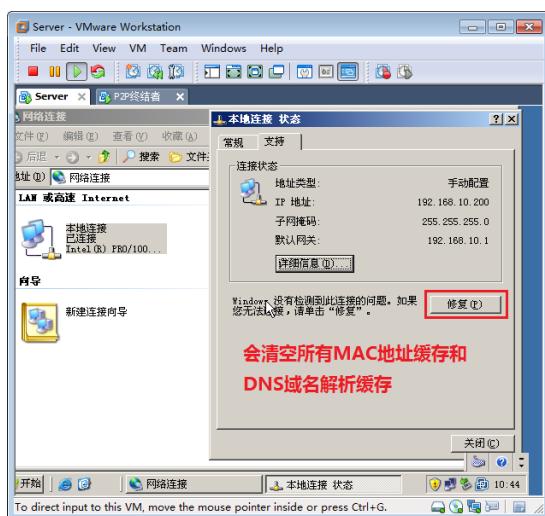
Interface: 192.168.10.200 --- 0x10003
Internet Address Physical Address Type
192.168.10.1 00-0c-29-3d-7f-fd dynamic
192.168.10.63 00-0c-29-3d-7f-fd dynamic
192.168.10.100 00-0c-29-3d-7f-fd dynamic

C:\>_
```

▲图 2-213 绑定网关和 MAC 地址

(12) 如图 2-214 所示，人为添加的 IP 地址和 MAC 地址映射，不会过一段时间自动删除，除非重启系统，或修复本地连接。

(13) 在路由器上，也要添加 Server 的 IP 地址和 MAC 地址的映射。



▲图 2-214 修复本地连接

```
Router#conf t
Router (config) #arp 219.239.144.134 abcd.abcd.abcd arpa
```

2.7 使用捕包工具排除网络故障

作为网络管理员，你可能会碰到访问 Internet 网速慢的问题，你要能够判断出是哪里出了问题，是局域网中有计算机发广播包堵塞了局域网，还是网络中有人使用 BT 下载软件或迅雷下载软件将广域网的带宽给占用了？你需要使用捕包工具来捕获网络中的数据包，通过分析网络中的数据包，排除网络故障。

2.7.1 示例：查看谁在发送广播包

我给某单位调试网络，发现计算机 ping 网关时通时断，不能判断是硬件故障还是软件故障，但是看到交换机的所有端口指示灯疯狂闪烁，看样子在疯狂地转发数据，初步判断网络中有广播包。到底哪台计算机在网上发送广播？需要使用抓包工具捕获网络中的数据包，通过查看数据包的源 IP 地址找到发送广播包的计算机。

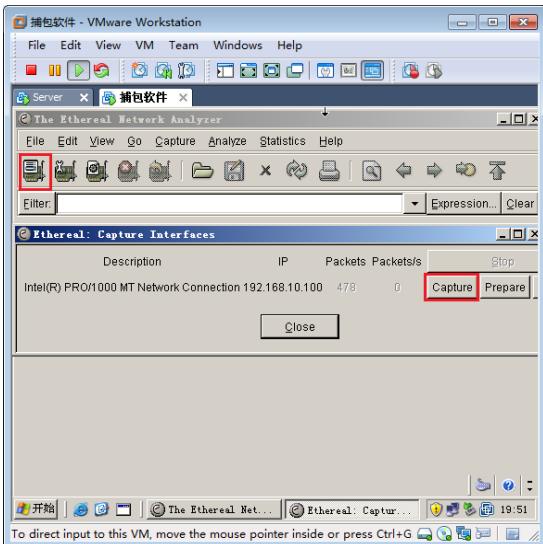
