

前言

随着互联网走进千家万户，计算机网络技术已经渗透到人们日常生活的方方面面，人们对网络技术的渴求日渐高涨犹如当年对 PC 技术的需求。本书是在《计算机网络技术基础》课程的理论上，培养学生对原理的理解，以及培养和增强学生的动手实践能力、综合运用网络知识的能力，通过实验能够搭建及管理一个小型的企业网。

本书的实验偏重于计算机网络技术基础，适合非计算机专业，对网络技术感兴趣的学生。本书共设计了七个基本实验。

实验一 网络基本概念，通过本次实验学生初步认识网络的相关概念；熟练掌握 Windows 环境下网络配置及查看的方法以及一些基本的网络检测命令。

实验二 Windows 环境下用户配置及管理，通过本次实验学生能够掌握 Windows 环境下用户和组的建立和管理方法；熟悉 Windows 环境下资源共享的方法。

实验三 简单局域网的实现，通过本次实验学生能够掌握局域网中的计算机之间的组网技术；含有线网和无线网；交换机的 VLAN 划分；了解物理连接与协议绑定之间的关系。

实验四 基于路由器的广域网的实现，通过本次实验学生能够掌握路由、路由器、路由表的相关概念；理解路由表的含义，掌握路由表配置方法，理解广域网的实现方法。

实验五 DNS 服务的实现，通过本次实验学生能够掌握域名解析服务的工作原理及配置方法。

实验六 站点的架构技术，通过本次实验学生能够掌握 Web 站点和 FTP 站点的基本架构技术，掌握虚拟主机和虚拟目录的概念。

实验七 小型网络上网服务的实现，通过本次实验学生能够为自己办公的网络环境中实现所有人都通过一台电脑上网，实现资源共享。

本书明确提出对学生的预习要求，避免学生做实验前一头雾水，不知从何做起。

感谢对我们工作给予大力支持的胡振山老师，也感谢在这门课程担任助教的曹林、王博、李婵娥、付殷、魏天宇等同学，以及参与相关 SRT 项目的张挺阳、侯凌云、黄伟德、沈力、安之等同学。

由于作者的水平有限，以及时间比较仓促，书中难免存在错误和不妥之处，欢迎广大读者批评指正。

编著者

2019 年 3 月

目录

实验须知.....	3
实验一 网络基本概念	4
实验二 WINDOWS 环境下用户配置及管理	10
实验三 简单局域网的实现	16
实验四 基于路由器的广域网实现.....	21
选做实验一 交换机 VLAN 的实现	27
实验五 DNS 服务的实现.....	30
实验六 站点的架构技术.....	36
实验七 小型网络上网服务的实现	41
选做实验二 代理服务的实现	48
附录一：IPV4 地址.....	53
附录二：网络配置方法	58
附录三：常用的 DOS 命令	61
附录四：SNIFFER PRO 软件	66
附录五：WINDOWS 环境下的用户配置和管理.....	73
附录六：双绞线及 EIA/TIA-568 标准.....	76
附录七：网线制作.....	78
附录八、如何读懂路由表.....	80

实验须知

一、预习要求

- 1、实验前认真阅读实验教程中的有关内容，明确实验目的和实验任务。
- 2、每次实验前应有预习报告，预习报告的目的是为了做实验有备而来。内容不要求写太多，包括实验的简单步骤，实验的重点，需要注意的地方，实验中的问题思考等。对于问题思考，预习中能回答的问题，回答在报告中，不能回答的做上记号，实验中回答。实验前检查预习报告，实验完成时，交预习报告，未预习者不许参加实验，抄实验指导书的预习不合格。

二、实验要求

- 1、实验是学习这门课程的重要环节，实验课请勿迟到，缺席。
- 2、爱护实验设备，保护环境清洁，不要随意更换实验设备。
- 3、认真完成实验任务，实验结果经教师检查，认真回答教师提出的问题
- 4、实验多数情况为两人一组，希望两个同学能够互相配合，有合作意识。
- 5、出现问题，认真思考，首先从底层开始查找，即先看物理连接有无问题，协议绑定关系是否正确，最后查找应用层的问题。实验过程中要求首先自己排查问题，养成独立解决问题的能力，对于解决不了的问题，通过其他同学和老师一起来解决。
- 6、实验完毕整理实验设备离开实验室。

三、报告要求

每次实验完成后提交实验报告，报告内容如下：

- 1、实验名称，实验人姓名、学号、班级、座位号。
- 2、实验目的、任务、内容。
- 3、记录和分析实验结果。
- 4、回答实验指导书中给出的问题思考。
- 5、自己在实验过程中遇到的问题及思考以及解决方法。
- 6、认真做小结。

实验一 网络基本概念

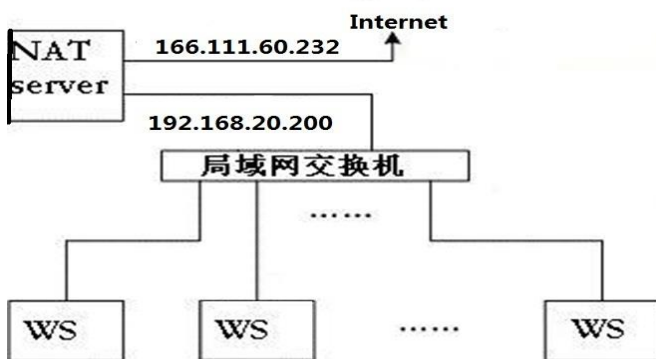
一. 实验目的

- 1、初步了解计算机网络的相关概念
- 2、熟练掌握 Windows 环境下网络配置方法
- 3、了解基本的网络命令及功能，并能够检测基本的网络问题
- 4、了解网络管理诊断软件 Sniffer pro 的简单操作。

二. 预习要求

自学实验指示书附录一至附录四中给出的相关理论知识及配置方法。重点是附录一中子网掩码的意义，附录三中 ipconfig 命令、ping 命令、nslookup 命令、tracert 命令、arp 命令。

三. 实验环境



西主楼1-215网络拓扑结构图

实验室的网络拓扑结构图如上图所示，教师机作为服务器，有两块网卡，一个网卡通过实验室交换机和每台学生机相连，另一块网卡连接校园网。实验过程每个同学自己一组，开机启动进入 Windows 2012 server。

四. 实验内容

1. 完成 Windows 环境下本地网络的配置；
设置 IP 地址、子网掩码、网关、首选 DNS 服务器、备用 DNS 服务器，了解各部分的含义。使用 ipconfig、ping、nslookup 等命令进行测试分析。
2. 熟悉常用的网络命令，如：tracert、arp、route、net、netstat 等命令。
3. DHCP 客户端的应用。
4. 利用 Sniffer pro 软件完成简单的网络诊断任务（选做）。

五. 实验步骤



(一) 本地网络配置

网络地址设置及测试

1、了解子网掩码的作用以及网段的概念。

a) 设置 IP 地址的子网掩码

根据附录一中给出的 Internet IP 地址分类原则, 实验室局域网采用 192.168.20.200+* (其中*为实验桌号) (子网掩码 255.255.255.0) 网段。参考附录二给出的配置方法, 选择正确的 IP 地址、子网掩码, 完成本地 IP 地址设置。**注意: 此时网关和 DNS 为空。**

设置方法: 点击“开始”→“控制面板”→“网络和 Internet”, 下面的“查看网络状态和任务”, 在出现的窗口左侧的“更改适配器设置”处单击, 弹出“网络连接窗口”, 此时显示本地连接和本地连接 2。或者在“状态栏”中找到“”也有的是“”图标, 右键或者左键都可以找到“打开网络和共享中心”→双击“以太网”→找到所用的网卡, 进行网络设置。

注意: 只设 IP 地址和子网掩码, 其它的网关和 DNS 均不设置。如果有多个网卡, 把其它网卡的网关和 DNS 设置也去掉。

b). 确认设置的 IP 地址是否生效

点击“开始”→“所有程序”→“附件”→“命令提示符”, 或者在键盘上用快捷键 win+R 打开运行, 输入 cmd 后, 回车, 进入命令行窗口, 调用 ipconfig 命令 (使用方法参见附录三, 下同), 查看本地 IP 地址的实际设置情况与窗口设置是否一直, 不一致时查找原因。(是否点击“确定”以及关闭设置的窗口)。

注意: 当在命令行中显示的地址和在网络连接属性设置时的地址不一致时, 确认是否点击“确定”以及关闭设置的窗口; 或者先禁用网卡, 然后再重新启用, 之后再用 ipconfig 命令查看地址。

C) 连通性测试。

在命令行窗口中, 使用 ping 命令测试本机同实验室网关服务器 (192.168.20.200)、相邻计算机的连接情况, 观察并记录测试结果。

注: 以前输入过的命令, 如 ipconfig、ping 192.168.20.200 等, 我们希望重复之前用过的命令, 不需一个字母一个字母再次输入, 可以在键盘上按下 F7, 即可看到之前输入过的命令, 用数字或者方向键选择相应的命令即可快速的输入。也可以用小键盘的“↑”“↓”找到需要的命令。

ping 命令测试本机与电机系网关服务器 166.111.60.1、DNS 服务器 166.111.8.28 的测试情况, 并记录测试结果。

ping 命令测试本机与未知 IP (192.168.2.1) 的连接, 观察并记录测试结果; 体会以上三种情况的测试结果有何不同。

2、网关的作用

《计算机网络技术基础》实验指导书

网卡的 IPv4 添加网关 192.168.20.200 之后, ping 命令测试本机与电机系网关服务器 166.111.60.1、DNS 服务器 166.111.8.28 的连通情况, 并记录测试结果。ping 命令测试本机与 192.168.2.1 的连通情况, 观察并记录测试结果。理解网关的作用。

结合实验记录和附录中的理论知识, 分析总结 IP 地址, 子网掩码, 网关各自在计算机进行网络通信中所扮演的角色, 分析 2 台计算机通过交换机和路由器连接需要注意哪些问题。

3、网线的通断判断

拔出网线, 注意观察和网线连通时图标有何不同。观察并记录结果。

DNS(Domain Name System, 域名系统)相关实验内容

1. 在上面没设 DNS 服务器的基础上, 命令行窗口下, ping info.tsinghua.edu.cn, 观察并记录测试结果;

2. 参见附录二, 将本机的 DNS 服务器 IP 地址设置为清华大学 DNS 服务器 166.111.8.28。再次 ping info.tsinghua.edu.cn, 观察并记录测试结果。

3. 在命令行窗口下, 使用 nslookup 命令, 查看以下域名对应的 IP 地址。分别对校园网站点(如 www.tsinghua.edu.cn)、教育网站点(如 www.pku.edu.cn)、公众网站点(如 www.sohu.com, www.microsoft.com)等你所感兴趣的域名进行域名解析, 记录实验结果。选择本机、邻近计算机、校内服务器等的 IP 地址, 尝试查找其是否有对应的域名, 记录实验结果, 分析原因, 体会域名和 IP 地址的对应关系。

注: 在命令行窗口下, 使用 ipconfig /displaydns 命令查看本机 DNS 解析缓存表。ipconfig /flushdns 可以清除本机 DNS 解析缓存表。

4. 设置为未提供 DNS 服务的主机地址(如 192.168.20.200), ping info.tsinghua.edu.cn 的结果又如何? 观察 DNS 服务器设置错误时的情况。

5、在有无 DNS 服务器的不同情况下, 分别在浏览器中访问清华大学主页 www.tsinghua.edu.cn, 观察、记录结果, 并对结果进行分析。

结合实验现象, 总结分析检查本地 DNS 设置是否正确的方法, 理解 DNS 服务对计算机访问网络的影响。

网络常用命令

1. Tracert(跟踪路由)是路由跟踪命令, 用于确定 IP 数据包访问目标所采取的路径。tracert 命令可以确定数据包在网络上的停止位置。在命令行窗口中, 使用 tracert 命令查看本机与邻近计算机、实验室网关服务器(192.168.20.200)、服务器(166.111.60.232)、校园网某主机(166.111.4.100 等)、公众网某主机(www.baidu.com 等)的通信情况, 观察并记录结果。

2. 在 TCP 网络环境下, IP 数据包在网络中的流向是靠路由表的定义来决定的。当 IP 数据包到达某网络后, 由哪台机器来响应这个 IP 数据包却是靠该 IP 数据包中所包含的 MAC 地址来识别。也就是说, 只有机器的 MAC 地址和该 IP 包中的 MAC 地址相同的机器才会应答这个 IP 数据包。在每台主机的内存中, 都有一个 IP 地址和 MAC 地址的

《计算机网络技术基础》实验指导书

转换表，俗称 ARP 表。ARP 协议（Address Resolution Protocol）是将 IP 转化为相对应的网卡的物理地址的一种协议，也可以说 ARP 协议是将 IP 地址转化成 MAC 地址的一种协议。它依靠内存中保存的一张表来使 IP 地址能够在网络上被目标计算机所应答。在命令行窗口中，使用 arp 命令查看本机当前的 IP 地址与 MAC 地址转换表，如何添加和删除 arp 列表并通过使用 ping 命令查看相邻计算机的通讯情况，观察现象，做好实验记录，并进行分析。

3. 当一台计算机同局域网中多个网段的计算机通信，可以在一个网卡上绑定多个 IP 地址，换言之局域网中对应的多个网段的计算机可以访问你的计算机，这样方便资源的共享。参考附录二中的方法，为本地配置多个网络地址，尝试与各网络地址所在子网的计算机进行通信。一个网卡绑定 2 个 IP 地址，在 IP 设置的高级中添加另外一个地址应与之前的 IP 地址不在同一网段（如 192.168.2.*），想想为什么？测试与网关服务器的连接情况；以及与相邻计算机的连接状况，观察并记录测试结果。

DHCP 客户端设置

1、自动获取 IP 地址

根据附录二提供的方法，配置计算机进行网络地址的自动获取，查看计算机自动获得 IP 地址的情况，并检查计算机与网络的连通性。

2、关闭 DHCP Client 服务。

由“开始”→“管理工具”→“服务”，在出现的控制台窗口找到“DHCP Client”。默认情况下此服务“已开启”，可以人工“停止”。如果人工设置 IP 地址不需要“自动获取”，可以把启动类型改为“禁用”以提高系统启动速度。

3、打开 DHCP Client 服务并自动获取 IP 地址。

方法类似“关闭 DHCP Client 服务”

结合附录一中的相关内容，分析实验现象并给出结论。

(二) Sniffer pro 软件的简单使用（选做）

参考附录四，初步学会使用 Sniffer Pro 软件的操作界面和主要功能。

1. 尝试监听所在网络的通信情况。

2. 使用 Sniffer pro 软件捕获通信数据，尝试对其进行分析，记录比较不同协议的数据结构特点，如源地址、目的地址等；

3. 修改捕获条件，查看源地址为本机或某特定计算机的报文，分析 IP 协议和 ARP 协议数据内容。

六. 实验说明

(一) 网络概念介绍

1、IP 地址、子网掩码和网关三者之间的关系

①计算机与同一网段其它主机进行通信时，必须要有 IP 地址和子网掩码。IP 地址和子网掩码共同决定计算机所在的网段号和主机号。（参看附录一 IPv4 协议）

②计算机与不同网段的主机进行通信，需要有网关。网关实现各网段之间的通信，如同桥梁。

③计算机访问某一网站，首先要把网站的域名解析成对应的 IP 地址，这就需要有 DNS 服务器帮忙。

④IP 唯一性，指的是公网 IP。私网 IP 可以重复，也就是说两个不同的局域网，可以有相同的 IP 地址存在，但同一个局域网里不允许有二个相同的 IP 地址存在。

2、DNS 概念

DNS 是计算机域名系统 (Domain Name System 或 Domain Name Service) 的缩写，它是由解析器和域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名和对应 IP 地址，并具有将域名转换为 IP 地址功能的服务器。域名解析是指将域名映射为 IP 地址的过程。域名必须对应一个 IP 地址，而 IP 地址不一定有域名。

当用户在应用程序中输入域名时，DNS 服务器可以将此域名解析为与之相对应的 IP 地址。所以，你在上网时输入的网址，是通过域名解析系统解析找到相对应的 IP 地址，这样才能上网。

3、DHCP 概念

DHCP 是动态主机设置协议 (Dynamic Host Configuration Protocol) 的缩写，它是一个局域网的网络协议，使用 UDP 协议工作。它主要有两个用途：给内部网络或网络服务供应商自动分配 IP 地址，也是内部网络管理员作为对所有计算机作中央管理的手段。

(二) 网络体系结构和网络协议 (TCP/IP 协议模型)

Internet 协议/ 传输控制协议(TCP/IP)是行业标准协议套件，此协议是专为通过路由器相连的不同网段构成的大型网络设计的。它起源于美国国防部(DoD)高级研究计划局(DARPA)在 20 世纪 60 年代后期和 70 年代早期进行的研究。

TCP/IP 协议套件映射为 1 个被称作 DARPA 模型的 4 层概念模型。这 4 个层分别是：应用层、传输层、Internet 层和网络接口层。

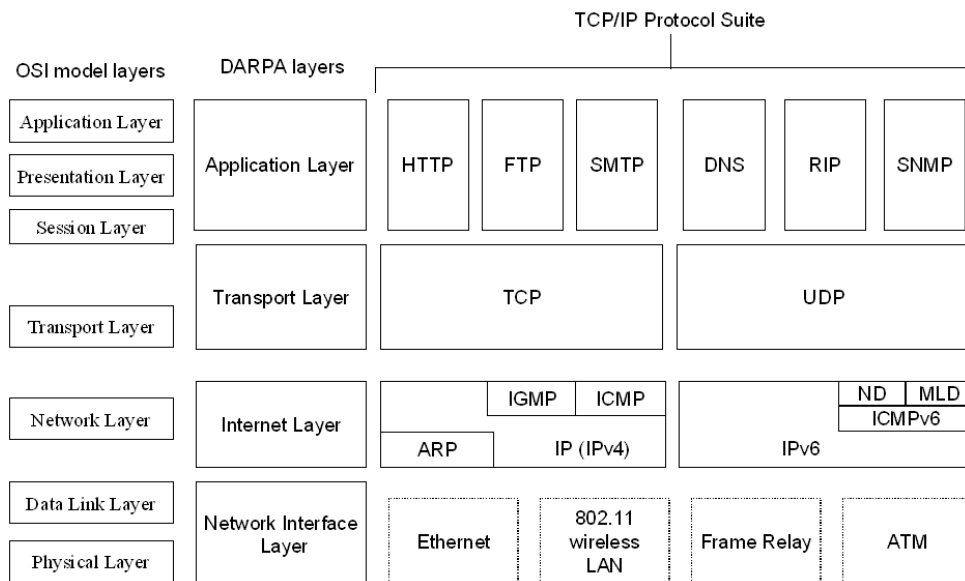


图 1-1 网络体系结构和网络协议示意图

实验二 Windows 环境下用户配置及管理

一. 实验目的

- 1、熟练掌握 Windows 环境下用户配置和管理的方法
2. 熟悉 Windows 操作系统，实现资源共享，掌握对本地及网络资源权限的管理。

二. 预习要求

预习附录五 windows 用户配置及管理，以及 Windows 环境下实现局域网中资源共享的方法（如：文件、打印机资源的共享）实验内容

三. 实验环境

两个同学一组，一台计算机作为服务器，另一台计算机作为客户机。两个同学协调合作，共同总结。

四. 实验内容

- 1.系统用户的配置和管理；
- 2.掌握 Windows 环境下 NTFS 格式文件系统的权限管理；
- 3.实现资源共享（文件、打印机），掌握资源服务器和客户端的配置方法。
- 4.TCP 端口 139、445、3389 的应用设置。

五. 实验步骤

（一）本地用户和组的配置和管理（此部分单独完成）

在充分理解附录五的基础上，完成下述实验内容：

1. 创建本地用户账号、更名和删除用户账号。

2012 server：由“开始”→“管理工具”→“计算机管理”→“本地用户和组” / 右键桌面的“计算机”→“管理”→“配置”→“本地用户和组”。

Win7：“开始”→“控制面板”→“系统和安全”→“管理工具”→“计算机管理”→“本地用户和组” / 右键桌面的“计算机”→“管理”→“本地用户和组”。

Win10：“开始”→“控制面板”→“用户账户”

修改本地用户的属性，留意各项设置所起的作用，如“用户下次登陆必须更改密码”、“用户已停用”等；

2. 创建本地组，并修改其属性；

3. 进行以下安全策略的设置和测试（由“开始”→“管理工具”→“本地安全策略”），设计测试方案，记录测试结果。

- ①分别设置用户及组的权限（如禁止某用户帐号在本地登录等）；

《计算机网络技术基础》实验指导书

②将用户帐号加入不同组中，测试并记录用户最终获得的权限；

③根据需要，自行进行其它设置和测试，注意记录实验结果。

注意：①用户和组的创建、更名、修改等的设置在“计算机管理”，用户和组的权限设置在“本地安全策略”

②**users** 组比较特殊，新建用户默认情况下都是 **users** 组成员。如果某用户 **userA** 仅是 **users** 组成员，则这个用户权限将较低，它不具有“关机”，“重启”，“修改系统时间”等权限。虽然权限有限，但不能从“**users** 组”中删除，如果把 **userA** 从 **users** 组中删除，注销原账户之后，**userA** 用户将不在登录选项中出现。

（二）资源的权限管理（此部分同组同学合作完成）

1、新建多个用户，将其加入多个不同的用户组中。

2、针对不同的系统用户或用户组，对具有 **NTFS** 文件格式的某一文件夹 / 文件进行“安全”属性的设置。

3、注销已登录的用户，用新建用户进行登录，在不同账户下打开之前设置过权限的文件夹，体会权限的限定，并做总结。

4、观察系统盘下的 **Windows** 文件夹以及 **Users** 文件夹的安全设置，体会 **Windows** 系统的用户权限设定，注意不能更改，避免系统崩溃。

5、共享文件夹的设置与管理。通过修改某文件夹“共享”权限可以将文件和文件夹设置为网络共享，并且不同用户在网络进行访问时所拥有的权限也不同。对于某一用户所属不同用户组分别设置不同“共享”权限，体会权限累积，包括拒绝策略的作用规律。

备注：①具备文件夹共享的用户必须是 **Administrator** 等内置组的成员；

②如果该文件夹位于 **NTFS** 分区，该用户必须对被设置的文件夹具备“读取”的 **NTFS** 权限。

方法一：找到要共享的文件夹，点击右键找到属性，在属性窗口的共享选项中设置“共享”和“高级共享”

方法二：在命令提示符下执行。例如，需要把驱动器 **F** 盘上 **software** 文件夹进行共享，共享名为 **tools**，可以键入：**net share tools=f:\software**；想删除前面共享的 **software** 文件夹的方法为：**net share tools /delete**；如果想查看本地计算机上有哪些共享资源可以键入 **net share**。

6、访问共享文件夹。当用户知道网络中某台计算机上有自己需要的共享信息，同时具有一定的访问权限时，就可以在自己的计算机上使用这些资源。实验过程中需注意 **guest** 用户的特殊性，**Guest** 帐户即所谓的来宾帐户，它可以访问计算机，但受到限制，同时 **Guest** 也为黑客入侵打开了方便之门。如果不需要用到 **Guest** 帐户，最好禁用它。需要说明的是：实验室的计算机是“克隆”出来的，所有实验用计算机中已有的用户名和密码都一样，实验时需新建用户，把所建的用户放入不同的组中。新建用户时可以分别采用以下四种情况：另一台计算机无此用户名；另一台计算机有此用户名但均没有设置密码；另计算机有此用户名且密码一致；另计算机有此用户名但密码不一致进行登录，体会不同情况下的结果有何不同，并做总结。

