项目一　集成公司办公网络实施

项目描述

ABC公司由于业务发展的需求，将营销团队独立出来，成立了另外一个独立的子公司DEF公司。DEF公司从今后公司网络运营、商业机密角度考虑，请该营销团队计算机专业毕业的员工小王和小李组建公司的办公网络环境。计算机专业的小王和小李也仅仅对网络搭建有所了解，并不能完全胜任公司组网的要求，为此，首先要学习网络搭建的相关知识，尤其是路由器和交换机等网络接入设备的相关知识，其次要进行公司网络的基本规划，最后要进行配置，并接入互联网。

如图1-1-1所示为小王和小李为DEF公司规划的拓扑图。为完成公司的办公网络，他们分三个阶段来学习和实践。首先从内网接入开始学习，其次再进行互联网的接入，最后考虑如何更好地让终端用户很容易获取IP地址。

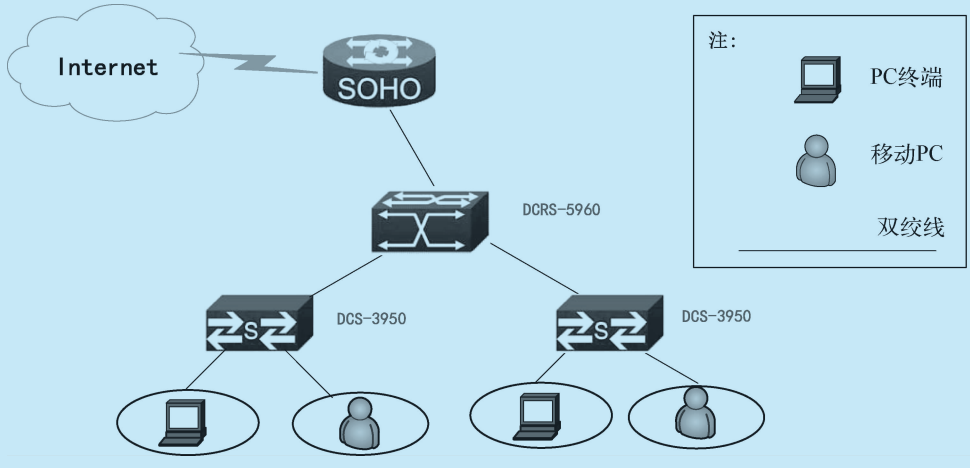

图1-1-1　网络拓扑图

能力目标

1. 了解交换机的基础知识。
2. 了解路由器的基础知识。
3. 掌握宽带接入的基础知识。
4. 掌握交换机、交换机设备的配置方式。
5. 掌握 VLAN 的工作原理及配置方式。
6. 掌握交换机 HDCP 的工作原理及配置方式。
7. 掌握无线宽带路由器的配置方式。

职业素养

1. 培养主动学习的意识。
2. 学会获取资料的多种方式。
3. 增强面试过程中的应试能力。
4. 积极关注行业发展动态。

任务一　内网终端接入

一、任务描述

随着计算机及其互联技术(即通常所谓的“网络技术”)的迅速发展,以太网成为了迄今为止普及率最高的短距离二层计算机网络,而以太网的核心部件就是以太网交换机。以太网交换机作为局域网的主要连接设备,已经成为应用普及最快的网络设备之一,其中二层交换技术的发展比较成熟。二层交换机属于数据链路层设备,可以识别数据包中的 MAC 地址信息,根据 MAC 地址进行转发,并将这些 MAC 地址与对应的端口记录在自己内部的一个地址表中。小王和小李将重点学习使用二层交换机(通常所说的交换机)接入内网的知识及相关操作。

二、任务目标

1. 认识交换机。
2. 进行交换机电源连接及加电。
3. 连接交换机 Console 线缆。
4. 配置 Console 口管理交换机实现带外管理。
5. 配置 Telnet 管理交换机实现带内管理。