下面将会演示使用捕包工具捕获数据包，并且查看数据包的层次结构、数据链路层的内容、网络层的内容以及传输层的内容和数据。排序数据包，保存捕获的数据包，打开捕获的数据包，查看网络中的广播帧。

现在演示使用 Ethereal-setup-0.99.0.exe 抓包工具，分析数据包结构，保存数据包，打开保存的数据包。

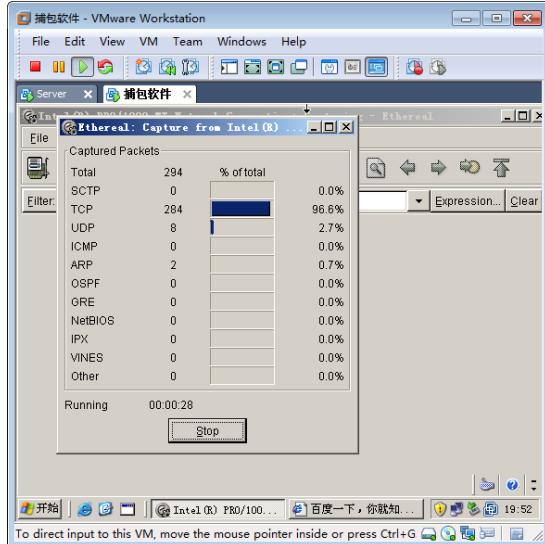
在“捕包软件”计算机上，安装 Ethereal-setup 并运行该软件。

- (1) 如图 2-215 所示，单击图标，选择网卡，单击 Capture 按钮，开始捕包。
- (2) 如图 2-216 所示，在出现的 Ethereal: Capture from...对话框中，可以看到网络捕包

中各个协议的比例，单击“Stop”按钮，停止并查看捕获的数据包。



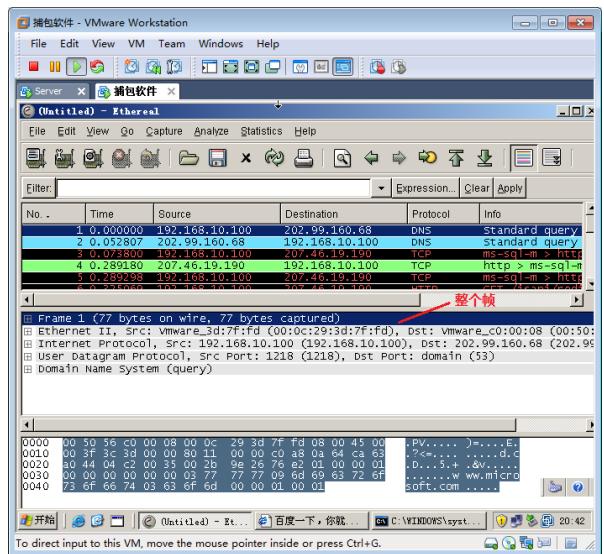
▲图 2-213 选择捕包网卡



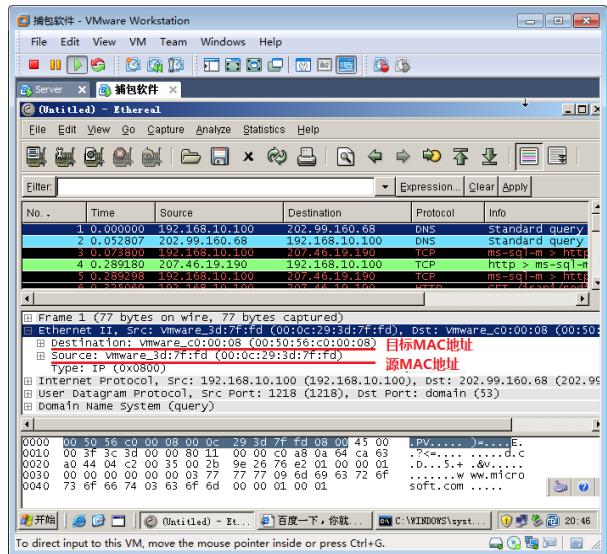
▲图 2-214 开始捕包

(3) 如图 2-217 所示，在上栏选中第一个数据包、中栏选中 Frame，在下栏可以看到整个帧。

(4) 如图 2-218 所示，在中栏选中 Ethernet，在下栏可以看到数据帧的源 MAC 地址和目标 MAC 地址，即整个数据帧的数据链路层部分。



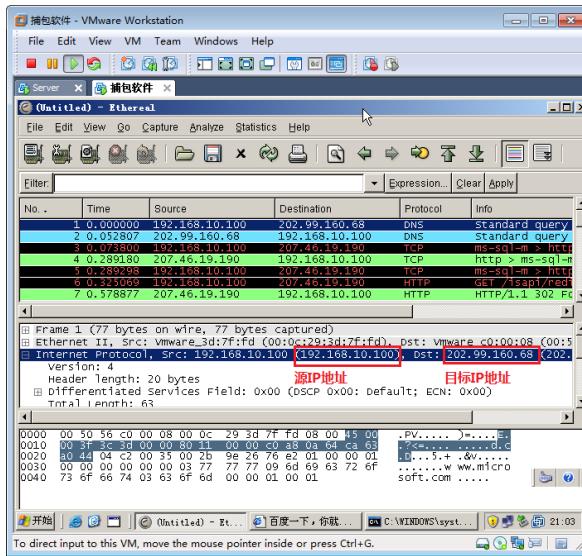
▲图 2-217 整个帧



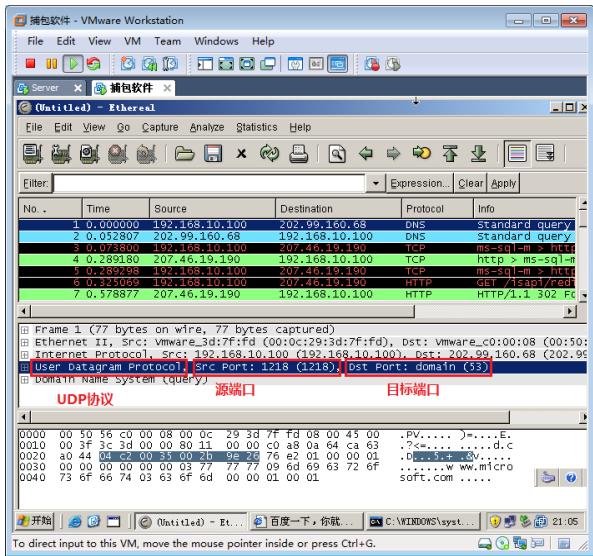
▲图 2-218 帧的数据链路层

(5) 如图 2-219 所示，在中栏选中 Internet Protocol，在下栏可以看到整个数据帧的网络层部分，包括数据帧的目标 IP 地址和源 IP 地址。

(6) 如图 2-220 所示，在中栏选中 User Datagram Protocol，可以看到数据帧的传输层部分，包括数据包的源端口和目标端口。



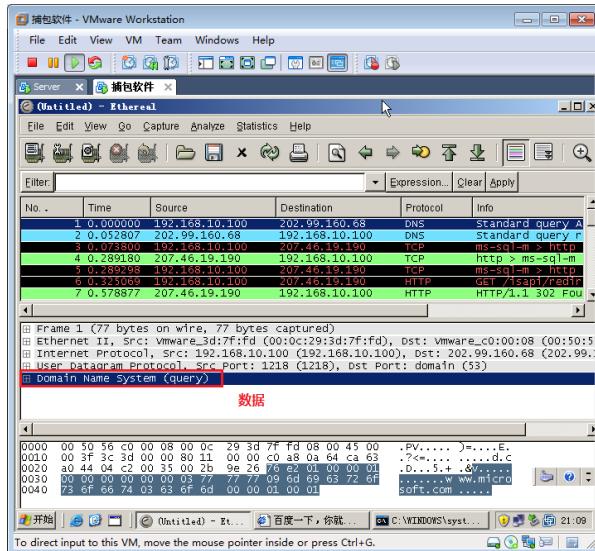