《计算机网络技术基础》实验指导书

方法一：“开始”→“运行”处输入被访问的计算机名

方法二：“开始”→“计算机”，在出现的窗口的地址栏输入被访问的计算机名

方法三：通过映射网络驱动器进行访问（“开始”→“计算机”，在出现的窗口找到“计算机”，右键“计算机”，出现“映射网络驱动器”）

方法四：在命令提示符下通过映射网络驱动器进行访问。如果把 IP 地址为 192.168.20.200 下的共享名为 tools 的目录映射为本地的 z 盘的方法是：

```
Net use z: \\192.168.20.200\tools "1-215" /user:administrator.
```

user:administrator 是 192.168.20.200 计算机的用户名，“1-215” 是密码。

思考题：了解“安全”权限和“共享”权限对某个账户限制时，只有用此账号访问本计算机时才能真正体会到权限设置的意义。体会“安全”和“共享”权限合适有效，当某一个文件夹“共享”权限和自身的“安全”权限不一致时，Windows 操作系统是如何确定用户的最终访问权限？

（三）安装和配置网络打印服务

打印机是我们常用的计算机输出设备，打印机共享也就是平常说的局域网内的网络打印机。如何让局域网中其他用户也可方便的使用同一台打印机，实现打印机共享，从而实现资源共享，充分的发挥了硬件的利用率。微软操作系统对打印机共享提供了友好的支持，局域网内（比如一个办公室），只要其中一台机器装了打印机。而且启用了打印机共享，那么其他用户只需要添加一下网络打印机，就可以直接打印。

本地连有打印机的同学作为服务器，安装本地打印机，打印成功后共享。

本地没打印机的同学作为客户端需要知道共享打印机所在的计算机，以及用户名，密码，通过网络链接找到共享的打印机。双击后会提示在本地安装打印驱动程序，安装成功，就可以像本地打印机一样进行打印。也可以在找到共享打印机之后，像安装本地打印机一样安装网络打印机。方法是：点击“开始”→“设备和打印机”，在弹出的窗口右上角点击“添加打印机”，选择“添加网络、无线或 Bluetooth 打印机”，此时会搜索网络中的打印机，点击右侧的“停止”。在“按名称选择共享打印机”下输入类似访问共享资源的方式（如：\\computer_name\printer），按照提示安装好网络打印机。

注意：

提供网络打印服务的同学，需要在共享前测试打印机性能，即打印测试页，并在测试通过后再将打印机进行共享。对于共享的各项配置，如名称等，需要及时向作为打印客户的同学通报。

作为打印客户的同学不用打印测试页，仅需通过打印简单文本证明服务配置成功即可。

（四）、TCP 端口 139、445、3389

2017-04-15 校信息化工作办公室发布“关于校园网出口封禁 TCP 端口 139、445、3389

《计算机网络技术基础》实验指导书

的通知”内容如下：

“由于近期有黑客组织放出针对于 windows 操作系统的攻击代码，使得 windows 操作系统面临入侵风险，被攻击的结果可能导致 windows 操作系统重要文件被修改，威胁等级较高。

基于上述原因，为防止校园网内部主机受到外部攻击，校园网出口将暂时封禁 TCP 协议 139 端口、445 端口、3389 端口的入校访问。

禁解除时间另行通知。”

下面我们认识一下这些端口的功能，以及如何封禁这些端口。

139 端口是一种 TCP 端口，该端口专门用于 NETBIOS 与 TCP/IP 之间的通信，系统使用固定的端口号，不能手动改变。也就是在通过网上邻居访问局域网中的共享文件或共享打印机时发挥作用。

关闭 139 端口方法：

win xp 以前版本：右点-本地连接-属性，点击 internet 协议/(TCP/IP)，接着点下面的属性，找到 NETBIOS 设置，把默认改到禁用 TCP/IP 上的 NETBIOS，确定即可。

Win7 以后版本：在“服务”中找到“TCP NetBIOS helper”之后“禁用”

445 端口也是一种 TCP 端口，该端口也在你通过网络访问局域网中的共享文件或共享打印机时发挥作用。但该端口基于 SMB(Server Message Block)Windows 协议族，用于文件和打印共享服务。

关闭 445 端口方法：右击-网上邻居-属性/本地连接 -属性，在 microsoft 网络客户端前的小勾去掉。

3389 端口是远程桌面的服务端口，通过这个端口，用“远程桌面”等连接工具来连接到远程的服务器，如果连接上了，输入系统管理员的用户名和密码后，将变得可以像操作本机一样操作远程的电脑，因此远程服务器一般都把这个端口修改数值或者关闭。默认状态下系统是关闭这个端口的。

用户远程桌面链接到另一台计算机的方法：

1、在计算机 A 上启用远程桌面

以管理员身份登录计算机 A，打开系统属性对话框，在“系统属性”对话框的“远程”选项卡中，选中“允许远程连接到此计算机”复选框。

2、在计算机 A 上给 userA 授予远程桌面连接权限。

以管理员身份登录计算机 A，建立 userA 用户，在“属性”对话框的“隶属于”选项卡，点击“添加”按钮，在弹出的“选择组”对话框中点击“高级”按钮，在“选择组”对话框中点击“立即查找”按钮，在“搜索结果”里找到“Remote Desktop Users”，然后确定，完成账户属性设置。

3、在计算机 B 上测试远程桌面连接

在“开始”菜单的“运行”命令对话框中输入“mstsc”，确定之后，出现“远程桌

《计算机网络技术基础》实验指导书

面连接”对话框，输入计算机 A 的名称或者 IP 地址，之后单击“连接”按钮。在“输入你的凭据”对话框输入 userA 和密码，为方便下次登录操作可以选择“记住我的凭据”复选框，单击“确定”。当远程桌面连接成功，可以看到计算机 A 的桌面。

关闭 3389 端口方法：开始-->设置-->控制面板-->管理工具-->服务里找到 Terminal Services 服务项，选中属性选项将启动类型改成手动，并停止该服务。

随着网络的普及，网络安全越来越得到大家的关心与重视，因为其中涉及到个人隐私和资金安全。在默认情况下计算机有些端口是开放的，这就给网络黑客创造了入侵机会。为了避免不必要的麻烦，提高网络安全，建议将一些不必要的端口关闭，减少隐患。

在 windows 命令行窗口下可以利用 netstat 显示协议统计信息和当前 TCP/IP 网络连接，tasklist 显示在本地或远程机器上当前运行的进程列表，使用 taskkill 工具按照进程 ID (PID) 或映像名称终止任务。命令用法可在命令后加 ‘/?’ 寻求帮助

1. 查看所有的端口占用情况 C:\>netstat -ano

活动连接

协议	本地地址	外部地址	状态	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	472
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	728
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	904
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	912
TCP	127.0.0.1:63209	127.0.0.1:63210	ESTABLISHED	9560
TCP	127.0.0.1:63210	127.0.0.1:63209	ESTABLISHED	9560
TCP	127.0.0.1:63211	127.0.0.1:63212	ESTABLISHED	9560
TCP	127.0.0.1:63212	127.0.0.1:63211	ESTABLISHED	9560
TCP	166.111.61.200:139	0.0.0.0:0	LISTENING	4
TCP	166.111.61.200:60776	166.111.8.28:53	TIME_WAIT	0

.....

2. 查看 PID 对应的进程 C:\>tasklist

映像名称	PID	会话名	会话#	内存使用
System Idle Process	0	Services	0	4 K
System	4	Services	0	5,456 K
wininit.exe	728	Services	0	3,532 K
services.exe	904	Services	0	5,684 K
lsass.exe	912	Services	0	52,632 K
svchost.exe	472	Services	0	11,660 K
svchost.exe	1356	Services	0	39,188 K

...

六. 实验说明

（一）什么是共享文件夹？

将存储在本地计算机上的文件夹共享，以让网络中的其它用户能够访问，这种文件夹叫共享文件夹。

共享文件夹的优点是方便、快捷；和其它存储介质（软盘、光盘）相比，不受文件数量和大小限制。

（二）共享权限和安全权限

共享的权限只能控制网络访问，不能控制本机访问，适合任何分区，但权限的种类少。

NTFS 安全权限对本机和网络访问都能控制，权限种类多，适合精确控制。

实验三 简单局域网的实现

一. 实验目的

1. 掌握局域网各种组网技术;
2. 掌握基本的网络扩展方式;
3. 了解物理连接与协议绑定的关系;
4. 掌握普通网线和级连网线的制作;

二. 预习要求

看实验说明, 自学实验指示书附录六至附录七中给出的相关知识, 了解网线的制作方法; 上网查找相关资料, 了解交换机和 HUB 的区别。

通过本次实验学生能够掌握局域网中的计算机之间的组网技术; 含有线网和无线网; 交换机的 VLAN 划分; 了解物理连接与协议绑定之间的关系。

三. 实验环境

实验方式

相邻两个同学一组, 每组 2 台计算机, 操作系统 Windows, 网卡选用非板载网卡。设备清单: 每组 8 口集线器 1 台、带交换机功能的小型路由器各 1 台、普通网线 2 根、级连网线 1 根。每行同学共享: 网络测试仪 1 台。

四. 实验内容

1. 通过级连网线, 实现两台计算机之间的相互通信;
2. 利用集线器和交换机构成简单局域网;
3. 利用集线器和交换机级连, 进一步扩展网络规模;
4. 利用无线实现两台计算机的互连 (选作);

五. 实验步骤

(一) 利用网线直接连接两台计算机

- 1、用测试仪对网线进行测试, 找出普通网线和级联网线, 并确保网线正常。
- 2、通过级联网线连接两台计算机的非板载网卡。
- 3、分别在各自操作系统中, 对通信用物理设备——网卡进行相关协议设置, 确保满足通信要求。
- 4、在各自操作系统中, 利用各种网络测试命令测试网络连通状态, 如 ping 对方 ip 地址等等, 最终实现两台计算机通过级联网线进行通信。

注意：第 3、4 步中涉及的相关配置方法可参见实验一附录。

（二）简单局域网的组网

1、选用 HUB 实现简单局域网的扩展

级联口主要用于连接其它集线器或网络设备。比如我们在组网时，集线器的端口数量不够，可以通过级联口将两个或多个集线器级联起来，达到拓展端口的目的。级联口一般标有"UPLINK"或"MDI"等标志。在级联时，我们可以通过直连线将集线器的级联口与另一台集线器的 RJ-45 接口连接起来，从而组建更大的网络。(注：一端为级联口，另一端为普通口，连线为直连线。当使用两个普通口级联时，应使用交叉线)

(1)选择 2 根普通网线将两台计算机的非板载网卡通过集线器的普通端口组成局域网。

(2)更换其中的 1 根普通网线为级联网线，连接到其中一台计算机的非板载网卡，这时 HUB 侧的端口又该如何选择。

(3)将简单局域网扩展至两组或多组，如图 3-1~图 3-3 所示。尝试采用不同类型的网线，进行简单局域网的扩展。**注意**此时网线的选择和 HUB 端口的选择。

(4)根据实验二中介绍的方法在简单局域网中设置文件共享。

(5)通过文件夹共享，在两台电脑之间拷贝文件，比较文件传输速度（注意：由于传输速度较快，文件相对较小，又可能感觉不到不同的拓扑结构对传输速度的影响）。

(6)几台电脑之间同时进行多个文件拷贝操作，比较文件传输速度。

思考：①不同的设备连接在 HUB 普通口和级联口上需要不同的网线，尝试给出所有可能的连接方式。

②当两台电脑之间存在多个网络连接时，数据传输通过哪一个网络连接进行？文件传输速度与网卡/网线的标称传输速度相差多少？当同一个网络当中有多个数据传输同时进行，整个网络的带宽是如何分配的？

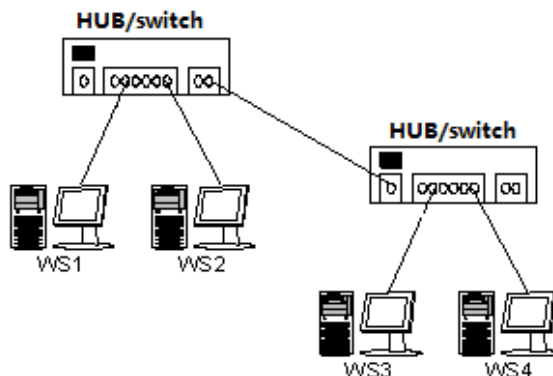


图 3-1 利用集线器 / 交换机实现两组计算机互联示意图

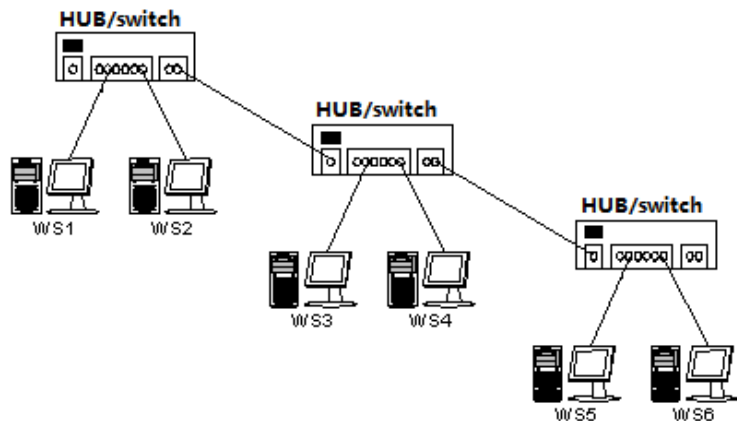


图 3-2 利用集线器 / 交换机实现多组计算机串联示意图

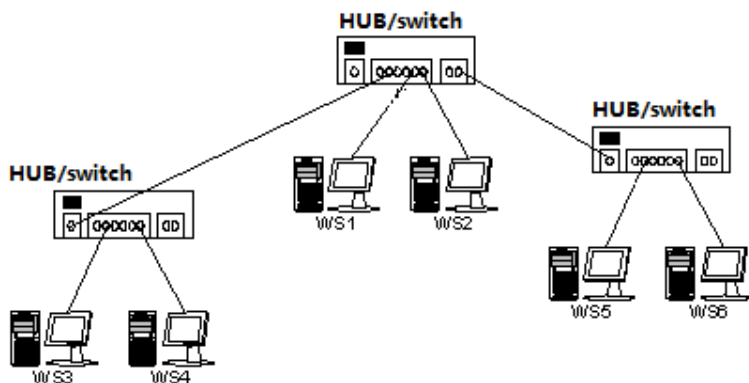


图 3-3 利用集线器 / 交换机实现多组计算机并联示意图

2、选用交换机实现简单局域网的组建

(1)选择 2 根普通网线将两台计算机的非板载网卡通过交换机组成局域网，注意交换机是否有端口的选择。

(2)更换其中的 1 根普通网线为级联网线，这时两台计算机是否能够正常通讯。

(3)将简单局域网扩展至两组或多组，拓扑结构如图 3-1~图 3-3 所示。尝试采用不同类型的网线，进行简单局域网的扩展。**注意**此时网线的选择和交换机端口的选择是否有关系。

(4)与 HUB 类似，进行文件共享操作，并比较文件传输速度

(三) 通过无线连接两台计算机（选作）

1、设置无线网关。

查看路由器的 IP，计算机的网卡设置为和路由器在同一网段，连接网卡的路由器的内网，在地址栏中输入路由器的 IP 地址，在提示的用户名和密码处输入路由器上标识的用户名和密码。如果连接不上，长按路由器上的“Reset”键大概 10 秒，系统自动回复出厂设置，重新连接即可。

《计算机网络技术基础》实验指导书

进入设置界面，找到“DHCP 服务”配置为“启用”DHCP 服务器，设置地址池开始地址，结束地址，地址租期，网关，主 DNS 服务器，备用 DNS 服务器等，配置完成进行保存。

2、连接网络

两台计算机都设置为自动获取 IP 地址，在命令提示符下查看计算机的 IP 地址，共享文件夹，传输文件，比较文件传输速度。

手机连网，在浏览器窗口输入共享计算机的 IP 地址或名称。查看共享文件夹内容，复制文件，比较文件传输速度。

六．实验说明

（一）正线和反线

观察平时使用的网线，你会发现网线的两个端头，即 RJ-45 头内有 8 根细线，且细线的颜色两两各不相同。根据排列顺序的不同（从左到右）可分为如下两种：

EIA/TIA 568A 标准：白绿 / 绿 / 白橙 / 蓝 / 白蓝 / 橙 / 白棕 / 棕；

EIA/TIA 568B 标准：白橙 / 橙 / 白绿 / 蓝 / 白蓝 / 绿 / 白棕 / 棕；

如果一根网线的两端采用相同标准（如均为 A 标准或均为 B 标准），则称之为正线，如果网线的两端采用不同的标准（一头 A 标准，另一头 B 标准），则称之为反线，又叫做级联线。

不同设备之间网线的选用，使用规则如下表所示：

网线的用途	网线种类
计算机 \longleftrightarrow 计算机	反线
计算机 \longleftrightarrow HUB（普通口）	正线
计算机 \longleftrightarrow HUB（UPLINK 口）	反线
计算机 \longleftrightarrow 交换机	正线/反线
HUB（普通口） \longleftrightarrow HUB（普通口）	反线
HUB（普通口） \longleftrightarrow HUB（UPLINK 口）	正线
HUB（普通口） \longleftrightarrow 交换机	正线/反线
HUB（UPLINK 口） \longleftrightarrow 交换机	正线/反线
交换机 \longleftrightarrow 交换机	正线/反线

（二）集线器、交换机和路由器

集线器（Hub），交换机（Switch），路由器（Router）是常用的网络设备。

集线器又称集中器，是多口的中继器。工作在 OSI 模型的第一层，即物理层。它将所有节点集中在以它为中心的节点上，同时对接收到的信号进行再生整形放大，以扩大网络的传输距离。采用“广播”的方式发送数据，不具备地址识别功能。

交换机（又名交换式集线器）工作在 OSI 模型的第二层，即数据链路层，完成数据帧的封装转发，能够识别和“学习”MAC 地址。

交换机和集线器的主要区别是：集线器采用共享带宽的工作方式，而交换机是独享带

《计算机网络技术基础》实验指导书

宽。所以当网络中有多台计算机时，为了保证每台计算机的带宽，应优先选择交换机。

路由器（Router）工作在 OSI 模型的网络层，主要作用连接不同网络的枢纽，选择最佳信息传送线路。和交换机相比，路由器利用 IP 地址识别目的主机，能够分割广播域，实现类似防火墙的功能。

简单来说，交换机是在集线器的基础上产生的，而路由器又是在交换机的基础上发展的。

实验四 基于路由器的广域网实现

一. 实验目的

- 1、掌握路由、路由器、路由表等概念；
- 2、掌握路由表配置；
- 3、理解广域网的实现方法。

二. 预习要求

自学实验指示书附录八中给出的相关知识，能够读懂路由表。下表是某个同学设置的某台路由器的路由表，请你分析每条路由表。

Destination IP	LAN	Subnet Mask	Default Gateway	Hop Count	Interface
0.0.0.0.		0.0.0.0	192.168..3.2	1	Internet
192.168.1.0		255.255.255.0	192.168..2.2	0	Local
192.168.2.0		255.255.255.0	0.0.0.0	1	Local
192.168.3.0		255.255.255.0	0.0.0.0	1	Internet

请在实验前自行设计 1 台路由器连接 2 个子网及 2 台路由器连接 3 个子网中各个路由器每一端口及各个主机的 IP 地址、子网掩码、网关。

三. 实验环境

实验方式

实验过程中，以 2 人为 1 个实验小组。每个小组领取路由器 1 台，网线 2 根（正线）。在完成一台路由器的正确配置后，理解路由表的含义基础上，和相邻同学一起利用 2 台路由器连接 3 个子网。有时间有能力的同学做选做任务。

四. 实验内容

1. 一台路由器连接 2 个子网。
2. 两台路由器连接 3 个子网。
3. （选做）多台路由器连接更复杂网络。
4. （选做）无线网和有线网互连。

五. 实验步骤

（一）路由器的管理

1. 按下面板上“Reset”键一段时间(约 5s)，使路由器恢复至出厂缺省设置。

提示：路由器的设置通过 LAN 口进行配置，默认的 LAN 口 Web 管理地址为：**192.168.1.1**；默认的用户名：空；密码：**admin**(注意：小写)

《计算机网络技术基础》实验指导书

2.用两条网线将两台计算机和路由器连接起来，一台计算机接路由器的任意一个 LAN 口（共 4 个），另一台计算机接路由器的 WAN 口（Internet 口）。

3.将连接 LAN 口的计算机网卡的 IP 设置为 192.168.1.x(x 可以为 2 到 254)，子网掩码设置为 255.255.255.0，网关和 DNS 服务器暂时不用进行设置。在这台计算机的网页浏览器中输入路由器 Web 管理地址为 <http://192.168.1.1>，在弹出的对话框内“用户名”保留为空，“密码”栏输入小写“admin”。确定后即可进入路由器配置界面。

4.沿路径“Setup→Advanced Routing”禁用 NAT 服务，沿路径“Security→Filter”禁用 Firewall 服务（Block WAN Requests 下的 Block Anonymous Internet Requests）。对任一个页面进行修改后，都必须通过“Save Settings”键保存设置。

（二）一台路由器连接 2 个子网

实验网络结构如图 4-1 所示，其中 R1 代表所用的路由器，接口 0 和接口 1 分别代表该路由器上用于连接 Internet 和局域网的端口，主机 a 和主机 b 为同一小组中的 2 台计算机，分属于子网 1 及子网 2。

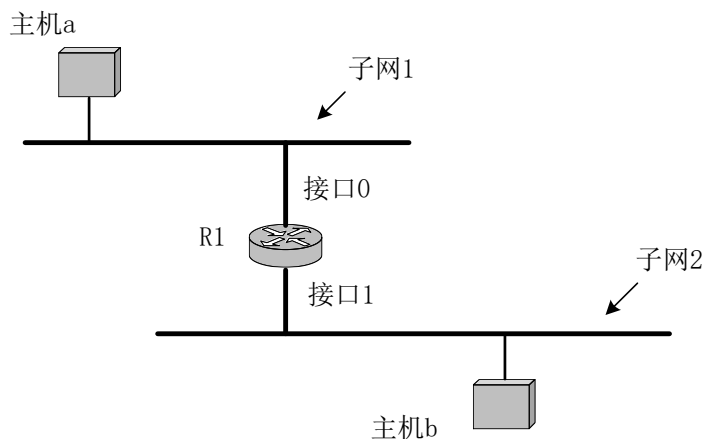
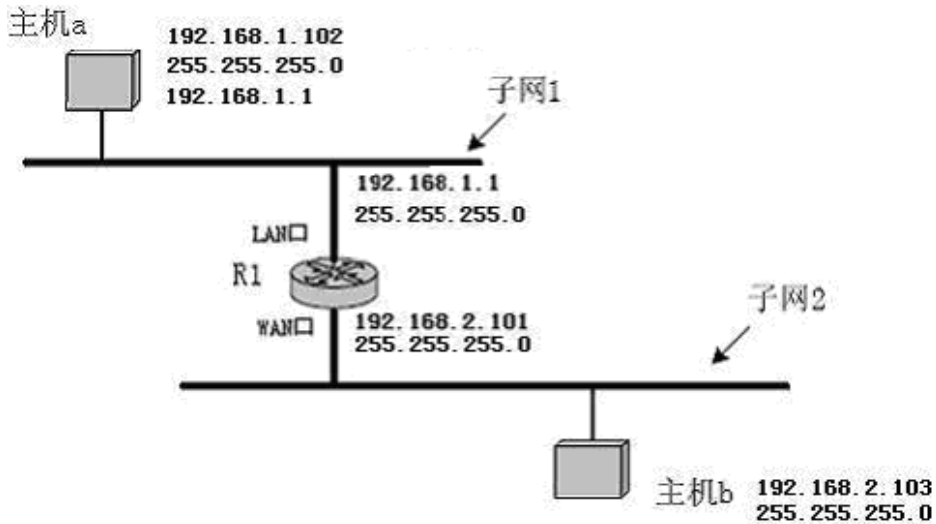