6. 认识并管理交换机的 MAC 地址表。
7. 使用 Ping 命令进行连通性测试。

三、任务使用设备清单

1. 神州数码 DCS－3950－28CT，如图 1－1－2 所示。

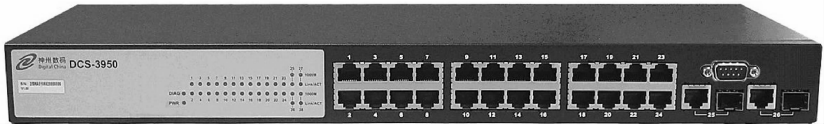

图 1－1－2　DCS－3950－28CT

2. PC：4 台台式计算机。
3. 神州数码专用 Console 线，如图 1－1－3 所示。

图 1－1－3　Console 线

四、任务相关知识和技能储备

1. 认识神州数码 DCS－3950－28CT 交换机

（1）观察交换机，并阅读交换机正面介绍后填写表格中的内容

如图 1－1－4 所示，从左到右分别是 DCS－3950－28CT 交换机的品牌及型号，电源及接口 LED 工作指示灯（如图 1－1－5 所示，LED 指示灯状态描述见表 1－1－1），以太网接口，Console 配置口（该接口的放大图如图 1－1－6 所示，也可称之为 DB－9 串口端口），光纤接

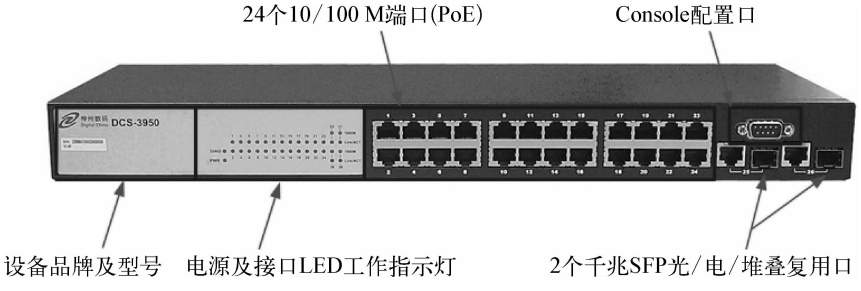

图 1－1－4　DCS－3950－28CT 交换机正面板

口。同时，还可以看到该交换机提供了 24 个 10/100 Mbps 以太网接口和 2 个千兆单膜光纤接口。

DCS－3950 系列交换机的 LED 指示灯包括 PWR、DIAG、Link/Act 和 1 000 M 指示灯。DCS－3950－28CT 交换机 LED 指示灯如图 1－1－5 所示。

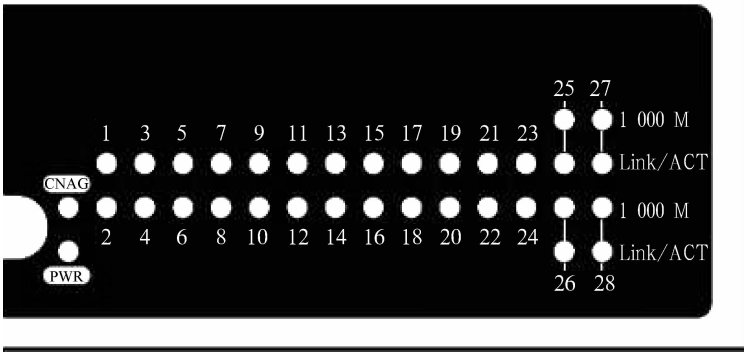

图 1－1－5　DCS－3950－28CT 交换机 LED 指示灯

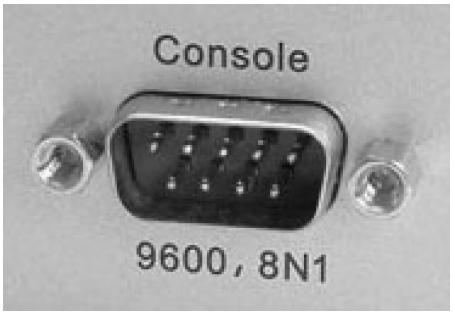

图 1－1－6　DB－9 串口端口

表 1－1－1　DCS－3950－28CT 交换机 LED 指示灯状态描述

LED	状　态	说　明
Link/ACT	闪　烁	端口 link 成功，正在收发数据
	熄　灭	端口处于 down 状态
	点　亮	link 成功
1 000 M 指示灯	点　亮	对应 G 口处于 1 000 M 连接状态
	熄　灭	对应 G 口处于 100 M 连接或者 down 状态
PWR	点　亮	电源已接通
	熄　灭	电源未接通
DIAG	绿色闪烁	程序初始化
	点　亮	程序初始化结束
	玻珀色闪烁	程序初始化失败