▲图 2-219 查看数据包的源地址和目标地址



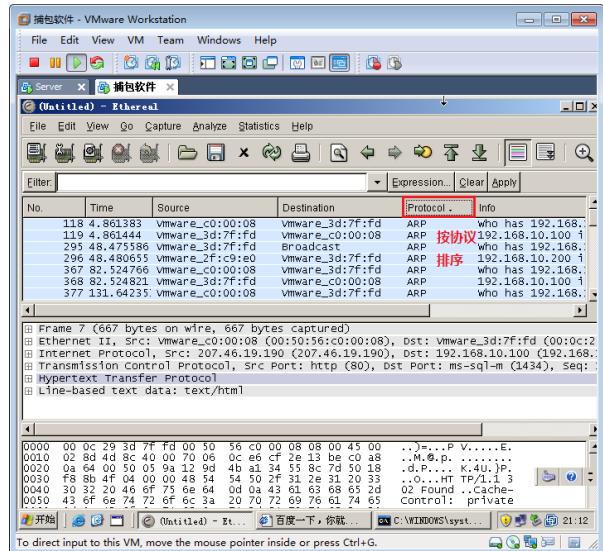
▲图 2-220 源端口和目标端口

(7) 如图 2-221 所示，在中栏选中 Domain Name System，可以看到整个帧的数据部分。

(8) 如图 2-222 所示，单击 Protocol 字段，可以将捕获的数据包按协议排序。



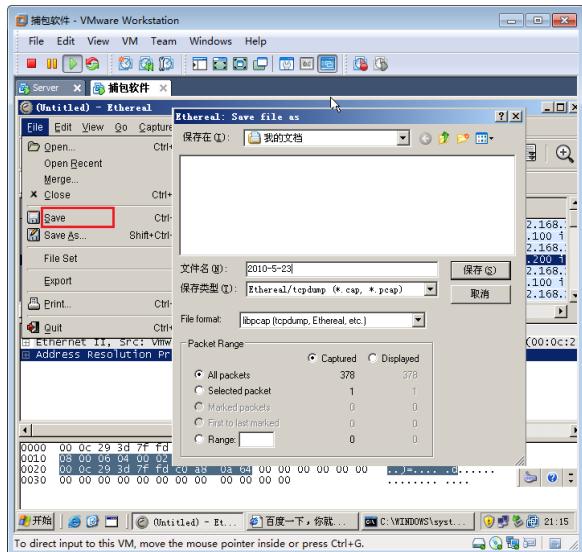
▲图 2-221 查看数据包的数据部分



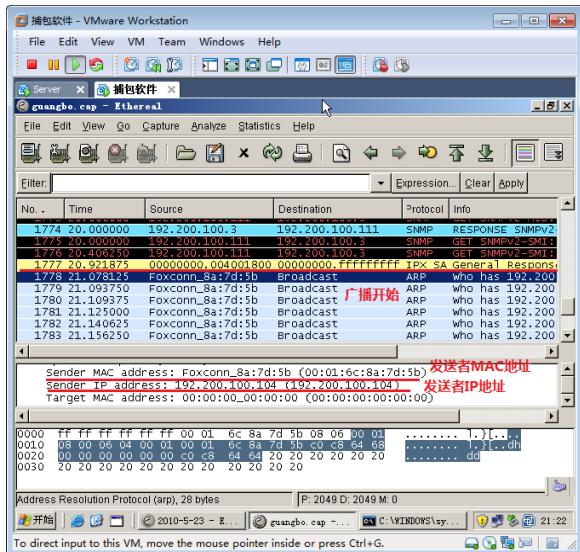
▲图 2-222 按协议排序数据包

(9) 如图 2-223 所示，选择 File→Save 菜单命令，可以将捕获的数据包保存，供以后分析使用。

(10) 选择 File→Open 菜单命令，可以打开以前捕获的数据包。图 2-224 是打开的以前排错网络故障抓获的数据包。可以看到捕获的数据包后面全是广播包，因此网络发生堵塞。通过查看广播的发送者的 IP 地址，就能找到发送者。



▲图 2-221 保存捕获的数据包

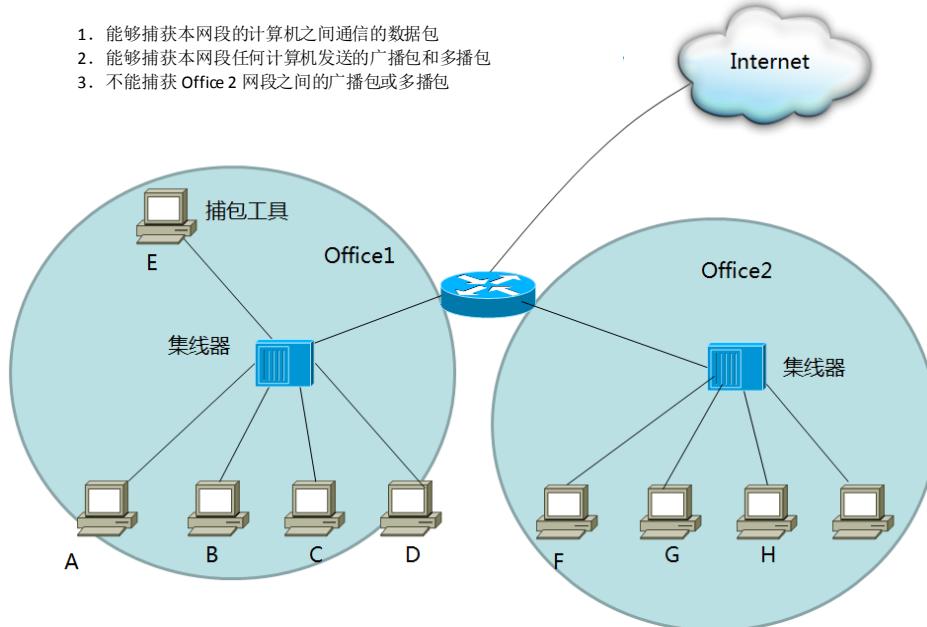


▲图 2-222 查看广播包

2.7.2 捕包软件安装的位置

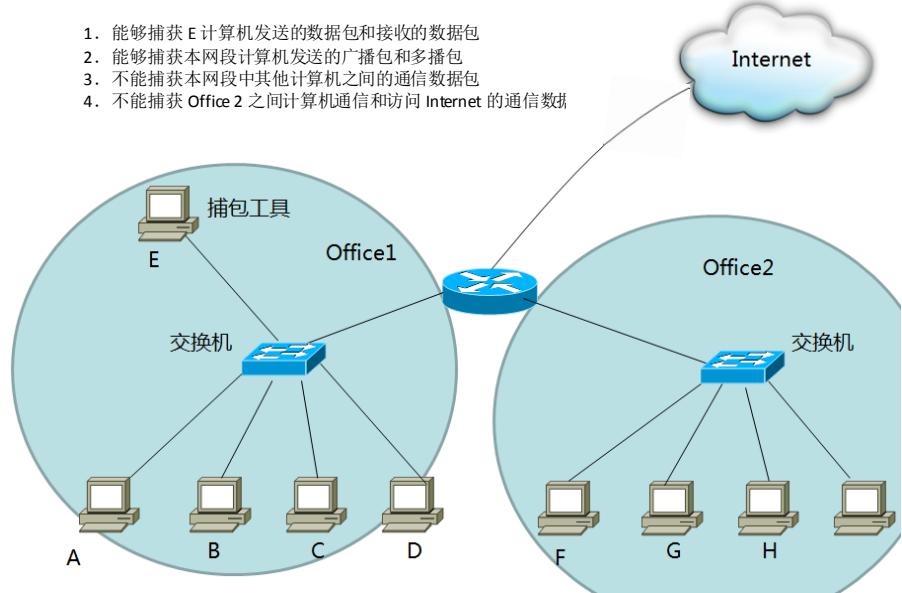
如图 2-225 所示, Office1 网段和 Office2 网段是使用集线器连接的, 路由器连接局域网, 通过路由器连接 Internet。在 Office1 网段的 E 计算机上安装捕包工具, 由于集线器是共享式网络, 能够捕获 Office1 网段中所有计算机之间的通信数据包, 还能够捕获该网段中的所有计算机发送的广播数据包。但是 Office2 网段计算机发送的广播包被路由器隔离, 所以 E 计算机不能捕获, Office2 网段计算机访问 Internet 的数据包也不能被 E 计算机捕获。