图 4-1 利用 1 台路由器连接 2 个子网示意图

1. 完成物理连接，通过指示灯确认连接。
2. 小组内协商拟定子网 1 和子网 2 所采用的 IP 地址和子网掩码。
3. 将小型路由器接口 0 及接口 1 的 TCP/IP 属性分别设置为商定好的子网 1 及子网 2 相关配置。
4. 相应的完成主机 a 和主机 b 的 TCP/IP 属性设置（注意：主机 a 和主机 b 的网关设置），确认各子网内部的正常通信。
5. 尝试 2 个子网间的通信，通过各种网络测试命令分析网络情况，观察并记录实验现象。分析并读懂路由表。

思考题：分析路由器在网络连接中的作用，路由表的各项属性的含义。



假设有一组同学做了如上设置，主机 b 肯定不能和主机 a 通信，请问此时主机 a 能够 ping 通主机 B 吗？为什么？

（三）两台路由器连接 3 个子网

实验网络结构如图 4-2 所示，其中各标注含义同图 4-1。

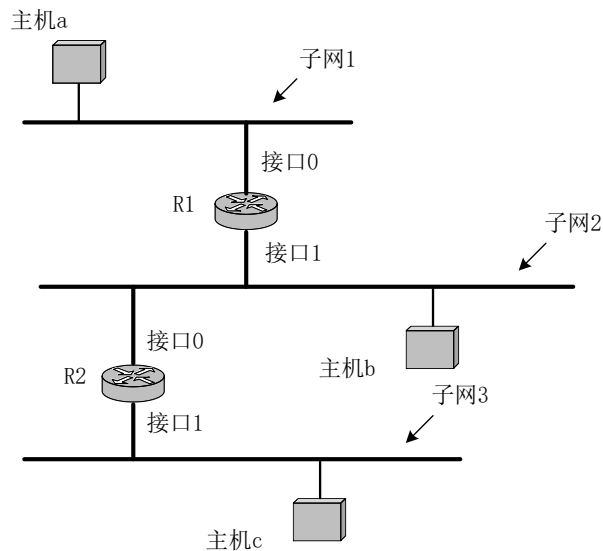


图 4-2 利用 2 台路由器连接 3 个子网示意图

基本步骤与利用 1 台路由器连接 2 个子网时类似：

注意：组网连线前确保 R1 路由器的接口 1 和 R2 路由器的接口 0 的 IP 地址不能相同，

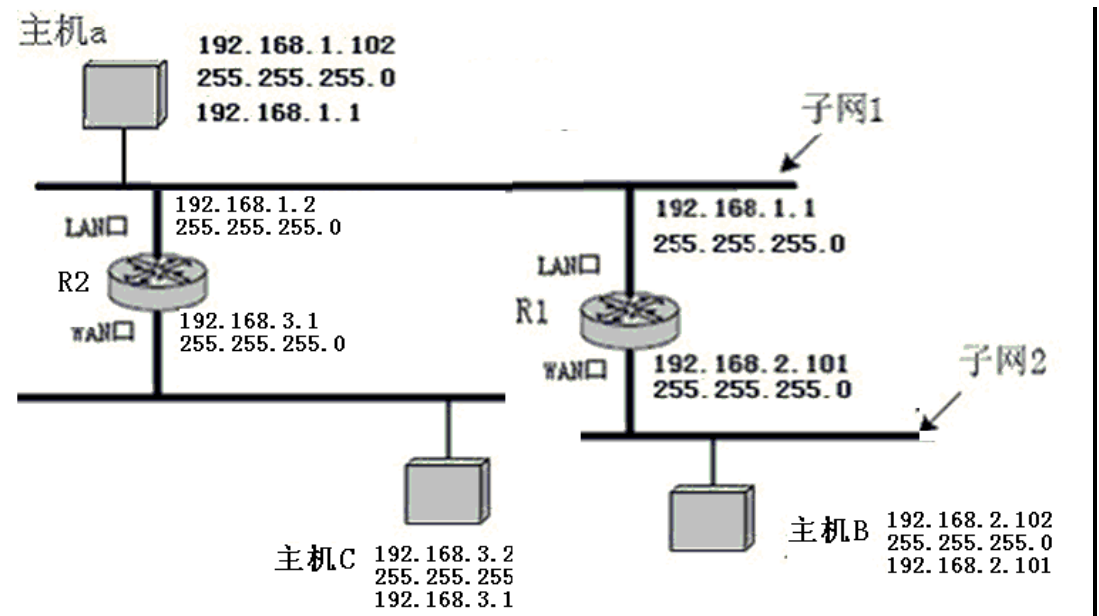
《计算机网络技术基础》实验指导书

否则造成 IP 冲突。

1. 通过指示灯确认物理连接的正确性。
2. 2 个小组的同学通过协商，明确 3 个子网所将要采用的 IP 地址及子网掩码。
3. 分别对 2 台路由器的接口 0 和接口 1 进行相应设置。
4. 根据所在子网规定，对各台主机进行 TCP/IP 的相关配置，确认各子网内部的正常通信。

注意：必须正确设置主机和路由器的网关。

5. 利用实验（二）的设置方法，确认相邻子网（如子网 1 和子网 2、子网 2 和子网 3）之间的正常通信。
6. 分析 2 台路由器的路由表，如有需要，则进行修改，最终实现 3 个子网之间的正常通信。利用各种网络命令进行测试，观察并记录实验现象。



假设有一组同学做了如上设置，R1，R2 路由器的路由表该如何设置，需要添加新的路由表吗？需要的话该如何添加，预习时需要想好 R1，R2 路由器的路由表设置情况。

思考题：①总结实现跨子网通信的条件。

②将路由器 R1、R2 的默认网关分别设置为 R2 接口 0、R1 接口 1 地址，分别从不同子网主机利用网络命令（ping、tracert 等）测试同某一不存在的 IP 地址的连接，观察并记录实验现象，尝试进行分析。

（四）无线网和有线网互连（选作）

由于所使用的无线路由器与 Linksys 小型路由器有相似的功能和配置方法，因此同学们既可以比照实验（一）至实验（三）的方法，建立由无线网关构成的多子网网络，也可

《计算机网络技术基础》实验指导书

以在已完成构建的网络中加入无线网关，对其进行进一步拓展。

对无线网关设备的使用参见实验说明（二）及相关设备手册。

六. 实验说明

（一）实验用路由器

实验所用路由器为 Linksys 公司生产的 EtherFast Cable/DSL 路由器（包含 4 端口交换机），产品编号 BEFSR41，如图 4-3 所示，其规格如表 4-1 所示。



图 4-3 EtherFast Cable/DSL 路由器

表 4-1 BEFSR41 主要规格

符合的标准	IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX)
端口	1 个用以连接 internet 的 10 M/100 M RJ-45 端口 4 个 10 M/100 M RJ-45 交换端口
指示灯	电源、局域网、Internet
支持的网络协议	TCP/IP、NetBEUI、IPX/SPX
电源输入	外接, AC 9V, 1000 mA

（二）WLAN、Intel 无线网络适配器、Intel 无线网关

WLAN (Wireless Local Area Network) 是一种利用高频无线电波在网络客户端和设备之间传送数据的局域网。在无线局域网中，客户端的工作模式分为 infrastructure 和 peer-to-peer 两种。在 infrastructure 模式下，客户端通过一个或多个接入点 (access point) 来发送和接收数据，如图 4-4 所示。相应的，在 peer-to-peer (Ad Hoc) 模式下，客户端之间可以直接进行通信，而不需要接入点或无线网关，如图 4-5 所示。

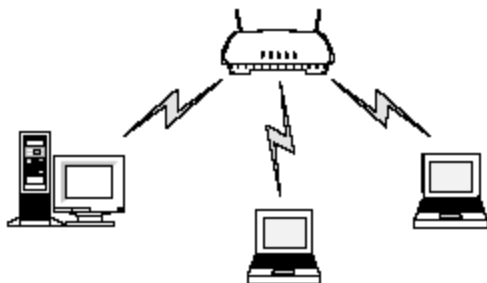


图 4-4 Infrastructure 模式



图 4-5 Ad Hoc 模式

实验所用的无线路由器符合 IEEE 802.11b 标准的提供无线接入点和宽带路由功能的设备，也可以仅作为无线接入点来使用。

其基本应用如图 4-6 所示。

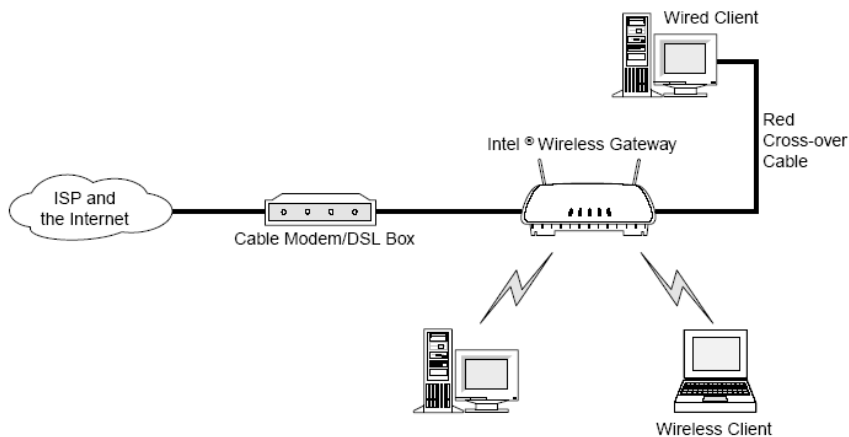


图 4-6 Intel Wireless Gateway 的基本应用

其他注意事项与配置 Linksys 路由器时类似。

选做实验一 交换机 VLAN 的实现

一. 实验目的

1、了解什么是“广播风暴”以及通过 VLAN 控制网络中广播流量的原理，掌握 VLAN 的作用与用途。

2、理解 VLAN 划分的几种方式：基于端口，基于 MAC 地址，基于 IP 子网、基于协议和基于策略。

3、掌握单一交换机及跨交换机划分 VLAN 的配置方法。

二. 预习要求

提前了解 VLAN 的作用与用途，理解划分方法。实验用的 H3C 交换机的管理可用 telnet 命令行的方式也可以通过 LAN 口进行配置。如果用命令行方式需提前掌握各命令。

三. 实验环境

实验方式

实验过程中，以 2 人为 1 个实验小组。每个小组领取 H3C 交换机 1 台，网线 2 根（正线）。在完成一台交换机的 VLAN 配置后，理解基于端口的 VLAN 划分基础上和另外一组同学一起实现 2 台交换机间 VLAN 划分。有时间有能力的同学做提高任务。

四. 实验内容

- 1、1 台 H3C 交换机配置 2 个 VLAN 的管理与实现
- 2、2 台交换机的 2 个 VLAN 之间的通信设置
- 3、2 台交换机的 2 个 VLAN 之间的汇聚（提高）

五. 实验步骤

实验所用交换机为华三（h3c）全千兆可管理交换机 S1850-10P，支持 WEB 页面配置，Telnet 命令行配置，FTP、TFTP、Xmodem 文件上下载管理。H3C 交换机的管理可用 telnet 命令行的方式也可以通过 LAN 口进行配置。默认的 LAN 口 Web 管理地址为：192.168.0.233。

注意：由于此交换机网页进不去，恢复出厂设置比较麻烦，希望做完实验的同学在关闭系统前恢复出厂设置。设备—>配置管理—>出厂设置。

（一）、1 台 H3C 交换机配置 2 个 VLAN 的管理与实现

任选一台计算机 A，用一条网线将这台计算机和 H3C 交换机连接起来。设置计算机网卡的 IPv4 地址，保证和 H3C 交换机在同一网段，可设置为 192.168.0.1，子网掩码：255.255.255.0。

《计算机网络技术基础》实验指导书

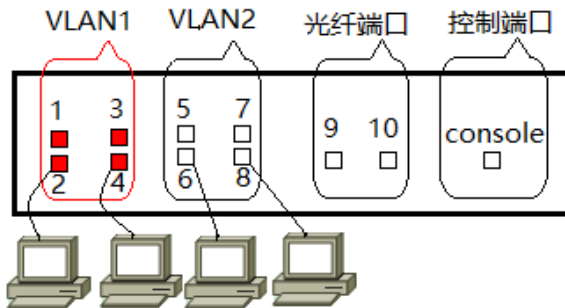
在 A 计算机的地址栏输入 192.168.0.233，回车后输入默认的用户名：admin；密码：admin(注意：小写)，验证码，选择语言，进入管理界面。

设备—>日期和时间：可以修改时间。

设备—>用户管理：一定不要修改用户名和密码，以避免其他人无法使用。

网络—>VLAN—>创建 VLAN：可以创建 VLAN

网络—>VLAN—>修改端口—>选择端口：修改端口的 VLAN ID(设置 1~2 为 VLAN1；3~4 为 VLAN2)

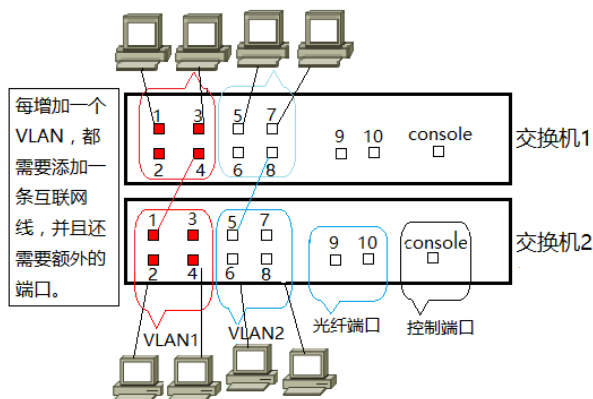


连接交换机的 4 台计算机可以和交换机在同一网段（即 192.168.0.X/24），也可以不在同一网段（如：192.168.20.X/24）验证 4 台计算机之间的连通性。

思考题：同一个端口可以同时属于两个不同的 VLAN？

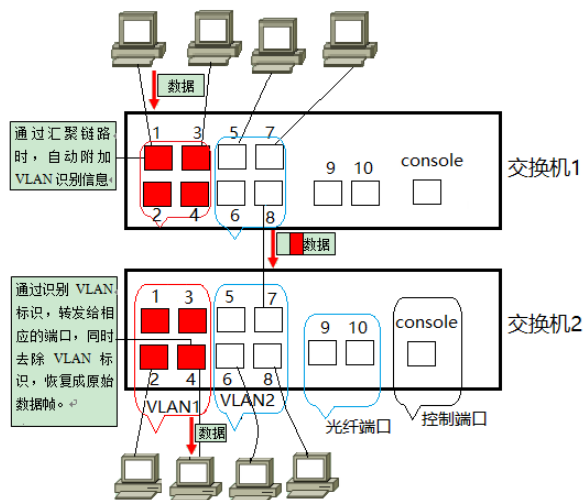
（二）、2 台交换机的 2 个 VLAN 之间的通信设置

分别配置 2 台交换机的 VLAN1 和 VLAN2，配置完成后用一根网线使得 switch1 的 VLAN1 和 switch2 的 VLAN1 相连，用一根网线使得 switch1 的 VLAN2 和 switch2 的 VLAN2 相连，测试各计算机之间的连通性。



用一根网线使得 switch1 的 VLAN1 和 switch2 的 VLAN1 相连，用一根网线使得 switch1 的 VLAN2 和 switch2 的 VLAN1 相连，测试各计算机之间的连通性，根据实验结果做总结。

(三)、2 台交换机的 2 个 VLAN 之间的汇聚（提高）



六. 实验说明

交换机的登录方式

1、控制口方式本地登录。

首先在 Windows 环境下选择“搜索”-》“超级终端”（有些 Windows 版本已没有超级终端，需要从网上下载一个超级终端，并安装在计算机上）；在“新建连接名称”输入连接名称，可以时任意的字母和数字，比如 3COM01.；然后根据连接交换机 Console 口的串口号选择端口号（如：COM1；确定后在属性设置页设置参数，包括“每秒数据位”，一般为 9600，“数据位”为 8 位，“奇偶校验”为“无”，“停止位”为 1，“数据流控制”为无；再次“确定”后即可进入交换机配置界面。

2、Telnet 虚拟终端远程登录

Telnet 协议是 TCP/IP 协议族中的一员，是 Internet 远程登录服务器的标准协议和主要方式。方法是在命令提示符下输入 Telnet IP 地址（如：192.168.1.1，注意 PC 机的 IP 地址要和交换机的 IP 地址在同一网段），此时需要输入用户名和密码进行验证，通过后，就可以在本机控制交换机了。注意默认的访问命令级别为 0 级，并不能进入系统试图，需要切换到相应的用户命令级别，如：super1, super2, super3 等。

3、WEB 方式通过网管软件登录

目前大部分交换机内嵌了 WEB 服务器，客户端通过客户端的 HTTP 协议进行网络通信。管理者可以 WEB 方式进行登录，管理网络设备。

实验五 DNS 服务的实现

一. 实验目的

- 1、了解 DNS 存在的意义；
- 2、了解 DNS 的工作原理
- 3、掌握 DNS 配置方法；
- 4、掌握 DHCP 配置方法（选做）。

二. 预习要求

了解域名的定义及结构，DNS 存在的意义，访问网站的过程；了解 DHCP 的相关概念。

三. 实验环境

软件：Windows Server 下的 DNS 组件以及 DHCP 组件。

实验方式：

DNS 服务：两人一组，其中一台计算机作为主 DNS 服务器，另一台计算机作为辅助 DNS 服务器或转发 DNS 服务器，两台计算机都可以作为客户端。操作系统都为 Windows Server。在配置完成各项服务后，其中一台计算机作为客户端，利用相关客户端工具软件及网络命令进行验证。

DHCP 服务：两人一组，其中一台计算机作为 DHCP 服务器，另一台计算机作为 DHCP 客户端，能够自动获取 IP 地址并能够通信。

四. 实验内容

- 1、配置 DNS 服务器的正向解析。
- 2、配置的 DNS 服务器的转发器或根提示
- 3、配置 DNS 服务器的反向解析
- 4、配置 DHCP 服务器（选作）

五. 实验步骤

（一）设置网络地址

1. 每台计算机拥有 2 块网卡，实验用板载网卡，非板载网卡 IP 地址设置为自动获取并断开。

2. 设置板载网卡的 IP 地址及首选 DNS 服务器（注意两台计算机之间的配合）。为避免 IP 地址在实验室局域网中发生冲突，可按以下方法进行地址的配置：IP 地址：192.168.20.200+*（*为实验桌号），子网掩码：255.255.255.0，默认网关：192.168.20.200，

《计算机网络技术基础》实验指导书

DNS 服务器为学校的 DNS 服务器：166.111.8.28 和 166.111.8.29

3. 记录 www.pku.edu.cn , www.tsinghua.edu.cn , info.tsinghua.edu.cn , learn.tsinghua.edu.cn , mail.tsinghua.edu.cn , mails.tsinghua.edu.cn , www.qq.com , www.baidu.com 域名对应的 IP 地址。

4. 把网卡的 DNS 服务器改为同组配置 DNS 服务器的地址（但 DNS 服务器还未配置）。在命令提示符下输入：ipconfig/flushdns，并验证能否解析 www.tsinghua.edu.cn（注：此时解析不成功）。

（二）安装 DNS 组件

- 1、DNS 组件安装：“开始”→“管理工具”→“服务器管理器”→“角色”→“添加角色”→“DNS 服务器”→“安装”
- 2、安装完成后点击“开始”→“管理工具”→“DNS”进入 DNS 控制界面

（三）配置 DNS 服务器的正向解析（两台计算机都配置）

1. 在“DNS 管理器”控制台下，用鼠标右键单击计算机名称，执行快捷菜单中的“属性”，在属性窗口找到“根提示”，删除里面的所有记录。

注意：在删除过程中的提示信息，思考此信息的含义。

2. 新建区域。在打开的 DNS 控制台环境中展开隐藏目录，在“正向查找区域”中新建区域，区域类型设定为主要区域，指定区域名称（如：一台计算机指定为：tsinghua.edu.cn，另一台计算机指定为：pku.edu.cn）。

注意：选择时依次选“创建正向查找区域（适合小型网络使用）”，“这台服务器维护该区域”，“不允许动态更新”，“不，不应转发查询”

3. 新建主机。利用向导成功创建了“tsinghua.edu.cn”或者“pku.edu.cn”区域，此时内部用户不能使用这个名称访问内部站点，因为它不是一个合格的域名。在其基础上创建指向不同主机的域名之后才能提供域名解析服务。在新建成的区域上新建主机，设定主机名（如：www/info/learn/mail/mails 等）及相应的 IP 地址。准备创建一个用以访问 Web 站点的域名如：“www.pku.edu.cn”，“www.tsinghua.edu.cn”等。

（四）客户端验证

确保本地网络连接配置中 DNS 服务器地址，设为本组 DNS 服务器地址，利用网络命令（如 ping、nslookup 等）测试 DNS 服务设置是否成功。

当 DNS 服务器不能正确解析，显示结果不正确的解决办法：

- ①可用 ipconfig/flushdns 删除本机上的 DNS 域名解析列表；
- ②DNS 服务器刷新（包括：“清除过时资源记录”，“更新服务器数据文件”，“清除缓存”），也可以停止 DNS 服务，然后再重新启动此 DNS 服务。

（五）配置 DNS 服务器的委派

随着公司业务的扩大，某公司在 aaa.com 域名下申请子域 bbb.aaa.com，为了减轻

《计算机网络技术基础》实验指导书

DNS 服务器的负担, 将 bbb.aaa.com 委派给另一台 DNS 服务器。

1. 在 A 服务器新建区域 aaa.com ;
2. 右键“aaa.com”, 在弹出的菜单中“新建委派”;
3. 在“受委派域名”页面输入“bbb”, 在“完全限定的域名(FQDN)”自动生成“bbb.aaa.com”, 单击“下一步”;
4. 在“名称服务器”页面, 单击“添加”按钮。在“新建名称服务器记录”对话框中“服务器完全限定的域名”处输入“bbb.aaa.com”, 在 IP 地址处输入 B 服务器的 IP 地址, 单击“确认”按钮;
5. 在 B 服务器中配置区域“bbb.aaa.com”, 并新建主机“www”及对应的 IP 地址;
6. 在客户端测试解析结果。

注意: 新建委派时, 域名要与另一台 DNS 的域名相同, 否则就不能验证成功。

(六) 配置 DNS 转发器或根提示

如果 DNS Client 所需要的记录并不在 DNS Server 上, DNS 服务器就会去查找别的 DNS。查找方式有两种, 分别是递归查询和迭代查询。查询的设置具体是体现在根提示和转发器上的。使用根提示是递归查询, 而转发器是迭代查询。

对于自己配置的 DNS 服务器不能解析的域名, 我们希望能够得到其它服务器的解析, 此时可以设置 DNS 转发器(同组的另一台 DNS 服务器作为转发器)与根提示(可以设为学校的 DNS 服务器, 域名: dns-a.tsinghua.edu.cn, IP 地址: 166.111.8.28)。

客户端测试一些自己 DNS 服务器未做解析的网址, 如: www.pku.edu.cn, www.baidu.com, www.qq.com 等。

思考: 如果在自己配置的 DNS 服务器建立了区域" tsinghua.edu.cn ", 并在此区域上建立了 www 主机和 info 主机, 但未定义 mail 和 mails 主机, 客户端测试时能否解析, 如果不能为什么? 应如何处理?