（续表）

观察对象	类型或功能描述	接口特性(性能)描述	通用标识
Console			
接口 1～26			
接口 27～28			

（2）阅读神州数码 DCS－3950－28CT 参数说明(表 1－1－2)

表 1－1－2 参数说明

主要参数	产品类型：运营级接入交换机 传输速率：10/100 Mbps 交换方式：存储、转发 背板带宽：48 Gbps 包转发率：9.6 Mpps MAC 地址表：16 K
端口参数	端口结构：非模块化 端口数量：28 个 端口描述：24 个 10/100 Mbps 端口(PoE)，2 个千兆 SFP 光/电/堆叠复用口，2 个千兆电/堆叠复用口
功能特性	堆叠功能：可堆叠 QOS：最大可支持 8 个端口队列 支持 802.1p，ToS，DSCP 端口优先级 支持 WRR/SP 等调度方式 组播管理：IGMP Snooping Query 纠错 网络管理：CLI、WEB、Telnet 管理界面 SNMP 系统日志 配置管理分级 SSH RMON 提供 MIB 接口 集中网管软件 Security IP 安全网管功能
其他参数	电源电压：AC 110 V～240 V，50 Hz～60 Hz 产品尺寸：440 mm×350 mm×44 mm 环境标准：工作温度为 0～50℃ 相对湿度：5%～95%(无凝结)

2. 进行交换机电源连接及加电

DCS－3950 系列后面板示意图如图 1－1－7 所示。

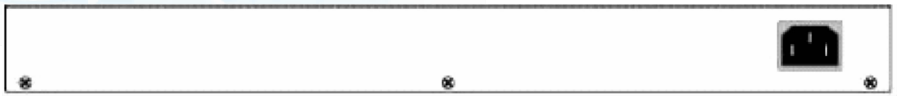

图 1－1－7　DCS－3950 系列后面板示意图

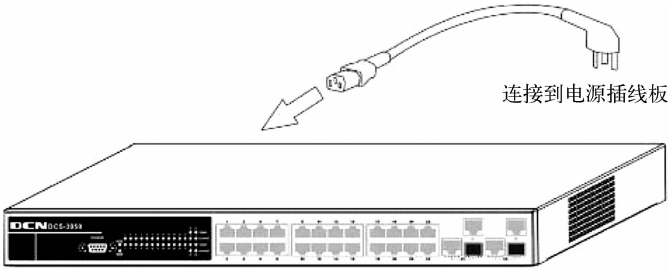

图 1－1－8　将电源线连接到 DCS－3950 系列交换机

DCS－3950 系列可堆叠智能安全以太网接入交换机的电源规格是 AC 100 V～240 V，50 Hz～60 Hz，可以适应一定范围内的电压浮动。请按照如下步骤连接电源线：

① 将电源线的一端插到交换机后面板上的电源插槽中，另一端插到标准的带过载和漏电保护的电源插座上。

② 检查交换机前面板上的 Power 指示灯是否点亮。DCS－3950 系列以太网交换机可根据电源的输入电压自动调节。因此，只要输入电压符合后面板上所标明的电压范围，交换机就可正常运行，而无须额外的调试。

③ 交换机加电后，将自动执行自检。

注意

输入电压必须符合交换机电源规格，不然可能损坏交换机或使交换机工作不正常，减少其使用寿命。如果电源加电后 Power 指示灯不亮或自检不正常，请与经销商或神州数码网络客户服务中心联系，不要擅自拆卸交换机机壳，以免造成损失和人身伤害。

3. 连接交换机 Console 线缆

DCS－3950 系列可堆叠智能安全以太网接入交换机提供了一个 DB－9 的异步串行 Console 配置口。连接图如图 1－1－9 所示，请按照如下步骤连接 Console 线：