1. 能够捕获本网段的计算机之间通信的数据包
2. 能够捕获本网段任何计算机发送的广播包和多播包
3. 不能捕获 Office2 网段之间的广播包或多播包



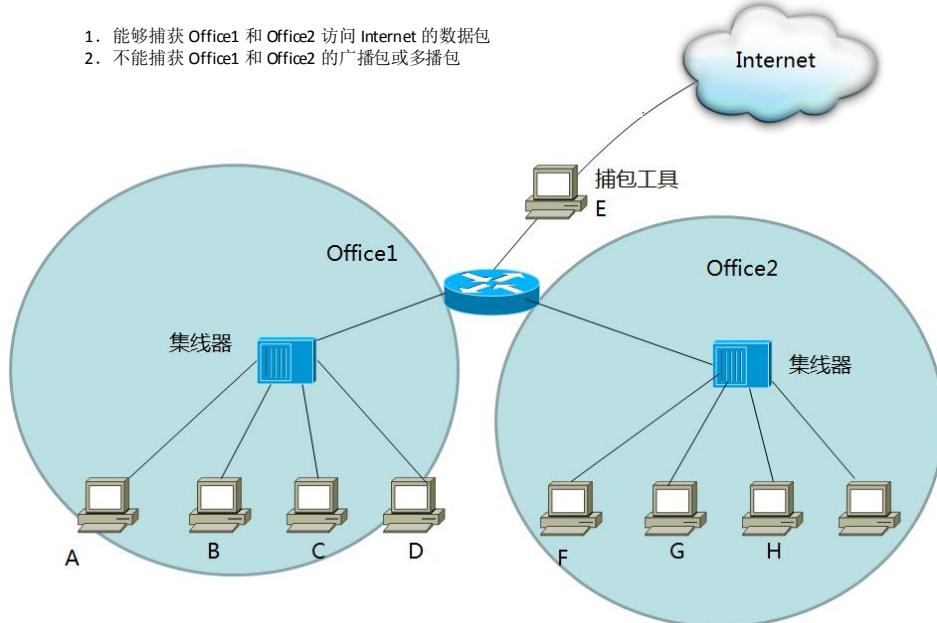
▲图 2-225 集线器与捕包工具

如图 2-226 所示，是使用交换机连接的局域网。安装捕包工具的计算机，能捕获 E 计算机发送的数据包和接收的数据包，也能够捕获本网段计算机发送的广播包和多播包；不能捕获本网段中其他计算机之间的通信数据包，除非配置了镜像端口（监视端口，这在交换章节中会讲到），也不能捕获 Office2 之间计算机通信和访问 Internet 的通信数据包。



▲图 2-226 交换机与捕包工具

如图 2-227 所示，如果想捕获 Office1 网段和 Office2 网段的计算机访问 Internet 的流量，需将安装了捕包工具的计算机 E 放置到图中所示的位置，就能够捕获 Office1 和 Office2 访问 Internet 的流量，但不能捕获 Office1 和 Office2 的广播包或多播包。



▲图 2-227 捕包工具的位置

2.8 习题

1. TCP/IP 是 Internet 采用的协议标准，它是一个协议系列，由多个不同层次的协议共同组成，用于将各种计算机和设备组成实际的计算机网络。

TCP/IP 协议系统分成四个层次，分别是网络接口层、网络层、传输层与应用层。

(1) 是属于网络层的低层协议，主要用途为完成网络地址向物理地址的转换。

(2) 起到相反的作用，多用在无盘工作站启动时利用物理地址解析出对应的网络地址。

(3) 是与 IP 协议同层的协议，更确切的说是工作在 IP 协议之上，又不属于传输层的协议，可用于 Internet 上的路由器报告差错或提供有关意外情况的信息。

(4) 是一种面向连接的传输协议，在协议使用中存在着建立连接、传输数据、撤销连接的过程；(5) 是一种非连接的传输协议，采用这种协议时，每一个数据包都必须单独寻径，特别适合于突发性短信息的传输。