(七) 配置 DNS 服务器的反向解析

1. 新建区域, 在打开的 DNS 控制台环境中展开隐藏目录, 在“反向查找区域”中新建区域, 区域类型设定为主要区域, 指定网络 ID (如: 166.111.4)。

注意: 选择时依次选"IPv4 反向查找区域", "不允许动态更新"。

2. 新建指针, 在新建的" 166.111.4 "区域上新建指向 www.tsinghua.edu.cn 的指针 166.111.4.100 和 info.tsinghua.edu.cn 的指针 166.111.4.98。

3. 客户端进行验证。

注意: 此处验证时不能用 ping 命令, 只能用 nslookup 命令。

(八) 配置 DHCP 服务器(选作)

DHCP 服务是基于 C/S 模式的, 为局域网中的用户提供动态指定 IP 地址和配置相应参数。有些配置参数虽然和 IP 协议并无关系, 但它使得网络上的计算机通信变得方便且容易实现。DHCP 池中的地址采用租用方式, 使得局域网中更多的用户可以方便访问网络。

1、DHCP 组件安装与配置

DHCP 组件安装：“开始”→“管理工具”→“服务器管理器 ”→“角色” →“添加角色”→“DHCP 服务器”→“下一步”→“安装”

注意：网卡选用非板载网卡，IP 地址设置为 192.168.X.1（其中 X 为组号），地址池设置为 192.168.X.2~192.168.X.100

2、配置 DHCP 服务器

安装完成后点击“开始”→“管理工具”→“ DHCP”进入 DHCP 控制界面

在 DHCP 管理窗口，右击“IPv4”，在弹出的菜单中选择“新建作用域”，在后面的对话框中输入起始地址和终止地址，子网掩码租期时间等信息。

3、客户端进行验证。

客户端自动获取 IP 地址或在“命令提示符”下输入“ipconfig/renew”命令更新 IP 租约，也可以使用“ipconfig/release”命令自行将 IP 地址释放，此时客户端会发送给 DHCP 服务器一个 DHCPRELEASE 消息，释放后，DHCP 客户端会每隔 5 分钟自动去找 DHCP 服务器租用 IP 地址，或由客户端用户使用“ipconfig/renew”来租用 IP 地址。

注意：在配置完 DHCP 作用域后，要手动激活作用域以便客户机获取 IP 地址。

六、实验说明

（一） DNS (Domain Name System 或 Domain Name Service)

DNS 是由解析器和域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名和对应 IP 地址，并具有将域名转换为 IP 地址功能的服务器。

域名服务器为客户机/服务器模式中的服务器方，它主要有两种形式:主服务器和转发服务器。将域名映射为 IP 地址的过程就称为"域名解析"。

DNS 服务器在域名解析过程中的查询顺序为:本地缓存记录、区域记录、转发域名服务器、根域名服务器。

（二）域名解析过程：

第一步：客户机提出域名解析请求,并将该请求发送给本地的域名服务器。

第二步：当本地的域名服务器收到请求后就先查询本地的缓存，如果有该纪录项则本地的域名服务器就直接把查询的结果返回。

第三步：如果本地的缓存中没有该纪录，则本地域名服务器就直接把请求发给根域名服务器，然后根域名服务器再返回给本地域名服务器一个所查询域(根的子域)的主域名服务器的地址。

第四步：本地服务器再向上一歩返回的域名服务器发送请求，然后接受请求的服务器查询自己的缓存，如果没有该纪录，则返回相关的下级的域名服务器的地址。

第五步：重复第四步，直到找到正确的纪录。

第六步：本地域名服务器把返回的结果保存到缓存，以备下一次使用，同时还将结果返回给客户机。

（三）创建区域

在打开的 DNS 控制台新建区域名称（如：tsinghua.edu.cn）。

第 1 步，在“DNS 管理器”控制台的“正向查找区域”点击右键；

第 2 步，在出现的菜单中选择“新建区域”，点击“下一步”；

第 3 步，在出现的“新建区域向导”对话框的“区域类型”中选择“主要区域”，点击“下一步”；

第 4 步，在出现的“区域名称”编辑框中键入一个能反映公司信息的区域名称(如“tsinghua.edu.cn”)，单击“下一步”按钮；

第 5 步，出现“区域文件”向导页中已经根据区域名称默认填入了一个文件名。该文件是一个 ASC II 文本文件，里面保存着该区域的信息，默认情况下保存在“%SystemRoot%\system32\dns”文件夹中。保持默认值不变，单击“下一步”按钮；

第 6 步，在打开的“动态更新”向导页中指定该 DNS 区域能够接受的注册信息更新类型。“不允许动态更新”，单击“下一步”按钮；

第 7 步，在“正在完成新建区域向导”对话框中点击“完成”按钮，结束“tsinghua.edu.cn”区域的创建过程。

（四）创建域名

在新建成的区域“tsinghua.edu.cn”上创建一个用以访问 Web 站点的域名“www.tsinghua.edu.cn”。具体操作步骤如下：

第 1 步，依次点击“开始”→“管理工具”→“DNS”，打开“dns 管理器”控制台窗口。在左窗格中“正向查找区域”目录下。用鼠标右键单击“tsinghua.edu.cn”区域，执行快捷菜单中的“新建主机”命令。

第 2 步，打开“新建主机”对话框，在“名称”编辑框中键入一个能代表该主机所提供服务的名称(本例键入“www”)。在“IP 地址”编辑框中键入该主机的 IP 地址(如“166.111.4.100”)，单击“添加主机”按钮。很快就会提示已经成功创建了主机记录。

最后单击“完成”按钮结束创建

（五）设置 DNS 转发器

以 Windows Server 2008 系统中的 DNS 服务器为例介绍设置 DNS 转发器的方法：

第 1 步，打开 DNS 控制台窗口，在左窗格中用鼠标右键单击准备设置 DNS 转发器的 DNS 服务器名称，选择“属性”命令。

第 2 步，打开服务器属性对话框，并切换到“条件转发器”选项卡。在“新建条件转发器”的“DNS 域”输入区域名，“主服务器的 IP 地址”编辑框中输入 ISP 提供的 DNS 服务器的 IP 地址（如：166.111.8.28 和 166.111.8.29），并单击“确定”按钮。

重复操作可以添加多个 DNS 服务器的 IP 地址。需要注意的是，除了可以添加本地 ISP 提供的 DNS 服务器 IP 地址外，还可以添加其他地区 ISP 的 DNS 服务器 IP 地址。

第 3 步，用户还可以调整 IP 地址列表的顺序。在转发器的 IP 地址列表中选中准备调

《计算机网络技术基础》实验指导书

整顺序的 IP 地址，单击"上移"或"下移"按钮即可进行相关操作。一般情况下应将响应速度较快的 DNS 服务器 IP 地址调整至顶端。单击"确定"按钮使设置生效。

（六）DNS 服务器的委派与转发器的区别

DNS 委派，将相关区域解析权限下放给某一台 DNS 服务器，在委派服务器上只存储一条委派方与被委派方的记录。

DNS 转发，即当 DNS 服务器不能解析客户端的请求时，如果设置了转发，则将其转到其它(需要设置)DNS 服务器进行解析。

（七）DHCP 请求 IP 地址的过程

1、发现阶段：即 DHCP 客户端寻找 DHCP 服务器的阶段。客户端以广播方式发送 DHCPDiscover 报文，此报文只有 DHCP 服务器才会响应。

2、提供阶段：即 DHCP 服务器提供 IP 地址的阶段。DHCP 服务器接收到客户端的 DHCPDiscover 报文后，从自己的地址池中挑选一个尚未分配的 IP 地址分配给客户端，向该客户端发送包含出租 IP 地址和其它配置的 DHCPOffer 报文。

3、选择阶段：即 DHCP 客户端选择 IP 地址阶段。如果有多台 DHCP 服务器向该客户端发来 DHCPOffer 报文，客户端只接受第一个收到的 DHCPOffer 报文，然后以广播的方式向各个 DHCP 服务器回应 DHCPRequest 报文，该信息中包含向所选定 DHCP 服务器请求 IP 地址的内容。

4、确认阶段：即 DHCP 服务器确认所提供 IP 地址的阶段。当 DHCP 服务器收到 DHCP 客户端回答的 DHCPReques 报文后，便向客户端发送包含它所提供的 IP 地址和其它配置的 DHCP_ACK 确认报文。然后客户端将其 TCP/IP 协议组件与网卡绑定。

实验六 站点的架构技术

一. 实验目的

- 1、了解 windows 2008 server 下的 IIS7；
- 2、掌握 WEB 站点和 FTP 站点的架构技术；
- 3、区分虚拟主机和虚拟目录的概念及实现方法。

二. 预习要求

了解域名的定义及结构， WWW 服务及 FTP 服务特点。

三. 实验环境

软件：Windows Server 下的 IIS 组件、DNS 组件

实验方式：两人一组，每位同学各自配置一台 IIS 服务器，另一位同学的计算机作为 DNS 服务器进行域名解析，并作为客户机进行访问；也可以 IIS，DNS 和客户机都是同一台计算机。

四. 实验内容

- 1、配置简单的 DNS 服务。
- 2、设计简单的网站
- 3、IIS 中 WWW 服务的配置和管理。
- 4、IIS 中 FTP 服务的配置和管理。

五. 实验步骤

（一）设置网络地址及域名解析

1.每台计算机拥有 2 块网卡，实验用非板载网卡，为避免 IP 地址在实验室局域网中发生冲突，配置为：IP 地址：192.168.2.200+*（*为实验桌号），子网掩码：255.255.255.0，默认网关：可以不设，首选 DNS 服务器为同组配置 DNS 服务器的地址。

2.配置简单的 DNS，为将要发布的网站解析域名。

注意：在本次实验中，DNS 服务器的设置必须与 IIS 中 WWW 及 FTP 服务的设置相互配合。

（二）编辑简单网页

编写网页的软件有很多种，常用的有 Dreamweaver、FrontPage 等，还有人直接用 HTML 语言编写。编写网站非本实验重点，同学根据自己的情况利用网页编辑软件编辑简单的网页也可以是自己以前编过的网页。没有编过网页的同学可利用 word 进行编写，保

《计算机网络技术基础》实验指导书

存时另存为网页文件，以便为 WWW 服务提供资源。要求所编写的网页应简洁大方，同时为了取得更好的实验效果，可适当多建一些超链接，多分一些层次。

注意：在制作过程中要确认所编辑网页的保存位置不能是“桌面”和“my document”文件夹，因为这两个位置只有当前用户才能访问，其他用户不能访问，造成网络访问时要求输入用户名和密码。可以在用户分区中建立一个自己的文件夹，所编辑的网页存放在此文件夹下。

（三）安装 Windows Server 下的 IIS 组件

1、IIS 组件安装：“开始”→“管理工具”→“服务器管理器”→“角色”→“添加角色”→“服务器角色”→“WEB 服务器（IIS）”→“安装”

注意：勾选“FTP 服务”，默认状态为不选。

2、安装完成后点击“开始”→“程序/控制面板”→“管理工具”→“IIS-Internet 信息服务（IIS）管理器”进入 IIS 控制界面

（四）WWW 服务的实现

1.在 IIS 控制台中，如果只有 WWW 服务，说明安装 IIS 组件时忘记勾选“FTP 服务”。

2. 新建 Web 站点，在“添加网站”窗口输入网站名称，方便管理时查找虚拟主机，设置虚拟主机对应的主页所在“物理路径”，确定虚拟主机对应得物理主机的 IP 地址，主机名也就是访问虚拟主机所对应的域名。

3. 对新建 Web 站点进行设置。

在虚拟主机所对应的窗口中进行相应的设置，主要设置“默认文档”，此文档是访问网站的主页。

5. 完成相关配置后，利用客户端软件验证 Web 站点设置是否正确。如在 IE 地址栏中如下的访问方式：`http://域名(/IP 地址) [: 端口号]/[网页文件名]`。例如：`http://www.aaa.com` 或者 `http://www.aaa.com:80` 亦或 `http://192.168.20.210` 等。

注意：此处的“[]”代表可选项。

6. 在已有 Web 站点基础上，新建虚拟目录，进行相关设置，利用如下方式进行访问：`Http:// 域名 (/IP 地址) [: 端口号] / 虚拟目录名称 / [网页文件名]`。例如：`http://www.aaa.com/tools` 等。

7.创建多个 Web 站点并确认设置的正确性。

思考：如何通过 IP 方式进行访问？

根据虚拟主机的概念，1 个 IP 地址可以绑定几台虚拟主机，如果在浏览器地址栏输入 IP 地址，不能通过 IP 地址找到对应哪台虚拟主机。Windows IIS 可以在设置虚拟主机时，在属性页中把主机头设成 IP 地址，就可以通过 IP 进行访问。

注意：

①IIS 环境中利用 IP 地址，端口号及主机头对 Web 站点进行区分。上述 3 点完全相同的两个 Web 站点将无法同时正常工作；

②可以不设置 Web 站点主机头，但一旦设置，则要求必须通过主机头来访问 Web 站

点:

访问方式: **http://主机头: [端口号]/[网页文件名]**。

③当建有虚拟目录时, 在 **Web** 站点中需含有添加虚拟目录中需要用到的网页文件, 否则无法正确访问。

(五) FTP 服务的实现

1. 新建 **FTP** 站点, 确认相应的 **IP** 地址及资源目录地址。
 2. 采用与 **WWW** 服务类似的设置方法, 对新建 **FTP** 站点进行配置, 包括 **IP** 地址, 端口号, 访问权限等。
 3. 利用 **FTP** 客户端软件对其进行测试, 验证站点各项设置。可以在 **IE** 地址栏中采用如下的访问方式: **ftp://域名 (/IP 地址) [: 端口号]**
 4. 在已有 **FTP** 站点的基础上, 新建虚拟目录, 进行相关设置, 利用客户端软件验证设置的正确性。
 5. 调整 **DNS** 服务中对主机域名的相应设置, 尝试利用域名方式进行访问。
 6. 创建多个 **FTP** 站点并确认设置的正确性。
- 注意:** **IIS** 环境中利用 **IP** 地址, 端口号对 **FTP** 站点进行区分。上述 2 点完全相同的两个 **FTP** 站点将无法同时正常工作。

思考题:

- 1、结合 **DNS** 服务的设置, 总结构建 **Web/FTP** 站点的操作流程以及各项属性参数 (**IP** 地址、端口号等) 的作用, 简述这些参数对 **Web/FTP** 站点访问方式的影响;
- 2、总结在同一台计算机上实现多个 **Web/FTP** 站点的方法。
- 3、尝试分析新建站点同新建虚拟目录的区别, 体会虚拟目录的作用;

(六) Apache 服务器的安装与配置 (选做)

该部分为选作内容。实验说明 (二) 中对 **Apache** 服务器的安装与配置进行了简要介绍, 更为详细的操作方法可参见相关用户手册进行。

尝试修改并验证 **Apache** 服务器各项设置, 以及创建虚拟主机、虚拟目录等。

六. 实验说明

(一) 虚拟主机和虚拟目录

通过 **IIS (Internet Information Services)** 中的虚拟主机功能, 可以将一台计算机配置为承载多个 **Web** 及 **FTP** 站点的服务器, 提供 **WWW** 服务或 **FTP** 服务的各站点互不相同, 各自独立, 并且具有不同的内容和权限。

对于 **WWW** 或 **FTP** 服务而言, 只要有一个参数不同于其它虚拟主机, 那么这些虚拟主机就可以在 **IIS** 服务器上同时运行。例如, 在 **IIS** 的 **WWW** 服务中, 只要给每个虚拟主机分配了唯一的主机头名, 就可以将多个 **Web** 站点全部映射到同一 **IP** 地址, 并使用同一

默认端口（80）。

虚拟主机可以有一个主目录，此外还可以有任意数目的发布目录。这些发布目录就被称为虚拟目录。在 Internet 服务管理器中定义一个虚拟目录时，就会有一个别名与该虚拟目录关联。客户端在访问虚拟目录中的信息时会使用该别名。如果管理员未指定虚拟目录的别名，则 Internet 服务管理器会自动生成一个别名。

注意：

- 为服务而创建的虚拟目录的数量几乎是不受限制的，但如果创建的虚拟目录太多，性能可能会有所下降。

- 要定位虚拟目录，必须为虚拟目录指定 URL。可以通过单击包含 URL 的超文本链接或在浏览器中键入 URL 来做到这一点。对于 FTP 服务，可以通过创建与虚拟目录同名的子文件夹，从而列出虚拟目录。

（二） Windows 环境下 Apache 的安裝配置

Apache 是源代码开放的 Web 服务器，它常用于 UNIX 环境下，但也有 Windows 环境下的版本。其软件版本目前有两个系列：1.3.x 和 2.0.x。

本次实验中以 1.3.x 系列为例加以说明。

1、安装 Apache

Apache 的安装过程很简单。只需要设置以下一些参数：

在“Network Domain”里输入服务器所在域。

在“Server Name”里输入服务器名。

在“Administrator's Email Address”里输入网站管理员的 Email 地址。

除此之外，安装过程里所有的选项全部采用默认设置即可。

2、运行 Apache

在 Windows 环境下，采用默认选项安装 Apache 服务器后，除了在“开始”→“程序”里增加一个“Apache HTTP Server”的组之外，还会在系统的服务里增加一个 Apache 服务。该服务被设置为系统启动时自动运行。

正确安装后，在浏览器地址栏中键入“http://localhost”或是“http://127.0.0.1”就可以打开 Apache 服务器的欢迎页面以及指向用户手册的链接。

注意：Apache 服务器默认监听端口为 80，因此须避免与其它本地程序发生冲突。

3、配置 Apache

Apache 服务器是一个后台运行的程序，没有图形界面。所有的配置都包含在配置文件里。其主配置文件是：

`$APACHE_ROOT\Apache Group\Apache\conf\httpd.conf`

如果要修改服务器的配置，可以用任何一个文本编辑工具（例如记事本）编辑这个配置文件。在配置文件里，以“#”开头的行是注释行。

配置文件里的部分选项包括：

Port 80: Apache 默认会绑定在本机所有 IP 地址的 80 端口上。

ServerName: Web 服务器的名字。安装时输入的“Server Name”就保存在这。

DocumentRoot "\$APACHE_ROOT/Apache Group/Apache/htdocs": Web 网站的根目录。

DirectoryIndex index.html: 默认网页文件名。在浏览器里输入一个地址（例如 `http://localhost`）的时候，Apache 服务器会查找这个默认的网页文件并打开。

注意：

①必须把网页文件放在所指定的网站根目录下，并且默认网页文件名要设置正确，否则将无法浏览网页。

②每次更改配置文件后，要重新启动 Apache 服务才能使更改生效。

③其它主要配置参数包括 **Listen**、**BindAddress**、**<VirtualHost>**等。

实验七 小型网络上网服务的实现

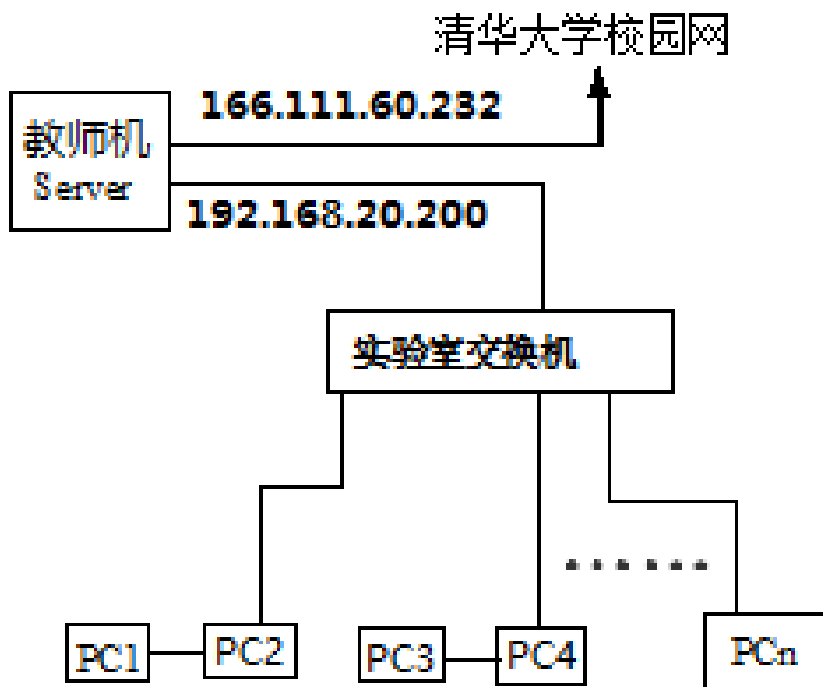
一、实验目的

- 1、了解 NAT 服务原理及存在的意义。
- 2、了解静态地址转换（Static NAT）、动态地址转换（Dynamic NAT）和端口地址转换（Port Address Translation）3 种转换之间的不同。
- 3、掌握安装和配置静态地址转换 NAT 和端口地址转换的方法。

二、预习要求

了解 NAT 服务的原理及存在的意义及三种转换方式。

三、实验环境



软件：Windows Server 下的“路由和远程访问服务”。

实验方式：相邻 2 名同学组成 1 个实验小组，每组领取级连用网线 1 根，此网线取代交换机连接两台计算机。

四、实验内容

1. 安装并配置 Windows Server 提供的“路由和远程访问”模块，实现静态地址转换；
2. 配置 Windows Server 提供的“路由和远程访问”模块，实现端口地址转换。

五、实验步骤

（一）静态地址转换

1、准备工作

(1) 以小组为单位，断开与实验室交换机的连接，协商小组内部局域网设定的网络地址。

(2) 一台计算机作为 NAT 服务器，其中一块网卡与实验室交换机相连，处于“外网”，另一块网卡与小组客户机相连，处于“内网”；

(3) 设置服务器和客户机所用网卡的 TCP/IP 属性，为避免 IP 地址冲突，要求各小组 NAT 服务器连接“外网”的网卡统一选用板载网卡，IP 地址设置为 192.168.20.200+*（其中*为实验桌号）（子网掩码 255.255.255.0），确认设置的正确性。尝试利用网络命令，如 ping、tracert 等，分别从客户机及服务器访问 192.168.20.200 及 166.111.60.232，记录实验现象：

注意：

① NAT 服务器同客户机相连时应选用恰当的网线；

② 回忆实验四内容，明确网关的作用，配置好各计算机网关 IP 地址。

2、服务器端设置

（2008server）安装“路由和远程访问”组件：“开始”→“管理工具”→“服务器管理器”→“角色”→“添加角色”→“服务器角色”→“网络策略和访问服务”→“角色服务”→“路由和远程访问服务”→“安装”。