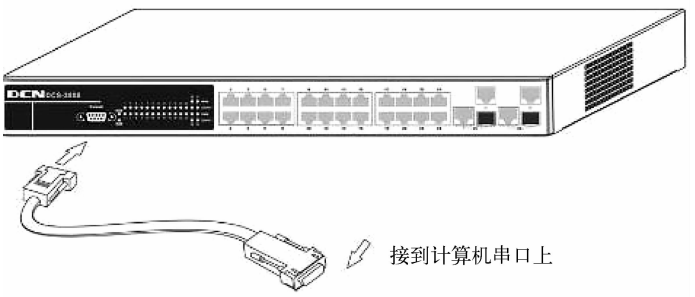

图 1－1－9　将 Console 线缆连接到交换机上

① 将 DB－9 的 Console 线缆一端连接到交换机的 Console 端口中。

② 将 Console 另一端连接到一台字符终端(通常是计算机)上。

③ 在交换机和计算机都已加电后,通过计算机可以与交换机建立管理配置连接。

注意

请使用交换机附带的 Console 线缆和 Console 转接头,不要将 Console 线缆误插到其他端口中,也不要将其他线缆误插到 Console 端口中,以免损坏线缆和端口。

读一读

交 换 机 管 理

用户购买到交换机后,需要对交换机进行配置,从而实现对网络的管理。神州数码交换机为用户提供了两种管理方式:带外管理和带内管理。

带外管理即通过 Console 口进行管理,通常情况下,在首次配置交换机或者无法进行带内管理时,用户会使用带外管理方式。

所谓带内管理(In-band management),即通过 Telnet 程序登录到交换机,或者通过神州数码网络(北京)有限公司自主研究的网络管理软件 LinkManager 对交换机进行配置管理。交换机提供带内管理方式可以使连接在交换机上的某些设备具有管理交换机的功能。当交换机的配置出现变更而导致带内管理失效时,可以使用带外管理对交换机进行配置管理。此处我们重点介绍通过 Telnet 管理交换机。

4. 配置 Console 口管理交换机实现带外管理

用户希望通过远程 Telnet 来访问交换机时,必须首先通过 Console 口给交换机配置一个 IP 地址。用户用 Console 口管理的步骤如下:

(1) 搭建环境

如图1－1－10所示,将 PC 的串口(RS－232 接口)和交换机通过 DB－9串口线连接,表 1－1－3 是连接中用到的设备说明。

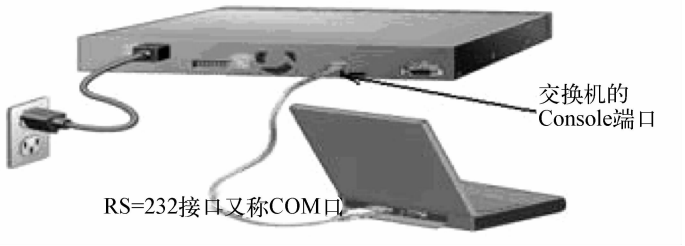

图 1－1－10 带外管理配置环境

表 1－1－3 设备说明

设 备 名 称	说 明
PC 机	有完好的键盘和 RS－232 串口,并且安装了终端仿真程序,如 Windows 9X/NT/2000/XP 自带的超级终端等
串口线	一端与 PC 机的 RS－232 串口相连,另一端与交换机的 Console 口相连
DSC－3950－28C	有完好的 Console 口