- | | | | |
|-------------|---------|---------|---------|
| (1) A. RARP | B. ICMP | C. ARP | D. IGMP |
| (2) A. RARP | B. ARP | C. IPX | D. SPX |
| (3) A. IGMP | B. ICMD | C. CDMA | D. WAP |
| (4) A. SNMP | B. NFS | C. TCP | D. UDP |
| (5) A. HTTP | B. FTP | C. TCP | D. UDP |

2. Internet 提供了大量的应用服务，分为通信、获取信息与共享计算机资源三类。

(1) 是世界上使用最广泛的一类 Internet 服务，以文本形式或 HTML 格式进行信息传递，而图形等文件可以作为附件进行传递。

(2) 是用来在计算机之间进行文件传输。利用该服务不仅可以从远程计算机获取文件，而且可以将文件从本地计算机传送到远程计算机。

(3) 是目前 Internet 上非常丰富多彩的应用服务，其客户端软件称为浏览器。目前较为流行的 Browser/Server 网络应用模式就以该类服务作为基础。

(4) 应用服务将主机变为远程服务器的一个虚拟终端；在命令行方式下运行时，通过本地计算机传送命令，在远程计算机上运行相应程序，并将相应的运行结果传送到本地计算机显示。

- | | | | |
|--------------|-----------|-----------|-----------|
| (1) A. Email | B. Gopher | C. BBS | D. TFTP |
| (2) A. DNS | B. NFS | C. WWW | D. FTP |
| (3) A. BBS | B. Gopher | C. WWW | D. NEWS |
| (4) A. ECHO | B. WAIS | C. RLOGIN | D. Telnet |