（2012server）安装“路由和远程访问”组件：“开始”→“管理工具”→“服务器管理器”→“角色”→“添加角色”→“服务器角色”→“远程访问”→“角色服务”→“路由”→“下一步”，按照向导要求完成安装。

安装完成后可以从“开始”→“程序/控制面板”→“管理工具”→“路由和远程访问服务”进入“路由和远程访问”控制台，在“路由和远程访问”控制台右键本地计算机名，打开“配置并启用路由和远程访问”选项，注意选择“网络地址转换（NAT）”，在“使用此公共接口连接到 Internet”处，选择连接到教师机的网卡（即：192.168.20.*），关于“DNS 和 DHCP 服务选择”窗口选择“启用基本的名称和地址服务”。

3、客户端上网

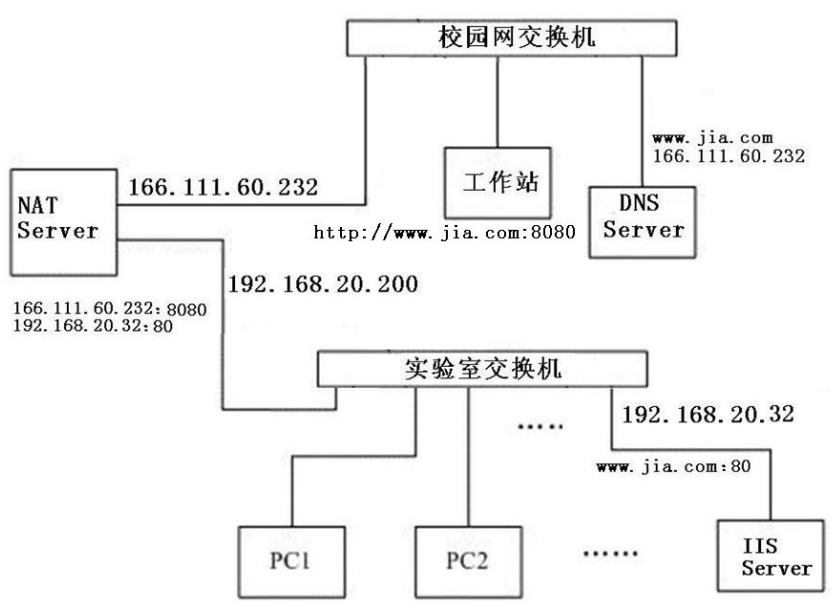
尝试利用网络命令，分别从客户机及服务器访问 192.168.20.200、166.111.60.232、166.111.60.1，166.111.8.28 等地址，记录实验现象，注意与步骤 3 中现象进行比较：

在客户机上尝试利用各种客户端软件访问“外网”Web 服务、FTP 服务等。

思考：

- ①在该条件下，客户机是否需要对各种客户端软件进行单独配置？
- ②DNS 服务器地址在客户机和服务器上分别应如何配置？
- ③结合实验室网络拓扑示意图，给出此时包括所在小组内部局域网在内的网络拓扑结构，做好网络地址标注；
- ④结合所学理论知识，总结 NAT 服务的主要功能和特点。

（二）NAT 服务的端口映射



利用 NAT 服务所提供的端口映射功能，实现小组内部网络 Web 网站的发布，根据上图，转换成小组内部的结构图，参考实验说明（二），通过修改“路由和远程访问”模块中对网络地址转换（NAT）协议的设置，使得处于外部网络的计算机能够通过访问 NAT 服务器某端口，如 8080，实现对内部网络 WEB 站点的访问。

六、实验说明

（一）NAT 基本原理

随着 Internet 的迅速发展，IP 地址短缺已成为一个十分突出的问题，NAT（Network Address Translation）技术也就应运而生。一般情况下服务器有两个 NIC，一个接 Internet，为合法 IP，一个接 LAN，为保留 IP；LAN 的用户的 default gateway 指向 NAT 的内部(LAN)接口；所有从 LAN 通过 NAT 出去的包在 NAT 处会进行一个转换，通常会把这些包的源 IP 地址转换成 NAT 的外部接口的合法 IP 地址送到 Internet，同时 NAT 在自己的连接表中添加一条记录，以便这个包对应的应答包到达时知道应该送回哪里；当应答包回到 NAT 的外部接口，NAT 接到应答包，查看自己的连接表记录，更改应答包目标 IP，送到发出

请求的工作站。

NAT 服务的优点：除了能帮助解决令人头痛的 IP 地址紧缺之外，NAT 技术还能使得内外网络隔离，提供一定的网络安全保障。按实现方法的不同，可以将其分为静态地址转换（Static NAT）、动态地址转换（Dynamic NAT）和端口地址转换（Port Address Translation）3 种。

①静态地址转换

静态地址转换是设置最为简单和最容易实现的。此时内部网络中的每个主机都被永久的映射成为了外部网络中的 IP 地址，如图 5-2 所示。

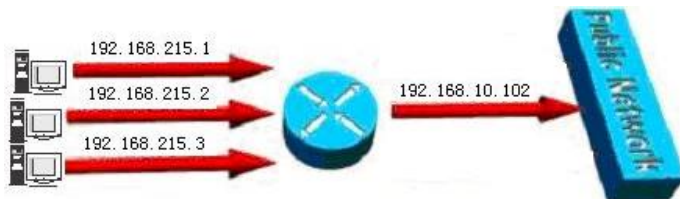


图 5-2 静态地址转换示意图

②动态地址转换

动态地址转换则是在外部网络中定义了一系列的 IP 地址，采用动态分配的方法映射到内部网络，如图 5-3 所示。

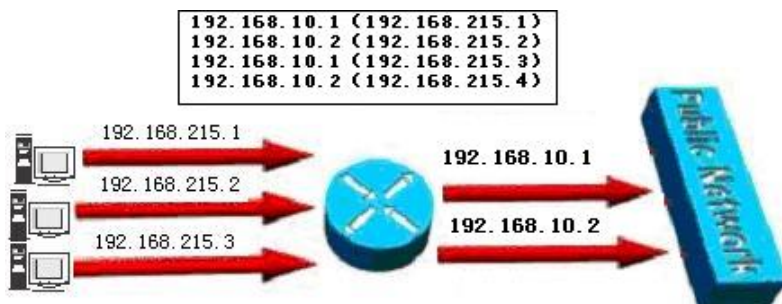


图 5-3 动态地址转换示意图

③端口地址转换

端口地址转换是把内部地址映射到外部网络 IP 地址的不同端口。它比较常用的一种转换方式，普遍应用于各种接入设备中。它可以将中小型的网络隐藏在一个合法的 IP 地址后面。与动态地址转换不同的是，它将内部连接映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加上一个由 NAT 设备选定的端口号，如图 5-4 所示。

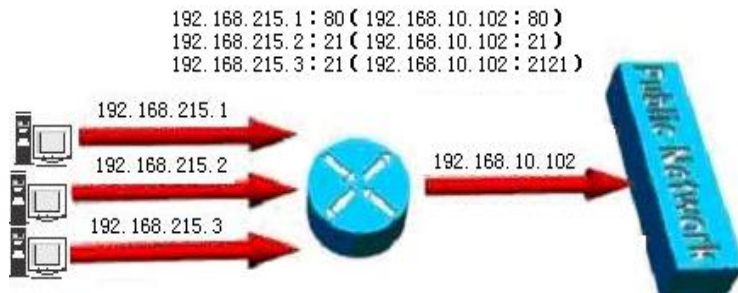


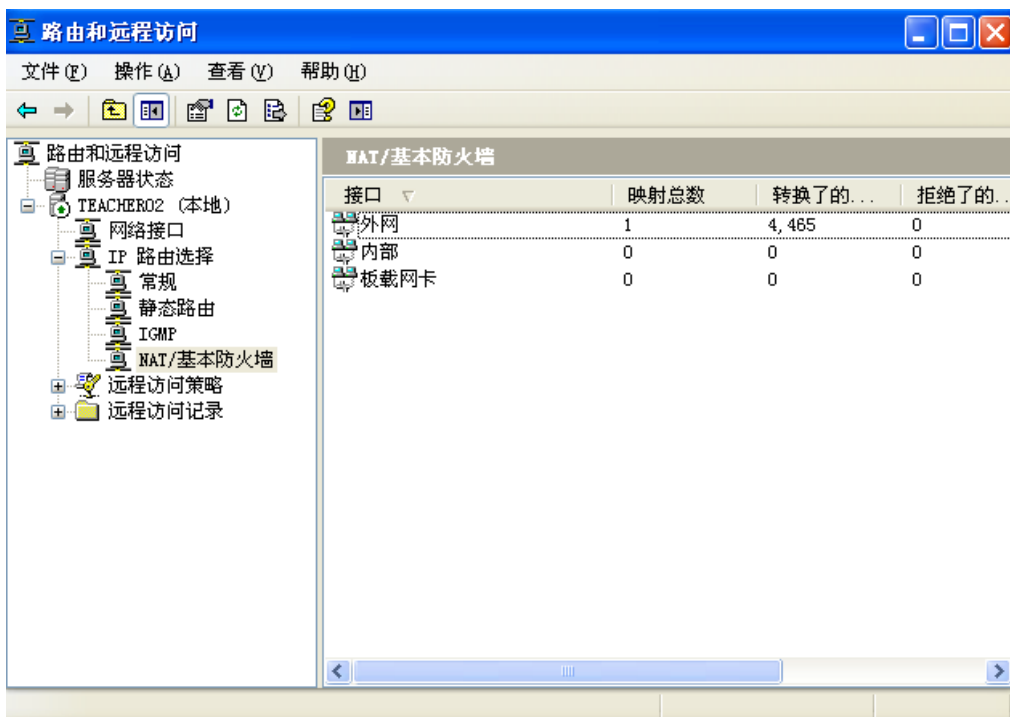
图 5-4 端口地址转换示意图

(二) NAT 映射端口的方法

假设连接Internet网卡的IP地址是 166.111.60.232，连接局域网内部的网卡地址是 192.168.215.28；局域网内另一台计算机（网卡地址是192.168.215.27）提供了Web服务，端口是80，需要设置的是从外网（用166.111.60.232：8080）访问内网192.168.215.27:80上的网页。

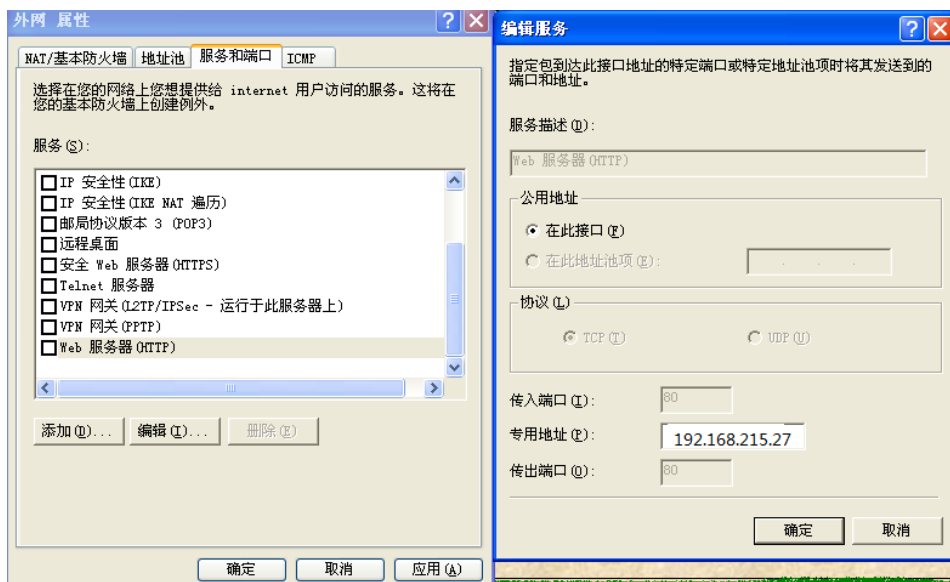
利用NAT来映射端口的方法步骤如下：

- 1、在已设置好的“路由和远程访问”窗口的“IP路由选择”下，选择“NAT/基本防火墙”。
- 2、在右侧的NAT/基本防火墙窗口中选择连向Internet的那个连接(如本地连接/外网等)，点击鼠标右键，选择“属性”



《计算机网络技术基础》实验指导书

- 3、在“属性窗口”的“服务和端口”找到“WEB服务器（HTTP）”，点击“编辑”按钮，出现“编辑服务”窗口。
- 4、在“编辑服务”窗口中输入“专用地址”，如：192.168.215.27，此时的“传入端口”和“传出端口”均默认为80端口，不能修改。



- 5、如需修改“传入端口”和“传出端口”的端口号，可在“属性窗口”的“服务和端口”，点击“添加”按钮，出现“添加服务”窗口。

添加服务

指定包到达此接口地址的特定端口或特定地址池项时将其发送到的端口和地址。

服务描述 (D):

192.168.215.27web

公用地址

☒ 在此接口 (F)

☐ 在此地址池项 (E):

协议 (L)

☒ TCP (T) ☐ UDP (U)

传入端口 (I): 8080

专用地址 (E): 192.168.215.27

传出端口 (O): 80

确定 取消

- 6、在“添加服务”窗口中，填写“服务描述”，输入“传入端口”、“传出端口”、“专用地址”，如：192.168.215.27。

说明：“传入端口”就是外网访问有公网IP的NAT服务器的端口，这里设为8080。

“专用地址和传出端口”就是内部主机的IP地址和提供特殊服务的端口。

- 7、此时完成了166.111.60.232上的8080端口映射到192.168.215.27上的80端口。这就是TCP协议端口的重定向。

- 8、通过外网的一台主机访问<http://166.111.60.232:8080>

注意：在访问之前192.168.215.27的80端口需开启WEB服务。

- 9、同样也可以对其它端口映射。

选做实验二 代理服务的实现

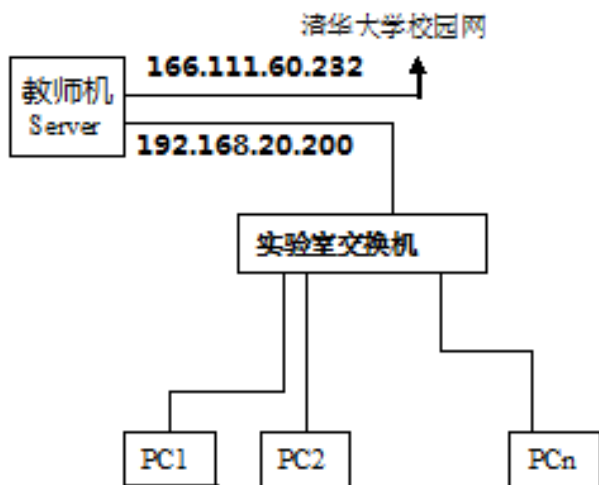
一、实验目的

- 1、了解代理服务的原理及存在的意义。
- 2、掌握安装和设置 WinGate 软件的代理服务
- 3、对比 NAT 和 Proxy 服务的异同，增强对二者基本原理的理解。

二、预习要求

了解代理服务的原理及存在的意义及了解 WinGate 软件。

三、实验环境



软件：WinGate 软件

实验方式：相邻 2 名同学组成 1 个实验小组，每组领取级连用网线 1 根，此网线取代交换机连接两台计算机。

四、实验内容

1. 安装 WinGate 软件实现代理服务
2. 安装 WinGate 软件实现 NAT 服务

五、实验步骤

（一）利用 Wingate 软件实现 Proxy 服务

1. 以小组为单位，协商小组内部局域网设定的网络地址。每台计算机的两块网卡只用

《计算机网络技术基础》实验指导书

一块，释放其中没有连接的网卡 IP 地址，并禁用。为避免冲突，要求各小组内部网络地址协调统一，作为客户机的计算机 IP 地址设置为 192.215.x.y（其中 x 为各小组奇数实验桌号，y 为桌号），作为 Proxy 服务器的计算机网卡上绑定 2 个 IP 地址（在高级里添加），分别为 192.168.20.*（其中*为 200+实验桌号）和小组内部网络地址，如 192.215.x.y。

注意：

正确配置客户机和 Proxy 服务器的网关地址。

2. 尝试利用网络命令，分别从客户机及 Proxy 服务器访问 192.168.20.200 及 166.111.60.232，记录实验现象；

3. 阅读实验说明对 Wingate 软件功能的简介，了解其功能结构，用户管理方式等；

4. 在 Proxy 服务器上安装 Wingate 软件服务器端。在安装 WinGate Server 时，注意看说明，按提示安装，选用 30 天试用，不选 ENS（NAT）服务。

注意：此时客户机无需安装 Wingate 软件；

5. 在客户机上对客户端软件进行相应配置，包括 Web 浏览器、FTP 客户端等，通过 Proxy 服务实现对其它子网资源的访问；

6. WinGate 安装成功后，启动 GateKeeper。初始用户名：Administrator，密码：空。

注意：Administrator 是系统的最高账号，拥有最高的权利，如果丢失其密码，将无法改变 WinGate 的所有设置，必须重装。

7. 在 Proxy 服务器端配置 Wingate 软件，实现基本的管理策略，如根据 IP 地址等限制客户机使用 Proxy 服务，限制客户机所能访问的站点等。要求完成以下 3 项：

- 1) 限制某台电脑不能上网
- 2) 限制只能某台电脑上网
- 3) 限制工作站不能访问带有"tsinghua"域名的站点。

思考：

①DNS 服务器地址在客户机和 Proxy 服务器上分别应如何配置？

②结合实验室网络拓扑示意图，给出此时包括所在小组内部局域网在内的网络拓扑结构，做好网络地址标注；

③尝试从网络体系结构的角度出发，从根本上分析比较 Proxy 服务与 NAT 服务的异同。

（二）WinGate 软件实现 WGIC 和 NAT 服务（选作内容）

结合附录说明及软件使用帮助，尝试 Wingate 提供的 WGIC 和 NAT 服务，注意整理实验环境，避免实验时与其它连接方式所提供的服务相混淆，总结 NAT 服务，Proxy 服务以及 WGIC 服务之间的异同。

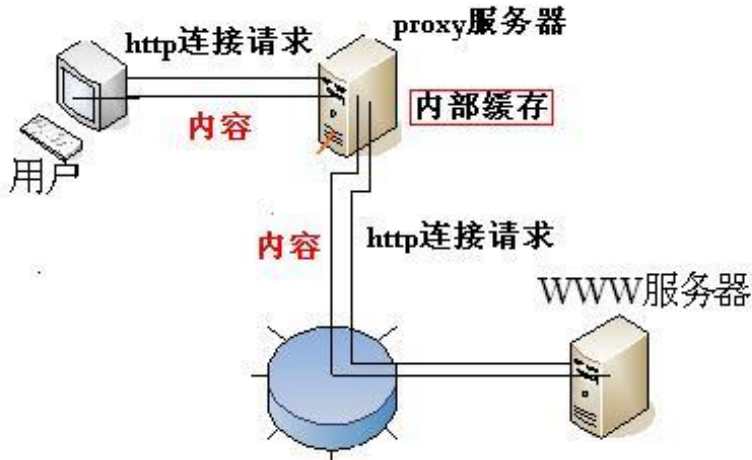
六、实验说明

（一）Proxy 服务简介

Proxy 在字面上的意思是代理人。Proxy Server 将客户端的请求转发到服务器端的

《计算机网络技术基础》实验指导书

机器，也就是接受使用者的要求到 Internet 上抓取网页，将资料存放至硬盘，再将资料传送给使用者。当有另一位使用者要求读取同一份资料时，Proxy Server 即可将存放于硬盘上的资料传送给使用者。具体过程如下：



Proxy 的工作过程

- (1) 使用者 (Client) 提出要求
- (2) Proxy Server 本身是否有所需资料,若有则跳至(6)
- (3) 向真正的 Web Server 提出索取资料需求
- (4) 真正的 Web Server 响应资料
- (5) Proxy Server 储存 WebServer 响应的资料
- (6) Proxy 响应使用者 (Client) 需求

(二) Wingate 软件简介

Wingate 是一款具有防火墙功能的多协议代理服务器软件。WinGate 可以通过一台电脑为局域网上的用户提供因特网访问的共享服务。多协议意味着 WinGate 支持几乎所有的因特网协议，比如 HTTP、FTP、POP3 以及视频、RealAudio 等。它可以分为 2 个主要部分：Wingate 主进程和 Gatekeeper 交互环境。其中，Wingate 主进程在服务器后台运行，提供服务；Gatekeeper 则作为控制接口，提供对远程或本地 Wingate 服务的详细配置。

为了最大程度的方便用户，Wingate 提供了 3 种独立、各不相同的连接方式：

① NAT (Network Address Translation)

在 Wingate 中，它也被称为 ENS (Extended Network Support)，提供与普通 NAT 服务类似的功能。同样地，客户机需要对网关进行设置。

② WGIC (Wingate Internet Client)

WGIC 模块是 Wingate 软件的一个组成部分。客户机在安装 WGIC 之后，一般情况下

《计算机网络技术基础》实验指导书

就可以不用进行其它设置而直接利用 Wingate 服务器的 WRS (Winsock Redirection Service) 服务访问 Internet。如果在安装 WGIC 之前客户机已经在客户端软件中配置了 Proxy 服务, 则应去掉这类设置, 否则这些客户端就仍然会利用 Proxy 服务进行连接。另外, 如果需要同时应用 NAT 服务, 那么也必须作出相应的调整。

③Proxy

Wingate 目前支持的协议包括 WWW, FTP, SMTP, POP3 以及 SOCKS 等。尽管 Wingate Internet Client (基于 WRP) 和 General Purpose Internet Sharing (基于 NAT) 已经削弱了 Proxy 服务的重要性, 但是由于利用此类服务可以实现对各项代理功能的策略控制, 因此也得到了广泛的应用。在 Proxy 方式下使用 Wingate 服务时, 必须在客户端软件中正确添加对应代理服务器的 IP 地址和端口号。值得指出的是, 在 FTP 客户端中除了需要正确添加 FTP 代理服务器 IP 地址和端口号之外, 还需要使能 Firewall, 并选择形如 username@hostname 的连接模式。

除上述主要功能以外, Wingate 还提供了诸如防火墙、DHCP 和 DNS 等服务。

(二) Wingate 软件使用说明

在用户管理方面, Wingate 允许使用 Wingate user database 和 Windows NT/2000 user database 中的任一种用户数据库。当选用后者时, Wingate 所有服务的身份验证都将基于操作系统本身的用户帐户和密码等进行。同时, 虽然可以通过 Gatekeeper 控制台环境查看用户属性, 但对其属性的修改必须在系统管理工具中才能进行。

在策略管理方面, Wingate 总体为 2 层结构: System Policies 定义各项服务和功能的默认访问和控制权限; Services Policies 则针对各项服务进行单独设置。二者之间可以灵活搭配, 以取得最好的管理效果。

通过应用策略, 可以在 Wingate 中自行定义多种规则, 如在 WWW 代理服务中禁止访问特定网站、包含特定字符的域名; 规定用户 Everyone 可以访问 WWW 代理服务, 但不能获取带有.gif 或.jpg 文件后缀的资源等等。

(三) WinGate 属性页

- 1、System 页: 管理 WinGate 的各种高级设置, 如缓存(Caching)、定时计划(Scheduler)和自动拨号(Dialer), 它还管理 WinSock 的各种基本服务, 如 DNS 和 DHCP 服务等。
- 2、Services 页: 管理各种代理服务, 如 FTP、WWW 等。
- 3、Users 页: 管理用户的权限。