（2）进入超级终端

连接成功后，打开 Windows 系统自带的超级终端。以下是 Windows XP 打开自带的超级终端的步骤。

① 点击超级终端：

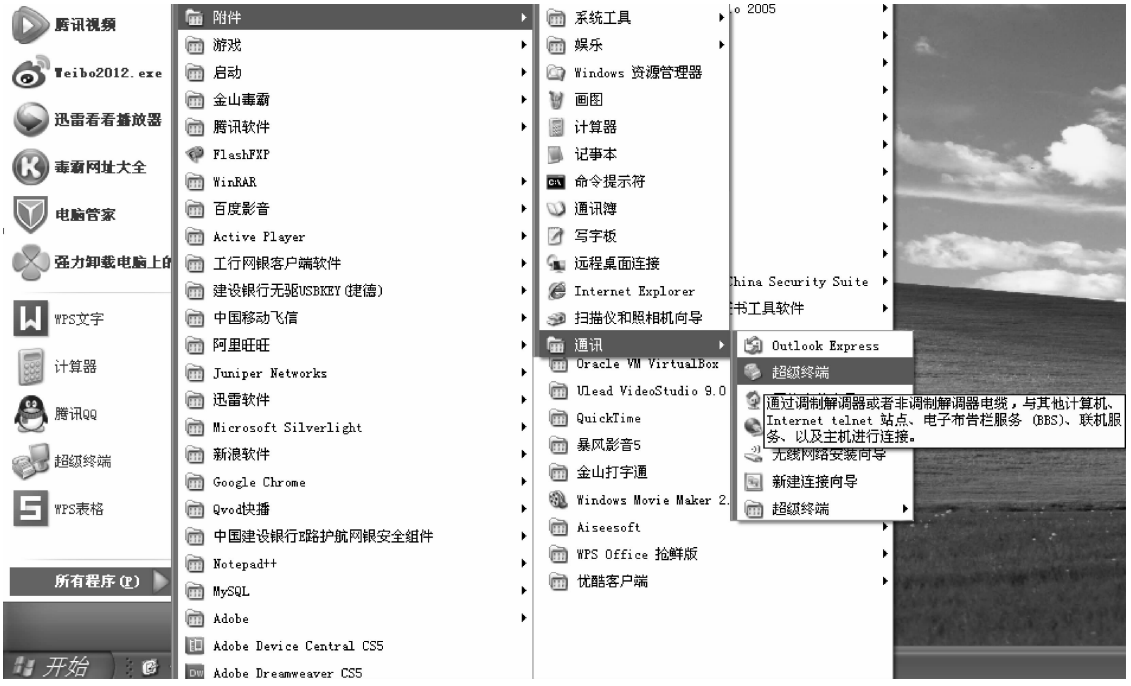

图 1－1－11　打开超级终端

② 在“名称”处填入超级终端的名称，如把它定义为“DCRS－SWITCH”。

图 1－1－12　给超级终端命名

③ 在“连接到”对话框中选择 PC 机使用的 RS－232 串口，如连接的是串口 6，则选择串口 6，点击“确定”按钮。

图 1－1－13　选择连接 PC 的串口

④ 随即弹出“COM6 属性”对话框，每秒位数选择“9600”，数据位选择“8”，奇偶校验选择“无”，停止位选择“1”，数据流控制选择“无”，或者直接点击“还原为默认值”按钮后，再点击“确定”按钮。

图 1－1－14　设置 COM 口属性

④ 弹出超级终端的配置界面。

图 1－1－15　超级终端的配置界面

（3）进入交换机的 CLI 配置界面

打开交换机的电源开关，在超级终端的配置界面上出现如图 1－1－16 所示的提示，进入到交换机的CLI配置方式，接下来用户可以输入相关的命令进行管理。

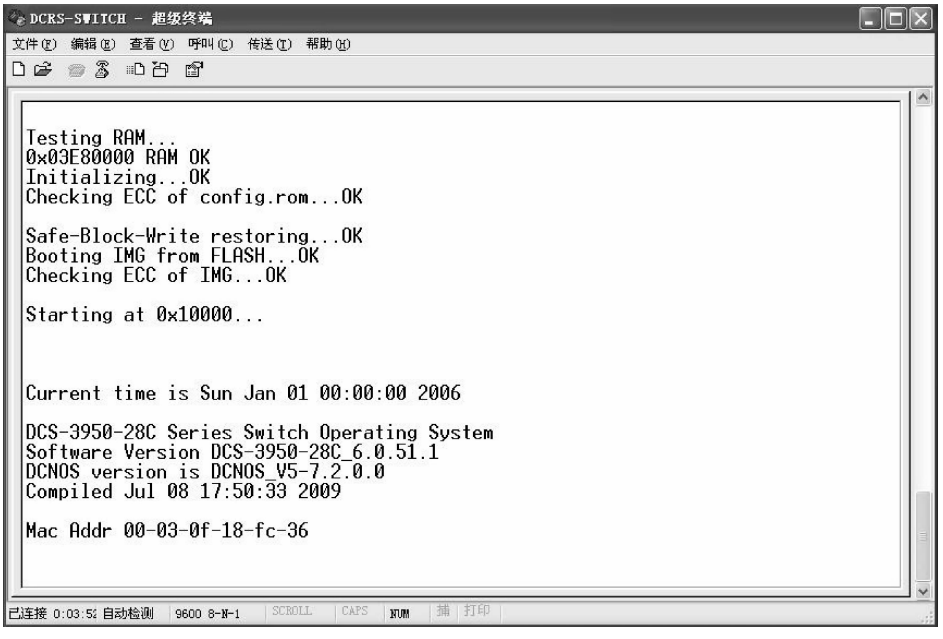

图 1－1－16　进入交换机的 CLI 配置界面

5. 配置 Telnet 管理交换机实现带内管理

Telnet 就是为了适应远程维护而提供的一种方便快捷的配置方式，但这种配置方式需要结合 Console 配置方式事先完成一些初始化配置。线缆连接方面除了 Console 口配置线缆的连接外，还需要保证主机和交换机具有网络互通性。当交换机的配置出现变更，导致带内管理失效时，必须使用带外管理对交换机进行配置管理。