3. 相对于 ISO/OSI 的 7 层参考模型中的低 4 层，TCP/IP 协议集中对应的层次有

(1)，它的传输层协议 TCP 提供(2)数据流传送，UDP 提供(3)数据流传送，它的互联网层协议 IP 提供(4)分组传输服务。

- (1) A. 传输层、互联网层、网络接口层和物理层

B. 传输层、互联网层、网络接口层

C. 传输层、互联网层、ATM 层和物理层

- D. 传输层、网络层、数据链路层和物理层
- (2) A. 面向连接的，不可靠的
B. 无连接的、不可靠的
C. 面向连接的、可靠的
D. 无连接的、可靠的
- (3) A. 无连接的
B. 面向连接的
C. 无连接的、不可靠的
D. 面向连接的、不可靠的
- (4) A. 面向连接的、保证服务质量的
B. 无连接的、保证服务质量的
C. 面向连接的、不保证服务质量的
D. 无连接的，不保证服务质量的
4. TCP/IP 协议的体系结构分为应用层、传输层、网络互联层和_____（1）。其中传输层协议有 TCP 和 _____（2）。
- (1) A. 会话层 B. 网络接口层 C. 数据链路层 D. 物理层
- (2) A. ICMP B. UDP C. FTP D. EGP
5. TCP/IP 网络的体系结构分为应用层、传输层、网络互联层和网络接口层。属于传输层协议的是_____。
- A. TCP 和 ICMP B. IP 和 FTP C. TCP 和 UDP D. ICMP 和 UDP
6. 在 WWW 服务器与客户机之间发送和接收 HTML 文档时，使用的协议是_____。
- A. FTP B. GOPHER C. HTTP D. NNTP
7. 下面关于 ICMP 协议的描述中，正确的是_____。
- A. ICMP 协议根据 MAC 地址查找对应的 IP 地址
B. ICMP 协议把公网的 IP 地址转换为私网的 IP 地址
C. ICMP 协议用于控制数据包传送中的差错情况
D. ICMP 协议集中管理网络中的 IP 地址分配
8. 下面关于 ARP 协议的描述中，正确的是_____。