(四) 限制局域网中某一电脑不能上网

选择 User 标签→打开 System Policies 对话框→ 双击 Everyone →打开 Properties for recipient Everyone 对话框→ 选择对话框中的 Location 标签→ 选中 Specify locations from where this recopies 单选钮,

《计算机网络技术基础》实验指导书

- 1、在 Included locations(即包括的位置)文本框中添加两个 IP 地址, 一个为 127.0.0.1 另一个为主机的 IP (即安装 Wingate Server 的电脑, 如: 192.168.215.1); 再依次添加局域网中不受限制上网的电脑的 IP 地址
- 2、在 Excluded locations 文本框中输入不能上网电脑的 IP 了。

(五) 限制工作站不能访问某些网站

1: 在 WWW 代理服务中建立一个策略

以 Administrator 登录到 Gatekeeper, 双击服务(Services)标签下的 WWW 代理服务(WWW proxy service)进行编辑。选择策略(Policies)标签, 在默认权利(System policies)选项中, 选择忽略(Are ignored)。点击增加(Add), 选定“所有人”单选钮(Everyone)作为接受策略的用户。点击禁止清单标签(Ban list), 点击开启禁止清单选项(Enable ban list option)。点击增加 (Add), 限制特定的站点, 点击 This criterion is met if, 选择 HTTP URL, 在中间的输入框中, 选择“包含”(Contains from the list)。在最后的输入框键入“tsinghua”, 增加其他要加入到禁止清单中的内容, 保存设置。

2: 应用策略

双击 Socks 代理服务, 选择 Socks 高级(Advanced)标签, 在 HTTP 协议选项中, 选择 Use following policy 钮。在选单中, 选择 WWW Proxy server 项, 点击 OK 后保存。

测试:

应用策略, 禁止客户访问带有“263”域名的站点。

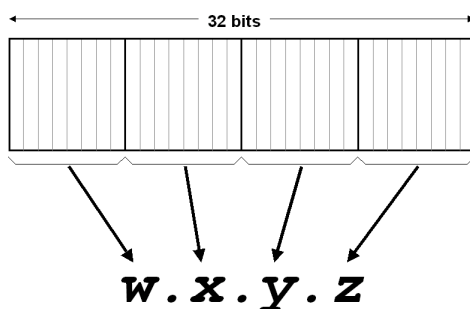
附录：

附录一：IPv4 地址

IP 地址是在 Internet 层分配给一个接口或一组接口的标识符。就像每个人的身份证号一样，任何连接到互联网上的计算机或设备也有一个身份标识方便查找，这个标识就是 IP 地址。IP 地址是互联网协议（Internet Protocol，IP）地址的简称。IPv4 地址是一个逻辑地址，它是在 Internet 层分配的，与网络接口层使用的地址没有关系，其长度为 32 位。

1. IPv4 地址语法

IP 地址由 4 个字节组成，共有 32 位。如果网络管理员使用二进制形式来表示 IPv4 地址，则每个地址都将显示为 1 个由数字 1 和 0 构成的 32 位字符串。因为这种字符串的表示和记忆非常麻烦，所以管理员使用点分十进制表示形式，即使用半角句号（圆点）来分隔 4 个十进制数（从 0 至 255）。每个十进制数叫做 1 个八位位组，代表 32 位地址中的 8 位（一个字节）。引用某个 IPv4 地址时，应使用 w.x.y.z 表示形式，如：192.168.20.200、66.111.60.232 等。



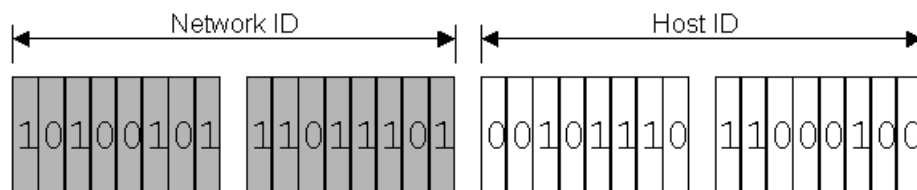
图附 1-1 IPv4 表示形式

2. IPv4 地址分类

每个 IPv4 单播地址包括一个网络 ID 和一个主机 ID。

- 网络 ID（又称网络地址）是 IPv4 单播地址的一部分，用来标识位于同一物理或逻辑网段（其边界由 IPv4 路由器定义）上的接口的集合。TCP/IP 网络上的网段又叫做子网或链路。同一物理或逻辑子网上的所有节点都必须使用相同的网络 ID，而且该网络 ID 在整个 TCP/IP 网络内必须是唯一的。

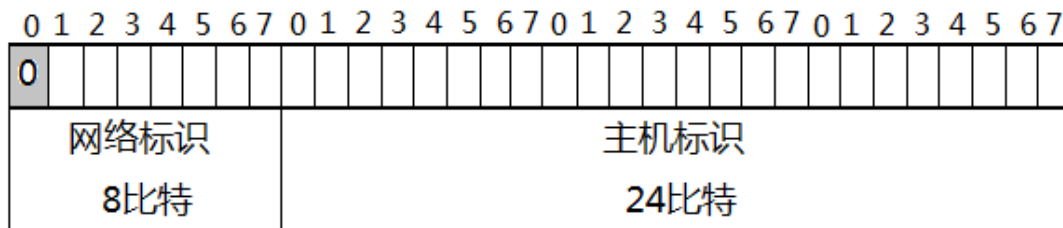
- 主机 ID（又称主机地址）是 IPv4 单播地址的一部分，用来标识子网上的网络节点的接口。主机 ID 在一个网段内必须是唯一的。



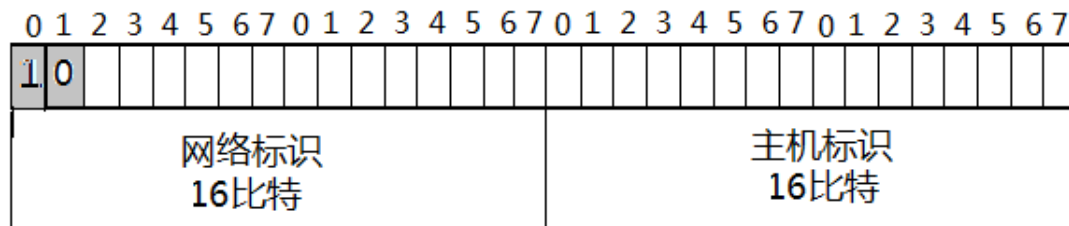
图附 1-2 IPv4 地址的结构示例

为了适应支持不同大小的网络，设计者认为 IP 地址空间应该分为几种。IPv4 地址空间被细化为 5 类：A 类、B 类、C 类、D 类、E 类。其中 D 类和 E 类地址是被保留的，常用的是 A 类、B 类、C 类。

每个 A 类地址由 8 比特网络标识和 24 比特主机号组成，网络标识的最高位指定为 0，其余的 7 位表示网络号。A 类地址表示为 “/8”，因为他们拥有 8 位网络标识。由于 7 位二进制数能够表示的最大十进制数是 128，因此 A 类地址有 128 种可能。在这 128 中需要减去两个被保留的特殊地址，A 类地址最多可以定义 126 (2^7-2) 个网络，每个网络可以容纳 ($2^{24}-2$) 台主机。其中主机号全 0 指“本网络”全 1 指“广播地址”不可以被分配。由于 B 类地址块包含 2^{31} 个地址，并且 IPv4 地址空间包含 2^{32} 的地址，就是全部 IPv4 单播地址空间的 50%。

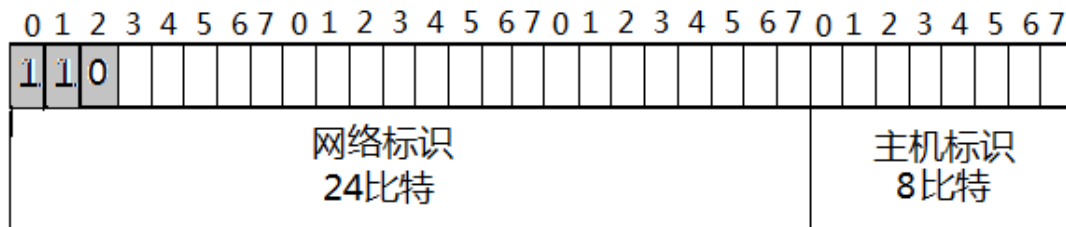


每个 B 类地址由 16 比特网络标识和 16 比特主机号组成，网络标识的最高 2 位指定为 10，其余的 14 位表示网络号。B 类地址表示为 “/16”，因为他们拥有 16 位网络标识。B 类地址最多可以定义 16384 (2^{14}) 个网络，每个网络可以容纳 65534 ($2^{16}-2$) 台主机。由于 B 类地址块包含 2^{30} 个地址，也就是全部 IPv4 单播地址空间的 25%。

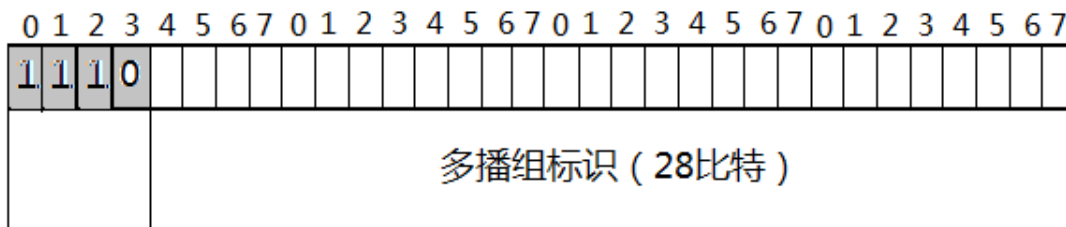


每个 C 类地址由 24 比特网络标识和 8 比特主机号组成，网络标识的最高 3 位指定为 110，其余的 21 位表示网络号。C 类地址表示为 “/24”，因为他们拥有 24 位网络标识。C 类地址最多可以定义 2^{21} 个网络，每个网络可以容纳 254 (2^8-2) 台主机。由于 C 类地址块包含 2^{29} 个地址，也就是全部 IPv4 单播地址空间的 12.5%。

《计算机网络技术基础》实验指导书



D 类地址的高 4 位指定为 1110，D 类地址用于支持 IP 多播。多播定义了一种机制，该机制对网络节点进行分组，并将 IP 消息发给某一组，而不是局域网上的所有节点（广播）或者是仅仅一个节点（单播）



E 类地址的高 5 位指定为 11110，地址从 240.0.0.0~247.255.255.255，保留用于实验和将来使用。

3. Internet 地址类别

公用地址

如果需要到 Internet 的直接（路由）连接，则必须使用公用地址。如果需要到 Internet 的间接（代理的或转换的）连接，则可以使用公用地址，也可以使用专用地址。如果 Intranet 没有以任何方式连接到 Internet，则可以使用任何单播 IPv4 地址。

专用地址

对于 Internet，子网上连接到 Internet 的每个 IPv4 接口都需要有一个在 Internet 内唯一的 IPv4 地址。这一需求对可用公用地址池提出了很高的要求。在分析组织的地址需求时，Internet 的设计者注意到，对于许多组织来说，大多数主机都不需要直接连接到 Internet。那些确实需要一组特定的 Internet 服务（例如 Web 访问和电子邮件）的主机通常通过应用层网关（例如代理服务器和电子邮件服务器）来访问 Internet 服务。因此，大多数组织只需要很少的公用地址，供那些直接连接到 Internet 的节点（例如代理、服务器、路由器、防火墙和转换器等）使用。组织中不需要直接访问 Internet 的主机则需要使用与已分配的公用地址不重复的 IPv4 地址。为解决这一编址问题，Internet 设计者保留了 IPv4 地址空间的一部分供专用地址使用。因为公用和专用地址空间不重叠，所以专用地址永远不会与公用地址重复。

RFC 1918 为专用地址空间定义了以下地址前缀：

- 10.0.0.0/8(10.0.0.0, 255.0.0.0)
- 172.16.0.0/12(172.16.0.0, 255.240.0.0)

- 192.168.0.0/16(192.168.0.0, 255.255.0.0)

因为 ICANN 永远不会把专用地址空间内的 IPv4 地址分配给一个连接到 Internet 的组织, 所以 Internet 路由器中也永远不会包含指向专用地址的路由, 也无法通过 Internet 连接到一个专用地址。因此, 使用专用地址的主机必须将其 Internet 通信量请求发送到一个具有有效公用地址的应用层网关(例如一个代理服务器), 或者通过一个网络地址转换(NAT)设备将此专用地址转换成一个有效的公用地址。

自动专用 IP 地址

可以在一台计算机上配置一个接口, 以便让该接口自动获取一个 IPv4 地址配置。如果计算机没有联系到动态主机配置协议(DHCP)服务器, 则 Windows 的 TCP/IP 组件就会使用自动专用 IP 地址(APIPA)。TCP/IP 组件从地址前缀 169.254.0.0/16 中随机选择一个 IPv4 地址, 并分配一个子网掩码 255.255.0.0。ICANN 保留了此地址前缀, 因而此地址前缀在 Internet 上是不可访问的。

特殊的 IPv4 地址

以下地址是特殊的 IPv4 地址:

- 0.0.0.0

称为未指定的 IPv4 地址, 用来表示地址缺失。未指定地址仅用作下述情况下的源地址: 某个 IPv4 节点没有配置 IPv4 地址配置, 正尝试通过某个配置协议(例如 DHCP)来获取一个地址。

- 127.0.0.1

称为 IPv4 环回地址, 它被分配给了一个内部环回接口。此接口可供节点用来向自己发送数据包

4. IPv4 网络中子网划分

谈到 IP 网络, 不能不提子网掩码。子网掩码的作用就是把“大网”划分为若干个“小网”, 也是用来确定子网数目的依据。A 类网络的默认掩码是 255.255.255.0; B 类网络的默认掩码是 255.255.0.0; c 类网络的默认掩码是 255.255.255.0。

子网掩码同 IP 地址一样也是由 4 个字节组成, 共有 32 位。正确有效的子网掩码必须满足左边的各个位全为 1, 右边的各个位全为 0, 1 和 0 不能间隔出现在子网掩码中。比方说 11111111.11111111.11111000.00000000 (255.255.248.0) 可以看到左边都是 1, 在 1 的中间没有 0 出现(0 都在 1 的右边), 这样就是一个有效的掩码。假如 11111110.11111111.11111000.00000000 (254.255.248.0), 就不是一个正确有效的子网掩码, 因为在 1 中间有一个 0 的存在。再如 11111111.11111111.11111001.00000000 (255.255.249.0), 也不是一个正确有效的掩码, 因为在 1 中间也有 0 的存在。有时我们会看到 IP 地址/数字 这样的形式, 这里的/数字是子网掩码的另一种表示方法。

5. 根据掩码来确定子网的数目

《计算机网络技术基础》实验指导书

首先看题中给出的掩码是属于哪个默认掩码的“范围”内，这样我们就可以知道是对 A 类还是 B 类还是 C 类大网来划分子网。比方说 202.117.12.36/30，我们先把/30 这种另类的掩码表示法转换为我们习惯的表示法：11111111.11111111.11111111.11111100，转为十进制是 255.255.255.252。我们可以看到，这个掩码的左边三节与 C 类默认掩码相同，只有第四节与 C 类默认掩码不同，所以我们认为 255.255.255.252 这个掩码是在 C 类默认掩码的范围之内的，意味着我们将对 C 类网络进行子网划分。因为 C 类网络的默认掩码是 255.255.255.0，将 C 类默认掩码转换为二进制是 11111111.11111111.11111111.00000000，这里的 8 个 0 表示可以用 8 位二进制数来表示 IP 地址，也就是说 C 类大网中可有 2 的 8 次方个 IP 地址，也就是 256 个 IP 地址。这道题中的掩码的最后一节是 252，转换为二进制是 11111100，因为 1 表示网络号，所以 111111 就表示将 C 类大网划分为 (111111) 2 进制个子网。将 111111 转换为十进制是 64，所以就表示将 C 类大网划分为 64 个子网，每个子网的 IP 地址数目是 $256/64=4$ ，去除子网中的第一个表示子网号的 IP 地址和最后一个表示广播地址的 IP 地址，子网中的可分配的 IP 地址数目就是子网中的总的 IP 地址数目再减去 2，也就是 $4-2=2$ 个

6. 综合实例：

已知 172.31.128.255/18，计算：1)网络号， 2)主机号， 3)和此主机所在相同网络 IP 地址的起止范围

1)网络号：

用公式：将 IP 地址的二进制和子网掩码的二进制进行“与”（and）运算，得到的结果就是网络号。“与运算”的规则是 1 与 1 得 1，0 与 1 得 0，1 与 0 得 0。172.31.128.255 转为二进制是 10101100.00011111.10000000.11111111

$$\begin{array}{r} 10101100.00011111.10000000.11111111 \\ \text{与 } 11111111.11111111.11000000.00000000 \\ \hline 10101100.00011111.10000000.00000000 \end{array}$$

将 10101100.00011111.10000000.00000000 转换为十进制就是 172.31.128.0，所以网络号是 172.31.128.0

2)主机号：

将子网掩码取反再与 IP 地址逻辑与运算，结果为即为主机号。

$$\begin{array}{r} 10101100.00011111.10000000.11111111 \\ \text{与 } 00000000.00000000.00111111.11111111 \\ \hline 00000000.00000000.00000000.11111111 \end{array}$$

3) 和此主机所在相同网络 IP 地址的起止范围：

和此主机所在相同网络 IP 地址起始地址为 10101100.00011111.10000000.00000000 转换为十进制就是 172.31.128.0，终止地址为 10101100.00011111.10111111.11111111 转换为十进制就是 172.31.191.255。

附录二：网络配置方法

一台计算机必须经过合适的硬件和软件设置，才能进行正常的网络通信，下面以经常使用的 LAN 局域网为例来介绍个人计算机网络的配置过程：

1. 安装网络硬件设备。

这里所指的硬件设备包括网络适配器（网卡）和保证网卡与网络可靠连接的网线。实验室计算机配置有两块网卡，下面的是单独插在主板插槽中的网卡，名称为“Realtek RTL8139/810x Family Fast Ethernet NIC”，上面的网卡是主板自带的板载网卡，名称为“Intel(R) Ethernet Connection I217-LM”。实验前请确认网线与网卡正确连接。

2. 安装网络操作系统。

目前广为使用的 Windows 系列、Unix、Linux 等操作系统都可以作为网络操作系统完成复杂的网络通信功能。实验中选择 Windows 2008 server 为网络提供软件支持，请在计算机启动时选择正确的操作系统。

3. 在操作系统中完成硬件配置。

Windows 2000 及以上操作系统大都可以自动完成网络适配器的驱动安装，并为之建立合适的配置页面（本地连接）。用户也可以在“开始”→右键“计算机”→“属性”→“设备管理器”中手动完成硬件的安装和设置；另外，可以通过“禁用”再“启用”的方法刷新系统对网络硬件的设置，清除与硬件相关的缓存信息。实验室机器已经对网络硬件进行了正确的设置，实验过程中可忽略这个步骤

4. 网络连接配置。

（1）完成网络硬件配置之后，可以在“开始”→“控制面板”→“网络和 Internet”中找到“网络和共享中心”下面的“查看网络状态和任务”。如：图附 2-1



图附 2-1

（2）找到与网络硬件相应的配置页面——“本地连接”，单击，如：图附 2-2。

《计算机网络技术基础》实验指导书



图附 2-2

(3) 在其属性页中找到“Internet 协议版本 4 (TCP/IPv4)”可以对本机网络进行配置，如：图附 2-3。



图附 2-3

配置只对相应的网卡生效。同时还可以通过“自动获得 IP 地址”完成 IP 配置，也可以在“高级”选项中为连接设置多个 IP 地址。

“自动获得 IP 地址”借助“DHCP”(Dynamic Host Configuration Protocol 动态主机配置协议)服务完成 IP 配置。此选项是否生效依赖于 3 个必要条件：本机已打开“DHCP Client”服务；网络中存在提供“DHCP Server”服务的主机；服务器端的 IP 资源充足。

在手动进行 IP 地址配置时，用户对 IP 地址和子网掩码的设置必须要保证本机与所处

《计算机网络技术基础》实验指导书

的网络工作于同一网段,“默认网关”可以为计算机访问本局域网以外的资源提供服务支持。

DNS 服务器用于保证用户可以通过域名(如 www.tsinghua.edu.cn)方式访问网络资源。用户可以通过“自动获得 DNS 服务器地址”选项由 DHCP 服务完成 DNS 配置,或者手动设置 DNS 服务器地址。

除了 IP 地址的设置,还要为连接安装一些其它必要的服务和协议,以保证用户可以正常使用网络提供的各项功能。“此连接使用下列项目”列表中显示了已经安装的选项,“Internet 协议版本 4 (TCP/IPv4)”是其中最重要的一项,它为用户使用 HTTP、FTP、Telnet 等相关常用应用程序提供支持。

附录三：常用的 DOS 命令

ipconfig 命令

该诊断命令显示所有当前的 TCP/IP 网络配置值。

命令格式：ipconfig [/? | /all | /release [adapter] | /renew [adapter] | /flushdns | /registerdns | /showclassid adapter | /setclassid adapter [classidtoreset]]

/all 产生完整显示。在没有该开关的情况下，ipconfig 只显示 IP 地址、子网掩码和每个网卡的默认网关值。

例如：

```
C:\>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter 本地连接:
```

```
Connection-specific DNS Suffix . :
```

```
IP Address. . . . . : 192.168.10.98 //IP 地址
```

```
Subnet Mask . . . . . : 255.255.255.0 //子网掩码
```

```
Default Gateway . . . . . : 192.168.10.1 //缺省网关
```

```
C:\>ipconfig /displaydns //显示本机上的 DNS 域名解析列表
```

```
C:\>ipconfig /flushdns //删除本机上的 DNS 域名解析列表
```

ping 命令

它是用来检查网络是否通畅或者网络连接速度的命令。工作原理是：当向目标 IP 地址发送 1 个数据包时，如果主机存在，则对方就要返回 1 个同样大小的数据包，根据返回的数据包就可以初步判断目标主机的操作系统等。该命令只有在安装了 TCP/IP 协议后才可以使用的。

命令格式：ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list] | [-k computer-list]] [-w timeout] destination-list

参数

-t 表示将不间断向目标 IP 发送数据包，直到强迫其停止。

-l 定义发送数据包的大小，默认为 32 字节，利用它可以最大定义到 65527 字节。

-a 将地址解析为计算机名

-n 定义向目标 IP 发送数据包的次数，默认为 4 次。

说明：如果 -t 参数和 -n 参数同时使用，ping 命令就以放在后面的参数为准，比如“ping IP -t -n 1”，虽然使用了 -t 参数，但并不是一直 ping 下去，而只 ping 1 次。另外，ping 命