(1) 通过 Telnet 管理交换机要具备的条件

① 交换机配置 IP 地址。

② 作为 Telnet 客户机端的主机 IP 地址与其所属交换机 VLAN 接口的 IP 地址在相同网段。

③ 若不满足②，则 Telnet 客户端可以通过路由器等设备到达交换机某个 IP 地址。

DCS－3950－28CT 是二层交换机，只能配置一个管理 IP 地址。下面以交换机出厂时的情况举例，系统只有 VLAN1 存在。

(2) Telnet 客户端 Telnet 到交换机的 VLAN1 接口的步骤

① 参照图 1－1－17 正确连接 Telnet 客户端与交换机。参照工作过程 1～4 完成 Console 线连接、交换机电源连接及加电。

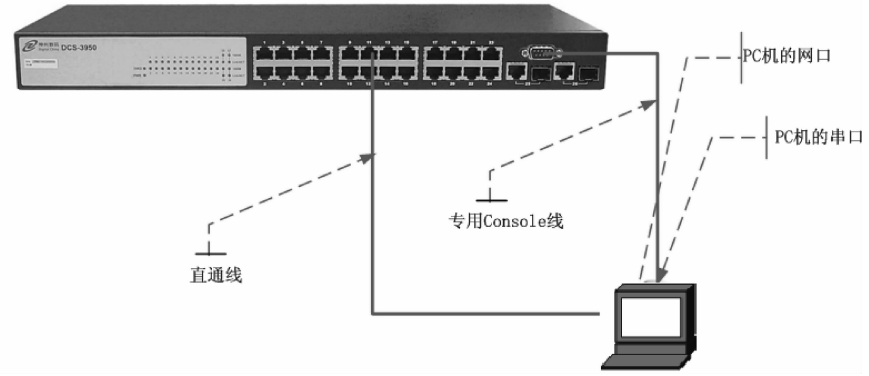

图 1－1－17　Telnet 客户端与交换机连接

② 设置交换机 IP 地址即管理 IP 地址。

首先配置主机的 IP 地址，如图 1－1－18 所示，注意该 IP 要与交换机的 VLAN1 接口的 IP 地址在同一个网段。如交换机的 VLAN1 的接口 IP 地址为 10.1.128.251，则可以设置 Telnet 客户端主机的 IP 地址为 10.1.128.252。