- A. ARP 报文封装在 IP 数据包中传送
B. ARP 协议实现域名到 IP 地址的转换
C. ARP 协议根据 IP 地址获取对应的 MAC 地址
D. ARP 协议是一种路由协议
9. 在使用路由器的 TCP/IP 网络中，两主机通过一路由器互连，提供主机 A 和主机 B 应用层之间通信的层是_____（1），提供计算机之间通信的层是_____（2），具有 IP 层和网络接口层的设备_____（3）；在主机 A 与路由器 R 和路由器 R 与主机 B 使用不同物理网络的情况下，主机 A 和路由器 R 之间传送的数据帧与路由器 R 和主机 B 之间传送的数据帧_____（4），主机 A 与路由器 R 之间传送的 IP 数据包和路由器 R 与主机 B 之间传送的 IP 数据包_____（5）。

- (1) A. 应用层
B. 传输层
C. IP 层
D. 网络接口层
- (2) A. 应用层
B. 传输层
C. IP 层
D. 网络接口层
- (3) A. 包括主机 A、B 和路由器 R
B. 仅有主机 A、B
C. 仅有路由器 R
D. 也应具有应用层和传输层
- (4) A. 是不同的
B. 是相同的
C. 有相同的 MAC 地址
D. 有相同的介质访问控制方法
- (5) A. 是不同的
B. 是相同的
C. 有不同的 IP 地址
D. 有不同的路由选择协议
10. 在 TCP/IP 网络中，为各种公共服务保留的端口号范围是_____。
A. 1~255
B. 1~1023
C. 1~1024
D. 1~65535
11. 下面关于 ICMP 协议的描述中，正确的是_____。
A. ICMP 协议根据 MAC 地址查找对应的 IP 地址
B. ICMP 协议把公网的 IP 地址转换为私网的 IP 地址
C. ICMP 协议根据网络通信的情况把控制报文传送给发送方主机
D. ICMP 协议集中管理网络中的 IP 地址分配
12. 下面信息中_____包含在 TCP 头中而不包含在 UDP 头中。
A. 目标端口号
B. 顺序号
C. 发送端口号