《计算机网络技术基础》实验指导书

令还可以直接 ping 主机域名，从而得到主机的 IP 地址。

- f 在数据包中发送“不要分段”标志。数据包就不会被路由上的网关分段。

- i ttl 将“生存时间”字段设置为 ttl 指定的值。

- v tos 将“服务类型”字段设置为 tos 指定的值。

- r count 在“记录路由”字段中记录传出和返回数据包的路由。count 可以指定最少 1 台，最多 9 台计算机。

- s count 指定 count 指定的跃点数的时间戳。

- j computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。

- k computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源）IP 允许的最大数量为 9。

- w timeout 指定超时间隔，单位为毫秒。

destination-list 指定要 ping 的远程计算机。

下面举例说明一下具体用法。

```
C: \>ping 192.168.215.1
```

```
Pinging 192.168.215.1 with 32 bytes of data:
```

```
Reply from 192.168.215.1: bytes=32 time <10ms TTL=128
```

```
Reply from 192.168.215.1: bytes=32 time <10ms TTL=128
```

```
Reply from 192.168.215.1: bytes=32 time <10ms TTL=128
```

```
Reply from 192.168.215.1: bytes=32 time <10ms TTL=128
```

```
Ping statistics for 192.168.215.1:
```

```
    Packets: Sent = 4,    Received = 4,    Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms,    Maximum = 0ms,    Average = 0ms
```

这里 time<10 表示从发出数据包到接受到返回数据包所用的时间小于 10 秒，从这里可以判断网络连接速度的大小。从 TTL 的返回值可以初步判断被 ping 主机的操作系统，所以说“初步判断”是因为这个值是可以修改的。这里 TTL=128 表示操作系统可能是 windows 2000。如果 TTL=32 则表示操作系统可能是 windows 98，而如果 TTL=250，则目标主机可能是 Unix。

tracert 命令

跟踪路由信息，使用此命令可以查出数据从本地机器传输到目标主机所经过的所有途径，这对了解网络布局 and 结构很有帮助。

命令格式: tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name
/d 指定不将地址解析为计算机名。

- h maximum_hops 指定搜索目标的最大跃点数。

- j computer-list 指定沿 computer-list 的稀疏源路由。

-w timeout 每次应答等待 timeout 指定的微秒数。
target_name 目标计算机的名称。

nslookup 命令

本命令可用于查看 DNS 服务器设置和工作情况，并完成从 IP 地址到域名和域名到 IP 地址的查找工作。

常用命令格式：

nslookup [IP_addr]

nslookup [Server_name]

格式一查找 IP 地址（IP_addr）对应的域名。命令会返回域名服务器名称、IP 地址和域名查询结果。

格式二查找域名（Server_name）对应的 IP 地址。命令会返回域名服务器名称、IP 地址和 IP 查询结果，如果要查找域名是别名（Aliases），结果还将返回目标域名和别名。

命令格式：

另外可以在 nslookup 上加上适当的参数。指定查询记录类型的指令格式如下：nslookup [-qt=类型] 目标域名或目标 IP 地址 [指定的服务器地址]

arp 命令

本命令用于显示和修改 IP 地址与物理地址之间的转换表。地址转换协议 ARP（Address Resolution Protocol）是个链路层协议，它工作在第二层的位置，在本层和硬件接口联系，同时对上层（网络层）提供服务，将 IP 地址转换为 MAC 地址，进而实现网络连接，ARP 协议自身设计了缓存功能，使用 arp 命令可以实现对缓存表的查看和修改。

常用格式：

arp -s inet_addr eth_addr [if_addr]

arp -d inet_addr [if_addr]

arp -a [inet_addr] [-N if_addr]

-a 显示当前的 ARP 信息，可以指定网络地址

-g 跟-a 一样。

-d 删除由 inet_addr 指定的主机.可以使用*号来删除所有主机。

-s 添加主机，并将网络地址跟物理地址相对应。

route 命令

本命令用于控制网络路由表。该命令只有在安装了 TCP/IP 协议后才可以使使用。

命令格式：route [-f] [-p] [command [destination] [mask subnetmask] [gateway] [metric costmetric]]

《计算机网络技术基础》实验指导书

参数

-f 清除所有网关入口的路由表。如果该参数与某个命令组合使用，路由表将在运行命令前清除。

-p 该参数与 **add** 命令一起使用时，将使路由在系统引导程序之间持久存在。默认情况下，系统重新启动时不保留路由。与 **print** 命令一起使用时，显示已注册的持久路由列表。忽略其他所有总是影响相应持久路由的命令。

command 指定下列的一个命令：

print 打印路由

add 添加路由

delete 删除路由

change 更改现存路由

destination 指定发送 **command** 的计算机。

mask subnetmask 指定与该路由条目关联的子网掩码。如果没有指定，将使用 255.255.255.255。

gateway 指定网关。

metric costmetric 指派整数跃点数（从 1 到 9999）在计算最快速、最可靠和（或）最便宜的路由时使用。

netstat 命令

显示协议统计和当前的 TCP/IP 网络连接。该命令只有在安装了 TCP/IP 协议后才可以使用。

命令格式：**netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]**

-a 显示所有连接和侦听端口。可以有效发现和预防木马，可以知道机器所开的服务等信息，如 FTP 服务、Telnet 服务、邮件服务、WEB 服务等。用法：**netstat -a IP**。

-e 显示以太网统计。该参数可以与 **-s** 选项结合使用。

-n 以数字格式显示地址和端口号（而不是尝试查找名称）。

-s 显示每个协议的统计。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计。

-p 选项可以用来指定默认的子集。**-p protocol** 显示由 **protocol** 指定的协议的连接；**protocol** 可以是 TCP 或 UDP。如果与 **-s** 选项一同使用显示每个协议的统计，**protocol** 可以是 TCP、UDP、ICMP 或 IP。

-r 显示路由表的内容。告诉本地机器的网关、子网掩码等信息。用法：**netstat -r IP**。

interval 重新显示所选的统计，在每次显示之间暂停 **interval** 秒。按 **CTRL+B** 停止重新显示统计。如果省略该参数，**netstat** 将打印一次当前的配置信息。

net 命令

这个命令是网络命令中最重要的一個，它的功能非常强大，它有很多子命令，通过键

《计算机网络技术基础》实验指导书

入 **net /?** 回车可以查看都有哪些命令。

net view: 可以使用此命令查看远端主机的所有共享资源。命令格式为 **net view \\IP 地址/计算机名**。

net use: 把远端主机的某个共享资源映射为本地盘符，命令格式为 **net use x: \\IP\sharename**。如：**net use z: \\192.168.215.1\netsoftbank** 是把 IP 地址为 192.168.215.1 下的共享名为 netsoftbank 的目录映射为本地的 Z 盘；**net use \\192.168.215.1\netsoftbank "password" /user:"name"** 表示和 \\192.168.215.1\netsoftbank 建立连接。

net start: 使用它来启动远端主机上的服务。当和远端主机建立连接后，如果发现想用的某个服务没有启动，就使用这个命令来启动它。用法：**net start servername**。

net stop: 当想停止远端主机的某个服务时，可以和远端主机建立连接后，使用此命令就可以停掉了，用法同 **net start**。

net localgroup: 查看所有和用户组有关的信息和进行相关操作，功能同 **net user**。键入不带参数的 **net localgroup** 即列出当前所有的用户组。如果刚才新建的用户 aaaa 加到 administrator 组里去，方法是：**net localgroup administrators aaaa /add**。

net time: 这个命令可以查看远端主机当前的时间。用法：**net time \\IP**。

net user: 查看和帐户有关的情况，包括新建帐户、删除帐户、查看特定帐户、激活帐户、帐户禁用等。键入不带参数的 **net user** 即列出当前所有的用户。

附录四：Sniffer pro 软件

Sniffer（嗅探器）是一种常用的收集有用数据的方法，分为软件和硬件两种。软件的 Sniffer 易于学习使用和交流，缺点是无法抓取网络上所有的传输，某些情况下也就无法真正了解网络的故障和运行情况。硬件的 Sniffer 通常称为协议分析仪，一般都是商业性的，价格也比较贵。

Sniffer pro 软件是 NAI 公司推出的功能强大的协议分析软件。Sniffer pro 4.6 可以运行在各种 Windows 平台上。

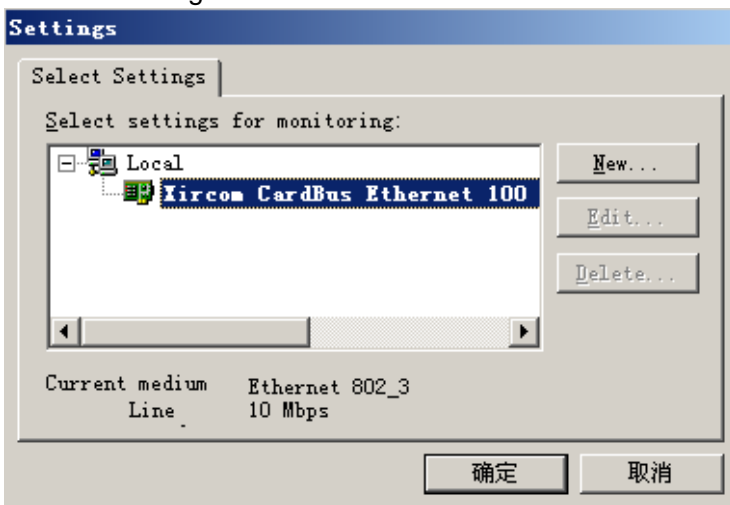
功能简介

下面列出了 Sniffer pro 软件的一些功能，其详细介绍可以参考 Sniffer pro 的在线帮助：

1. 实时监控网络活动；
2. 收集网络利用率和错误等；
3. 捕获网络流量进行详细分析；
4. 利用专家分析系统诊断问题。

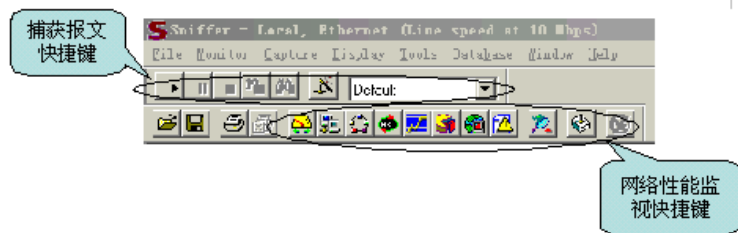
使用方法

在进行流量捕获之前首先应选择网络适配器，确定从计算机的某一网络适配器上接收数据。位置：File->select settings



图附 5-1 选择网络适配器

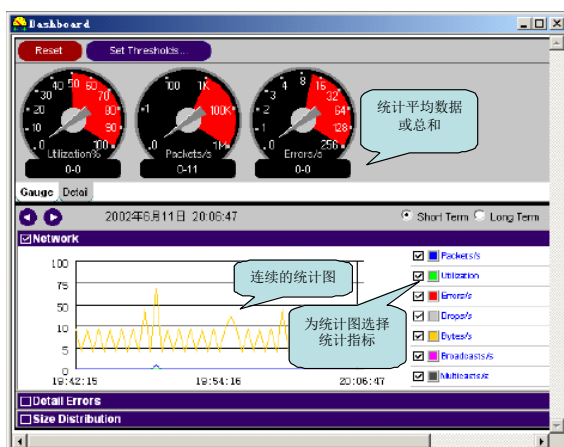
报文捕获及网络性能监视等功能在软件中快捷键的位置如图附 5-2 所示。



图附 5-2 快捷键位置示意图

网络监视功能

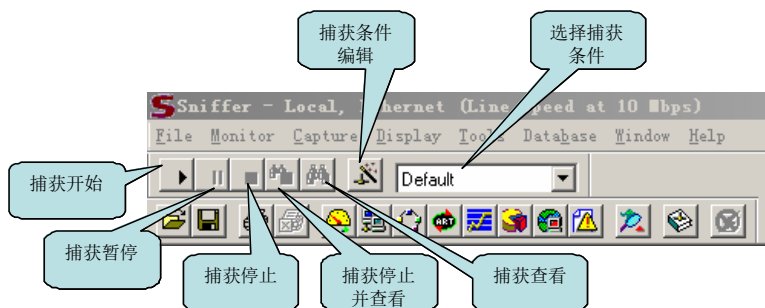
网络监视功能能够时刻监视网络，统计网络上资源的利用率，并能够监视网络流量的异常状况。



图附 5-3 网络监控功能示意图

报文捕获解析

报文捕获功能可以在报文捕获面板中完成，图附 5-4 中显示的是处于开始状态的面板。



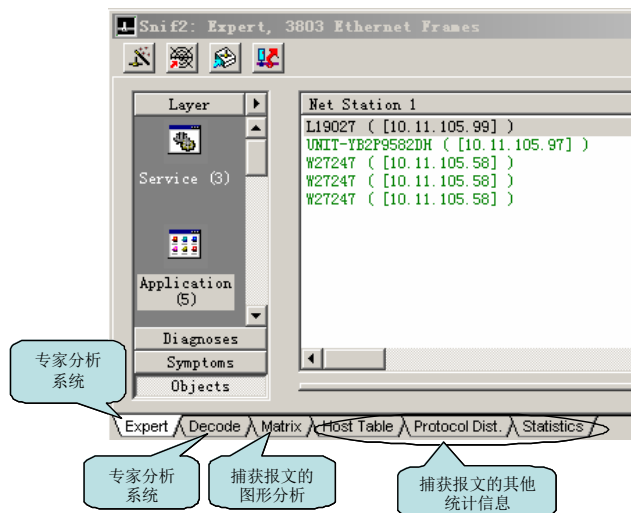
图附 5-4 捕获面板功能图

捕获报文查看

Sniffer pro 软件具有强大的分析解码功能。如图附 5-5 所示，对于捕获的报文提供了

《计算机网络技术基础》实验指导书

专家系统进行分析，还有解码选项及图形和表格的统计信息。

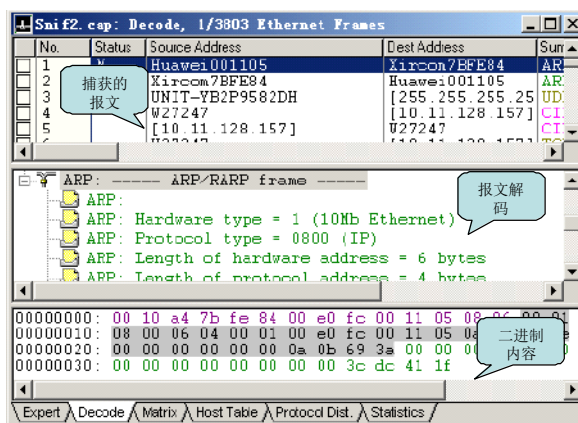


图附 5-5 捕获报文查看示意图

解码分析

图附 5-6 是对捕获报文进行解码的显示，通常分为三部分，目前大部分此类软件都采用这种结构显示。解码主要要求分析人员对协议比较熟悉，这样才能看懂解析出来的报文。使用该软件是很简单的事情，要能够利用软件解码分析来解决问题关键则是要对各种层次的协议了解的比较透彻。工具软件只是提供一个辅助的手段而已。

对于 MAC 地址，Snffier pro 软件进行了头部的替换，如 00e0fc 开头的就替换成 Huawei，这样有利于了解网络上各种相关设备的制造厂商信息。



图附 5-6 报文解码分析

设置捕获条件

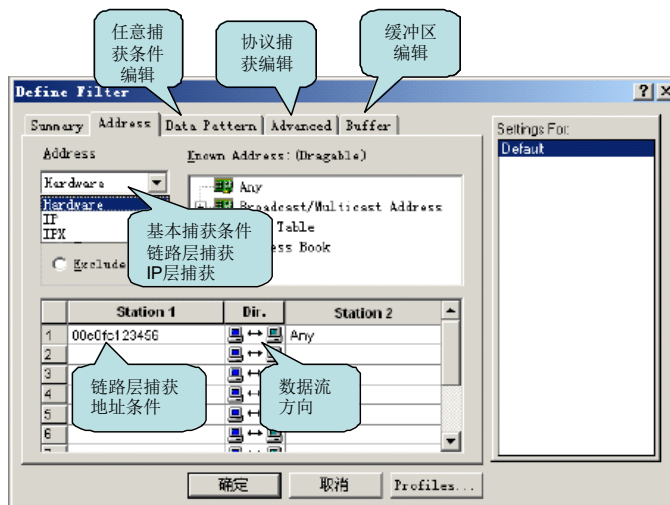
基本捕获条件

基本的捕获条件有两种：

《计算机网络技术基础》实验指导书

1、链路层捕获，按源 MAC 和目的 MAC 地址进行捕获，输入方式为十六进制，如：00E0FC123456。

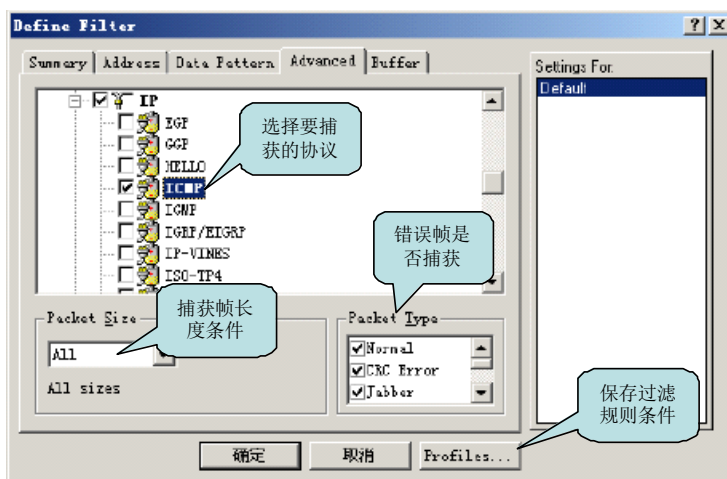
2、IP 层捕获，按源 IP 和目的 IP 进行捕获。输入方式为点间隔方式，如：10.107.1.1。如果选择 IP 层捕获条件，则 ARP 等报文将被过滤掉。



图附 5-7 基本捕获条件

高级捕获条件

在“Advance”页面下，可以编辑特定的协议捕获条件。



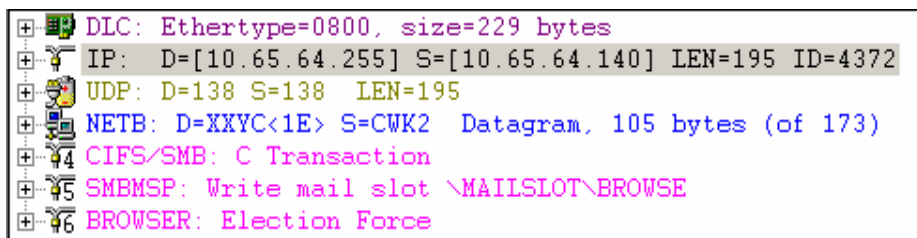
图附 5-8 高级捕获条件

在协议选择树中可以选择需要捕获的协议条件，如果什么都不选，则表示忽略该条件，捕获所有协议。在捕获帧长度条件下，可以捕获等于、小于、大于某个值的报文。在错误帧是否捕获栏，可以选择当网络上有如下错误时是否捕获。可以将当前设置的过滤规则进行保存，在捕获主面板中可以选择保存的捕获条件。

《计算机网络技术基础》实验指导书

数据报文解码分析

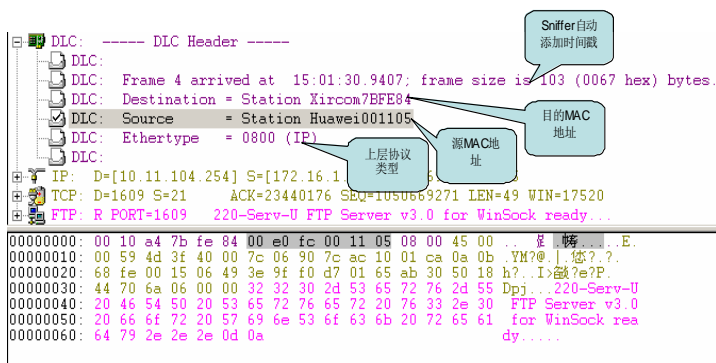
对于四层网络结构，其不同层次完成不同功能。每一层次由众多协议组成。



图附 5-9 数据报文分层

如图附 5-9 所示，在 Sniffer pro 的解码表中分别对每一个层次协议进行解码分析。链路层对应“DLC”；网络层对应“IP”；传输层对应“UDP”；应用层对应的是“NETBT”等高层协议。Sniffer pro 可以针对众多协议进行详细结构化解码分析，并利用树形结构良好的表现出来。

Ethernet II 以太网帧类型报文结构为：目的 MAC 地址(6bytes)+源 MAC 地址(6bytes)+上层协议类型 (2bytes) +数据字段 (46~1500bytes) +校验 (4bytes)。



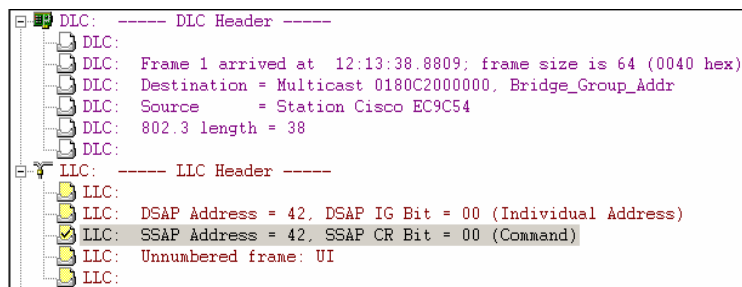
图附 5-10 Ethernet II 以太网帧类型报文

Sniffer pro 会在捕获报文的时候自动记录捕获的时间，在分析问题提供了很好的时间记录。

源目的 MAC 地址在解码框中可以将前 3 字节代表厂商的字段翻译出来，方便定位问题，例如网络上 2 台设备 IP 地址设置冲突，可以通过解码翻译出厂商信息，方便将故障设备找到，如 00e0fc 为华为，010042 为 Cisco 等等。如果需要查看详细的 MAC 地址，则用鼠标在解码框中点击此 MAC 地址，在下面的表格中就会突出显示该地址的 16 进制编码。

上层协议的类型主要包括 0x800 为 IP 协议，0x806 为 ARP 协议。

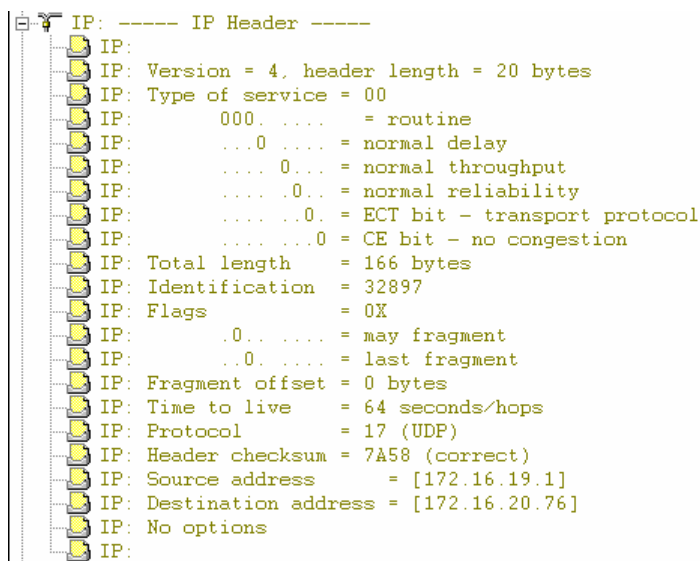
IEEE 802.3 以太网报文



图附 5-11 IEEE 802.3 以太网报文

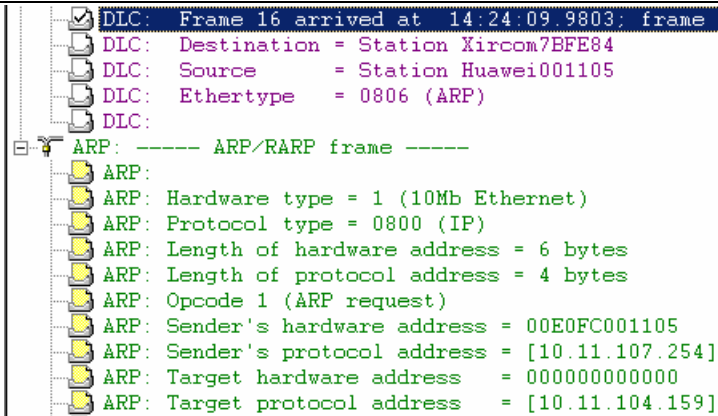
图附 5-11 为 IEEE 802.3 帧结构，与 Ethernet II 不同点是目的和源地址后面的字段代表的不是上层协议类型而是报文长度，并多了 LLC 子层。