下面简单介绍配置交换机 VLAN1 接口 IP 地址的配置命令，在进行带内管理之前，必须要通过带外管理即 Console 口方式配置交换机的 IP 地址。

在超级终端配置方式下配置命令如下：

注：以后如不特殊说明，所有的交换机配置时的提示符均采用 Switch。

① Switch>enable　　* 使交换机进入特权用户配置模式

② Switch#set default　* 恢复出厂配置

　Are you sure? [Y/N]　Y　　* 是否确认？是

③ Switch#write　　* 清空 startup-config 文件

④ Switch#reload　* 重新启动交换机

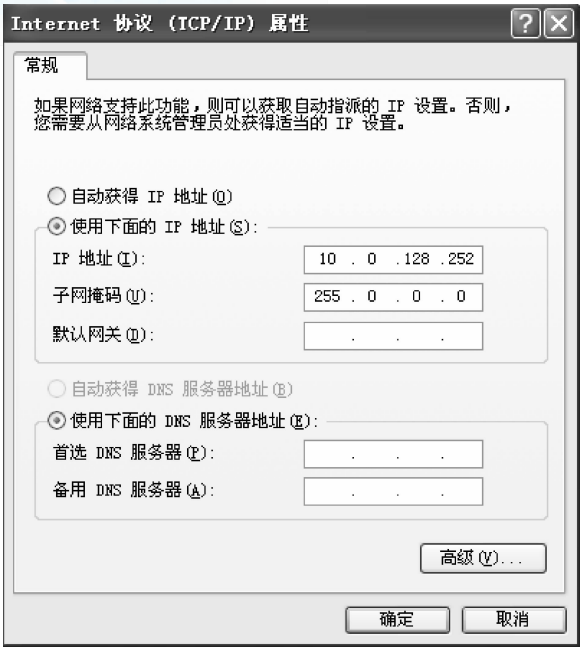

图 1－1－18　配置主机 IP 地址

Process with reboot? [Y/N]　Y

⑤ Switch＃config terminal　　＊进入全局配置模式

⑥ Switch(config)＃hostname DCS－3950－28

⑦ DCS－3950－28 (config)＃interface vlan 1　　＊进入 VLAN1 的接口配置模式

⑧ DCS－3950－28 (config-if-vlan1)＃ip address 10.1.128.251 255.255.255.0 ＊给 VLAN1 设置 IP 地址

⑨ DCS－3950－28 (config-if-vlan1)＃no shutdown　＊重启 VLAN1 接口(激活 VLAN 接口)

⑩ DCS－3950－28 (config-if-vlan1)＃exit　＊退出

注意

可以使用命令 SHOW RUN 检查交换机的配置信息，若在第一条命令之后执行该命令，如观察交换机是默认出厂配置，则不用再进行第二、三、四条命令了，今后也可以使用该条命令检查交换机的配置信息。

(3) 设置交换机授权 Telnet 登录用户及密码

登录到 Telnet 的配置界面，需要输入正确的登录名和口令，否则交换机将拒绝该 Telnet 用户的访问。该项措施是为了保护交换机免受非授权用户的非法操作。若交换机没有设置授权 Telnet 用户，则任何用户都无法进入交换机的 CLI 配置界面。因此在允许 Telnet 方式配置管理交换机时，必须在 Console 口方式的全局配置模式下使用命令为交换机设置 Telnet 授权用户和口令。如交换机授权用户名为 test，口令为 123456，则设置方式如下：

① Switch＞enable

② Switch＃config terminal

③ Switch(config)#telnet-server enable　　*使 Telnet 登录服务功能

④ Switch(config)#username test privilege 15 password　7 123456

*设置 Telnet 使用用户名 test 及登录密码 123456 进行登录

A. Username <username> password {0|7} <password>,其中"0|7"分别表示口令不加密显示和加密显示。

B. Username <username> [privilege <privilege>][password {0|7} <password>],此完整命令格式,权限可以不设置,默认为 1。

C. 本地 Telnet 用户的执行命令权限必须进行设置(权限范围为 1～15,15 为最高权限)。

读一读

什么是 Telnet?

对于 Telnet 的认识,不同的人持有不同的观点,一般可以把 Telnet 当成一种通信协议,但是对于入侵者而言,Telnet 只是一种远程登录的工具。一旦入侵者与远程主机建立了 Telnet 连接,入侵者便可以使用目标主机上的软硬件资源,而入侵者的本地机只相当于一个只有键盘和显示器的终端而已。

(4) 验证 Telnet 客户端与交换机的连通性

在客户端主机上执行"ping 10.1.128.251"命令,查看 ping 是否通,若 ping 不通,则检查原因,如图 1-1-19 所示。

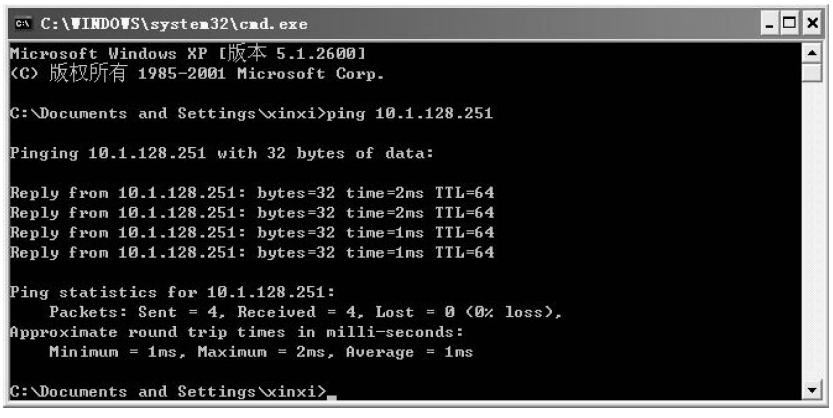

图 1-1-19　Telnet 客户端 ping 交换机

(5) 运行 Telnet 客户端程序(如图 1-1-20 所示)