D. 校验和
13. 某校园网用户无法访问外部站点 210.102.58.74，管理人员在 Windows 操作系统下
可以使用_____判断故障发生在校园网内还是校园网外。

- A. ping 210.102.58.74
- B. pathping 210.102.58.74
- C. netstat 210.102.58.74
- D. arp 210.102.58.74

14. ARP 协议的作用是____(1)， ARP 报文封装在____(2) 中传送。

- (1) A. 由 IP 地址查找对应的 MAC 地址
 - B. 由 MAC 地址查找对应的 IP 地址
 - C. 由 IP 地址查找对应的端口号
 - D. 由 MAC 地址查找对应的端口号
- (2) A. 以太帧
 - B. IP 数据包
 - C. UDP 报文
 - D. TCP 报文

15. 关于 Windows 防火墙的作用，描述正确的有_____。

- A. Windows 防火墙能够阻止进入计算机的流量
- B. Windows 防火墙能够控制出计算机的流量
- C. Windows 防火墙能够阻止木马产生的网络流量
- D. Windows 防火墙能够打开某些端口

16. 关于 Windows 上设置 IPSec，其功能描述正确的有_____。

- A. IPSec 只能限制出去的流量
- B. IPSec 只能限制进入计算机的流量
- C. IPSec 只能严格限制出入计算机的流量
- D. IPSec 能够基于端口和 IP 地址进行控制

习题答案

1. (1) C (2) A (3) A (4) C (5) D
2. (1) A (2) D (3) C (4) D
3. (1) B (2) C (3) C (4) D
4. (1) B (2) B
5. C
6. C
7. C
8. C
9. (1) B (2) C (3) A (4) A (5) B
10. B
11. C
12. B
13. B
14. (1) A (2) A
15. A、D
16. C、D