IP 报文结构为 IP 协议头+载荷，其中对 IP 协议头部的分析是主要内容之一。这里给出了 IP 协议头部的一个结构。

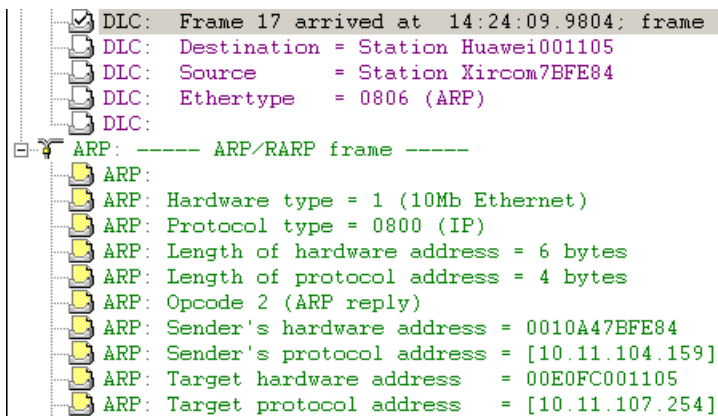


图附 5-12 IP 报文结构

图附 5-13 和图附 5-14 分别是通过 Sniffer pro 解码的 ARP 请求和应答报文的结构。



图附 5-13 ARP 请求报文结构



图附 5-14 ARP 应答报文结构

附录五：Windows 环境下的用户配置和管理

1. 用户是 Windows 2008 server 中一个很重要的概念，用户权限好比员工在公司有不同的业务，有不同的活动范围，要保证工作组织的有序，最基本的要求就是要标识不同的员工，并保证不同员工从事他们应该的工作。Windows 2008 server 提供基于用户的安全性，任何人访问某一主机时，都必须有一种身份，也就是账号。其中 Guest 账号的作用是：当用户访问网络中的某一台主机身份不能被验证时，如果此时 Guest 账号被 Enable，则系统会自动赋予他 Guest 账号的身份，让他以 Guest 账号访问主机，否则，将被拒绝访问。

2. 组是用户账号的集合。用组来管理是一种有效的管理手段，组可以向用户一样被赋予权限和许可，组内的用户可获得组所具有的权限和许可。管理员可以使用简化用户对资源的管理，避免多次重复此操作。

本地组是本地用户账户的集合，与域中基于 AD（活动目录）的组相区别，本地组仅存在于本地，本地组是非域控制器的 Windows 2008 server 上创建的，所以本地组就像本地用户一样，只存在于本地计算机中，只在本地起作用。

3. Windows 2008 server 在安装完成后，进入账号管理器时，即使没有建立任何账号和组，也会看到许多用户和组，称之为内置账号和组。除本地账户外系统还内建了本地的组，这些本地的组是根据用户访问系统资源的权限划分的。

内置本地账号包括 Administrator 和 Guest：

Administrator 是本地管理员账号。在安装 windows 2008 server 系统后，第一次都需要使用管理员账号。Administrator 拥有管理用户账号、管理共享资源、管理磁盘和文件系统、系统配置和管理、以及软件和硬件的安装权限。总之管理员拥有对系统完全控制的权利，所以密码应妥善保管。

Guest 是客户的访问账号，如果系统允许所有人都可以访问时，Guest 账号是非常有用的。

内置本地组包括：Administrators 管理员组、Backup operators 和 Power user：

Administrators 管理员组是系统中权限最高的组，让用户成为系统管理员的方法就是让用户成为这个组的成员。管理员组的成员可以进行以下工作：安装服务包、升级操作系统、修复操作系统、配置操作系统的关键设置（如：密码策略，访问控制）获得无访问权的所有权（管理员组成员并不能无条件的访问所有资源，在 NTFS 文件系统中，当文件所有权限限制管理员的访问时，管理员可以通过获得所有权的操作来访问到这些资源，也就是赋予自己这方面的权利）、管理安全日志和审计日志、备份和恢复系统、安装操作系统和组件（包括硬件驱动程序和系统服务）。

Backup operators 备份操作组是系统中实现安全性管理很重要的组。它的成员可以不受文件访问权限的限制，备份和恢复计算机上的文件。这意味着，系统中任何关键文件、数据，这个组的成员都可以进行备份，所以这个组的成员应该严格控制。

Power user 这个组的成员的权限介于用户组和管理员组之间，可进行系统中一般的管

《计算机网络技术基础》实验指导书

理工作。他不能通过获得文件所有权的办法在 NTFS 分区上访问其他用户的数据，不能对 Administrator，Backup Operators 组的成员进行修改。

4. 创建用户账号必须注意：

(1) 用户名长度不得超过 20 个字符，不能使用诸如 \/:;|=,+-?*[] 这 12 个字符

(2) 密码长度最多长达 128 字符，为了保护未授权用户访问他人的资源，希望为用户建立密码；密码作为身份验证的关键信息，应该避免过于简单，建议使用大写，小写字母，符号以及数字组成密码。

5. 更名和删除用户账号：

在 Windows 2008 server 创建用户账号后，系统分配给此账号一个唯一的安全标识码 SID (Security Identifier)。它与用户名无关，重命名操作不会修改 SID，因此能够继承原有用户名所对应的权限，避免管理员重新为其分配权限。如果公司内发生人事调动，不必创建新用户，只需修改原有的用户名，并将其分配给代替者即可。

由于不是永久性的原因，Windows 2008 server 一般不推荐使用删除操作。删除账号，实际删除了账号对应的 SID，即使用户再次创建同一用户名的账号，其所获的 SID 也不同，原先的权限及许可都会丢失，需要重新分配。

6. 账号创建完之后，管理员可以对用户的“常规”属性进行以下配置：

“用户下次登录时需修改密码”如果选中用户登录时系统会自动提示修改密码，更改后此选项会自动去掉；

“用户不能更改密码”管理员可以决定是否不允许用户修改密码，一般情况下，建议将修改密码的权利赋予用户；

“密码永不过期”用户账号是否受密码过期策略的限制；

“账号已停用”如果组织成员或公司职员离职，可以不删除账号，等新的替代者到来后，可以通过修改用户名和密码，将此账号分配给替代者并使其继承原有的权限；

“锁定账号”账号只有锁定时才可选，当用户账号因为一定次数的登录失败，而被锁定时，管理员可以清除此复选框，解除用户的锁定，这个账号便可以重新使用。

“隶属于”可以把选定的账号加入到不同的组中。

7. 安全策略和 NTFS 文件系统的权限是 Windows 2008 server 的系统安全性两个首要条件。NTFS 文件系统的权限设置，是用来提供对文件访问的安全性的，同时通过对 Windows 2008 server 系统文件的权限的设置，也提供对系统一定程度的保护。而安全策略则是直接对系统本身的一些操作提供的安全性保护，用来实现 Windows 2008 server 计算机和用户的控制。

在本地安全策略中，最基本的是“账号策略”和“本地策略”：

账号策略：是用户账号安全性的增强，包括：“密码策略”“账号锁定策略”

本地策略是对本机系统的安全性的配置，包括：“审核策略”、“用户权利指派”和“安全选项”。

密码策略主要有：

“密码必须符合复杂性要求”

"密码长度最小值"

"密码最长保留期"

"密码最短保留期"

"强制密码历史"

"为域中所有用户使用可以还原的加密储存密码"

账号锁定策略是用来对付试探口令的黑客行为。账号可以在指定的次数的口令试探后锁定，也就是不能再使用。对一般的账号可以设定在一段时间后解锁，这样就可以大大减慢试探口令的速度。对于关键账号可以一直锁定到管理员来处理。包括：

"账号锁定阈值" 当用户开始输入口令时，系统内部有一个计数器开始记录错误的口令的次数，当这个次数达到这个阈值参数后，账号就被锁定。这个值 0 表示不锁定。（在锁定计算机和屏幕保护中输入的错误口令不在计数器的记录范围中）

"账号锁定时间"这个时间是用户的账号被锁定后自动解开锁需要的时间。可以选择的范围是 1~99999 分钟，0 表示一直保持锁定直到管理员在"用户管理"工具中先手工解除锁定。

"复位账号锁定计数器"这个设置用来指定账号锁定计数器的复位时间，范围也 1~99999 分钟。这个值不能大于锁定时间的值，也就是要在账号解锁之前复位。

审核策略配置的是对系统行为的审核，也就是将某些操作的成功或失败记录在事件日志中。一般情况下可以对操作的成功和失败都进行记录，主要有：

审核登录事件：用户在本机的登录；

审核账号登录事件：用户在其它计算机上登录，但是用户的身份验证是在这台计算机上进行的；

审核账号管理：对账号的管理操作，如建立用户和组，修改重命名用户和组，修改和重置口令；

审核对象访问：用户对对象的访问（文件，文件夹，系统注册表，打印机）。具体到某个对象，如某个文件的审核，还需要在文件本身的属性安全性选项中指定审核。

审核系统事件：系统的启动和关机，对系统安全性产生影响的一些事件；

用户权利用来对计算机上进行某种操作进行授权。用户权利可以分为两种类型：登录权利和特权。登录权利可以控制用户和其他对象访问计算机，可以通过键盘登录或是通过网络连接登录；登录者可以是一个用户也可以是一个服务，或者是某个批处理的作业。特权可以控制用户操作系统资源，例如：装载或是卸载驱动程序，备份或是恢复文件和文件夹。允许用户本地登录：为了保证系统的安全，不让所有用户都能够在服务器上登录，只有需要完成必要任务的用户才可以在服务器上本地登录。

注：默认情况下 Administrator 组和 Account Operators 组，Backup Operators 组，Server Operators 组的成员有本地登录的权利。

用户权利还有其它的一些策略配置如"允许用户关闭系统"、"备份文件和目录"

8. 作为一个网络操作系统，跟踪并记录服务器中发生的事件很必要，日志文件就是记录操作系统发生事件的文件。根据日志文件，可以发现很多有用的信息和线索，为管理员正确掌握服务器工作情况提供了第一手资料。

附录六：双绞线及 EIA/TIA-568 标准

局域网中常见的网线有双绞线、同轴电缆、光缆三种。双绞线，是由许多对线组成的数据传输线。分 STP 和 UTP 两种，我们常用的是 UTP。

STP(屏蔽双绞线)：内有一层金属隔离膜，在数据传输时可减少电磁干扰，稳定性高。STP 的双绞线的价格较高，便宜的几元 1 米，贵的十几元 1 米。

UTP(非屏蔽双绞线)：内没有金属膜，稳定性较差，价格便宜，一般在几角至 2 元多 1 米不等。

双绞线由 8 根不同颜色的线分成 4 对绞合在一起，成对扭绞的作用是尽可能减少电磁辐射与外部电磁干扰的影响。在 EIA/TIA-568 标准中，将双绞线按电气特性区分为：双绞线常见的有 3 类线、4 类线、5 类线和超 5 类线、6 类线，以及最新的 7 类线。前者线径细而后者线径粗，网络中最常用的是三类线和五类线。

1)一类线：主要用于传输语音(一类标准主要用于八十年代初之前的电话线缆)，不同于数据传输。

2)二类线：传输频率为 1MHz，用于语音传输和最高传输速率 4Mbps 的数据传输，常见于使用 4Mbps 令牌传递协议的旧的令牌网。

3)三类线：在 ANSI 和 EIA/TIA568 标准中指定的电缆，该电缆的传输频率 16MHz，用于语音传输及最高传输速率为 10Mbps 的数据传输主要用于 10BASE-T。

4)四类线：该类电缆的传输频率为 20MHz，用于语音传输和最高传输速率 16Mbps 的数据传输主要用于基于令牌的局域网和 10BASE-T/100BASE-T。

5)五类线：该类电缆增加了绕线密度，外套一种高质量的绝缘材料，传输率为 100MHz，用于语音传输和最高传输速率为 100Mbps 的数据传输，主要用于 100BASE-T 和 100BASE-T 网络。这是最常用的以太网电缆。

6)超五类线：超 5 类具有衰减小，串扰少，并且具有更高的衰减与串扰的比值(ACR)和信噪比(Structural Return Loss)、更小的时延误差，性能得到很大提高。超 5 类线的最大传输速率为 250Mbps。

7)六类线：该类电缆的传输频率为 1MHz~250MHz，六类布线系统在 200MHz 时综合衰减串扰比(PS-ACR)应该有较大的余量，它提供 2 倍于超五类的带宽。六类布线的传输性能远远高于超五类标准，最适用于传输速率高于 1Gbps 的应用。六类与超五类的一个重要的不同点在于：改善了在串扰以及回波损耗方面的性能，对于新一代全双工的高速网络应用而言，优良的回波损耗性能是极重要的。六类标准中取消了基本链路模型，布线标准采用星形的拓扑结构，要求的布线距离为：永久链路的长度不能超过 90m，信道长度不能超过 100m。

8)超六类线：超六类线是六类线的改进版，同样是 ANSI/EIA/TIA-568B.2 和 ISO 6 类/E 级标准中规定的一种非屏蔽双绞线电缆，主要应用于千兆位网络中。在传输频率方面与六类线一样，也是 200~250 MHz，最大传输速度也可达到 1 000 Mbps，只是在串扰、衰减和信噪比等方面有较大改善。

《计算机网络技术基础》实验指导书

9)七类线:该线是 ISO 7 类/F 级标准中最新的一种双绞线,它主要为了适应万兆位以太网技术的应用和发展。但它不再是一种非屏蔽双绞线了,而是一种屏蔽双绞线,所以它的传输频率至少可达 500 MHz,是六类线和超六类线的 2 倍以上,传输速率可达 10 Gbps。

(资料来源: <http://baike.so.com/doc/100934-106503.html>)

EIA / TIA 的布线标准中规定了两种双绞线的线序 568A 与 568B。

标准 568A: 绿白--1, 绿--2, 橙白--3, 蓝--4, 蓝白--5, 橙--6, 棕白--7, 棕--8;

标准 568B: 橙白--1, 橙--2, 绿白--3, 蓝--4, 蓝白--5, 绿--6, 棕白--7, 棕--8;

在整个网络布线中应采用同一种布线方式,但两端都有 RJ-45 接口的网络连线无论是采用端接方式 A,还是端接方式 B,在网络中都是通用的。双绞线的顺序与 RJ-45 头的引脚序号一一对应。10 M 以太网的网线使用 1, 2, 3, 6 编号的芯线传递数据,100 M 以太网的网线同时还使用 4, 5, 7, 8 编号的芯线传递数据。由于按 100 M 方式制作的网线 10 M 网卡也能够使用,因而即使使用 10 M 网卡,一般也按 100 M 网卡要求来制作网线。

附录七：网线制作

步骤 1：利用斜口钳的剥线口将所给双绞线的外皮剥去 2~3 cm。

步骤 2：接下来就要进行拨线的操作。将裸露的双绞线按橙、绿、蓝、棕（A 标准按绿、橙、蓝、棕）四对线从左向右排列；

步骤 3：小心地剥开每一对线，注意每一对浅色线在前，深色线在后。排列如下

（以 B 标准为例）左起：白橙 / 橙 / 白绿 / 绿 / 白蓝 / 蓝 / 白棕 / 棕

（以 A 标准为例）左起：白绿 / 绿 / 白橙 / 橙 / 白蓝 / 蓝 / 白棕 / 棕

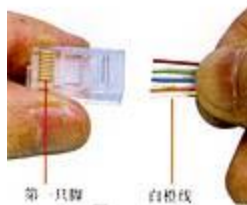
步骤 4：把第二对线分开，第三对线包中间，第三对线的深色线与浅色线对调。

B 标准为：白橙 / 橙 / 白绿 / 蓝 / 白蓝 / 绿 / 白棕 / 棕；

A 标准为：白绿 / 绿 / 白橙 / 蓝 / 白蓝 / 橙 / 白棕 / 棕。

注意：常见的错误接法是将绿色线放到第 4 只脚的位置。应该将绿色线放在第 6 只脚的位置才是正确的，因为在 100 base-T 网络中，第 3 只脚与第 6 只脚是同一对的，所以需要使用同一对线。

步骤 5：将裸露出的双绞线用剪刀或斜口钳修剪，只剩约 14 mm 的长度（**注意：**剪完线之后手就不要再动了，排完线向水晶头插入时，要求铜片向上，插入口朝向自己），最后再将双绞线的每一根线依序放入 RJ-45 接头的引脚内，第一只引脚内（左起为 1）应该放白橙色的线，其余类推，如图附 7-1 所示。



图附 7-1 接线示意图

步骤 6：确定双绞线的每根线已经正确放置（排线顺序是否正确，每根线是否顶到头）之后，就可以用 RJ-45 压线钳压接 RJ-45 接头，这样一个头就做好了。

说明：100 BASE-T 4 对双绞线的规定如下：

1、2 用于发送，3、6 用于接收，4、5，7、8 是双向线。

其中 1、2，3、6，4、5，7、8 分别双绞在一起。

做好的网线要将 RJ45 水晶头接入网卡或 HUB 等网络设备的 RJ45 插座内。相应地 RJ45 插头座也区分为三类或五类电气特性。RJ45 水晶头由金属片和塑料构成，制作网线

《计算机网络技术基础》实验指导书

所需要的 RJ-45 水晶接头前端有 8 个凹槽，简称"SE"(Position，位置)。

凹槽内的金属触点共有 8 个，简称"8C"(Contact，触点)，因此业界对此有"8P8C"的别称。特别需要注意的是 RJ45 水晶头引脚序号，当金属片面对我们的时候从左至右引脚序号是 1~8，序号对于网络连线非常重要，不能搞错。

有一种 RJ-45 接头的保护套，可以防止接头在拉扯时造成接触不良。使用这种保护套时，需要在压接 RJ-45 接头之前就将这种胶套插在双绞线电缆上。

用 RJ-45 测线仪对线路进行通断测试时，发射端的 8 个绿灯依次闪烁，接收端灯亮的顺序依次是 3、6、1、4、5、2、7、8。

我们将两端线序排列相同的网线称为正线（Normal Line），即同为 A 标准或同为 B 标准，而将两端线序排列不同的网线称为反线（级联线），即一端为 A 标准，另一端为 B 标准。对于网络设备普遍遵循的接口类型而言，连接同种类型（同为 MDI 或 MDIX）的接口必须使用反线，而连接不同类型的接口必须使用正线。PC 机网卡接口，集线器级连口为 MDI 类型接口；集线器普通口为 MDIX 类型接口。

对不同用途的网线，水晶头的制作方法不同，规则如下表：

网线的用途	水晶头的做法
计算机 \longleftrightarrow HUB/交换机	A \longleftrightarrow A/B \longleftrightarrow B
计算机 \longleftrightarrow 计算机	A \longleftrightarrow B
HUB/交换机 \longleftrightarrow 下级 HUB/交换机（普通口）	A \longleftrightarrow B
HUB/交换机 \longleftrightarrow 下级 HUB/交换机（UPLINK 口）	A \longleftrightarrow A/B \longleftrightarrow B

附录八、如何读懂路由表

我们可以通过“开始”→“程序”→“命令提示符”进入命令提示符状态，键入“route print”就可以查看本机的路由表。下面是某台计算机的 IPv4 路由表。

```
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          166.111.60.1     166.111.60.77    20
127.0.0.0                  255.0.0.0        127.0.0.1        127.0.0.1        1
166.111.60.0               255.255.254.0    166.111.60.77    166.111.60.77    20
166.111.60.77              255.255.255.255  127.0.0.1        127.0.0.1        20
166.111.255.255            255.255.255.255  166.111.60.77    166.111.60.77    20
192.168.10.0               255.255.255.0    192.168.10.1     192.168.10.1     20
192.168.10.1               255.255.255.255  127.0.0.1        127.0.0.1        20
192.168.10.255             255.255.255.255  192.168.10.1     192.168.10.1     20
224.0.0.0                  240.0.0.0        166.111.60.77    166.111.60.77    20
224.0.0.0                  240.0.0.0        192.168.10.1     192.168.10.1     20
255.255.255.255            255.255.255.255  166.111.60.77    166.111.60.77    1
255.255.255.255            255.255.255.255  192.168.10.1     192.168.10.1     1
Default Gateway:          166.111.60.1
=====
Persistent Routes:
None
```

上图中 Active Routes: 活动路由；Network Destination: 目的网段；Netmask: 子网掩码；Gateway: 网关，下一跳路由器入口的 IP；Interface: 到达该目的地的本地路由器的出口 IP；Metric: 跳数，也是该条路由记录的质量，一般情况下，如果有多条到达相同目的地的路由记录，路由器会选用 Metric 值小的那条路由。

第一条是缺省路由，目的网段为 0.0.0.0，当接收到一个数据包的目的网段不在你的路由记录中，会将此数据包通过 166.111.60.77 这个接口发送到 166.111.60.1 这个地址，这个地址是下一个路由器的一个接口，这个数据包就可以通过 166.111.60.77 这个接口交付给下一个路由器来处理。该路由记录的线路质量为 20。

第二条是本地环路，目的网段为 127.0.0.0 的，当接收到这样的一个数据包，则说明这个数据包是指向自己的。该路由记录的线路质量为 1。

第三条是直连网段的路由记录，目的网段为 166.111.60.0 的，当接收到这样的一个数据包时，则会将此数据包通过 166.111.60.77 这个接口直接发送出去。观察发现 interface 和 gateway 同是 166.111.60.77，这说明这个端口直接连接着 166.111.60.0 网段。该路由记录的线路质量为 20。

第四条本地主机路由，目的网段为 166.111.60.77，观察这条路由表发现此地址是本地的 IP 地址，当接收到一个数据包的目的网段是 166.111.60.77 时，把该数据包收下，因为这个数据包是发送给本地的，该路由记录的线路质量 20

第五条本地广播路由，目的网段为 166.111.255.255，子网掩码也均为 255，当接收到这样的一个数据包时，则会将此数据包通过 166.111.60.77 这个接口以广播的形式发送出去，该路由记录的线路质量 20。

《计算机网络技术基础》实验指导书

第六条同第三条，第七条同第四条，第八条同第五条。

第九条是组播路由，目的网段为 224.0.0.0，子网掩码也均为 255，当收到这样的一个组播数据包时，会将此数据包通过 166.111.60.77 这个接口以组播的形式发送出去，该路由记录的线路质量 20。

第十条同第九条

第十一条是广播路由，目的网段为 255.255.255.255，子网掩码也均为 255，当收到这样的一个广播数据包时，表示向整个网络广播。此时会将此数据包通过 166.111.60.77 这个接口以广播的形式发送出去，目的是为了找到目标计算机。当找到后，路由器会将 IP 地址与 MAC 地址绑定这就是所谓的地址学习。该路由记录的线路质量 1。

第十二条同第十一条