图 1-1-20　运行 Windows 自带的 Telnet 客户端程序

运行 Windows 自带的 Telnet 客户端程序，并且指定 Telnet 的目的地址。

在 Telnet 配置界面上输入正确的登录名和口令，Telnet 用户就可成功地进入到交换机的 CLI 配置界面。Telnet 登录后与通过 Console 口进入后使用的命令完全一致，登录界面如图 1－1－21 所示。

图 1－1－21　Telnet 登录界面

（6）限制 Telnet 客户端登录地址

可设置只有指定 IP 地址才可以登录交换机，设置命令如下：

DCS－3950－28（config）＃authentication security ip 10.1.128.252

注：只有 IP 为 10.1.128.252 的主机才能 Telnet 连接交换机。

练一练

将客户机的 IP 地址改为其他同网段地址再进行验证，查看是否可以登录到交换机，注意观察现象并截图保存。

注意事项和排错

① 在默认情况下，交换机所有端口都属于 VLAN1，因此我们通常把 VLAN1 作为交换机的管理 VLAN，因此 VLAN1 接口的 IP 地址就是交换机的管理地址。

② 密码只能是 1～8 位。

③ 删除一个 Telnet 用户可以在 config 模式下使用“no telnet-user”命令。

思考

① 二层交换机的 IP 地址可以配置多少个？

② 能不能为 VLAN2 配置 IP 地址？

③ Telnet-user xxx password 0 123456 中把“0”换成“7”会产生何种现象？

练一练

① 删除 test 用户(不准使用 set default)。

② 设置交换机的管理 IP 为 10.1.1.1/24。

③ 使用用户名为 aaa,密码 bbb,并且选择“7”作为参数配置 Telnet 功能。

读一读

了解交换机的组成及功能

交换机类似于一台专用的特殊通信主机,它包括硬件系统和操作系统。交换机信息转发的核心通过 ASIC 芯片实现,由于采用硬件芯片来转发数据信息,因此信息在网络中传输的速度很快,是一个“处处交换”的廉价方案。它在星形网中为所连接的两台设备提供一条独享的点到点的链路,避免了冲突发生,所以能够比集线器更有效地进行数据传输。

虽然不同的交换机产品由不同的硬件设备构成,但组成交换机的基本硬件一般都包括 CPU、RAM、ROM、FLASH、接口。

交换机的基本功能包括地址的学习、帧转发及过滤、环路避免。

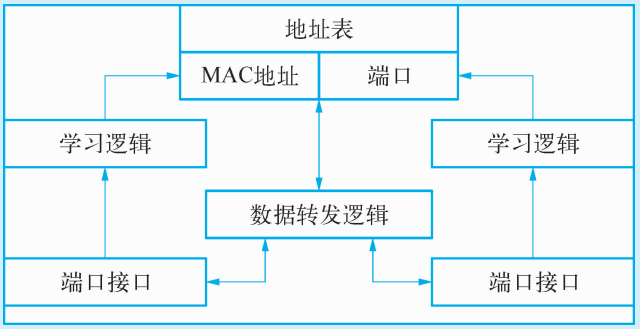

图 1-1-22　交换机的逻辑结构图

6. 交换机的 MAC 地址表管理

(1) MAC 地址表介绍

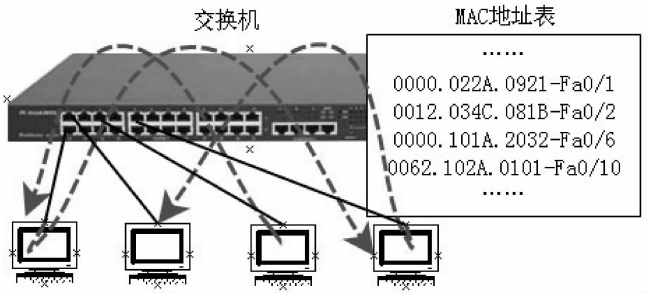

图 1-1-23　交换机基于 MAC 地址的通信

交换机的地址学习就是基于 MAC 地址的学习。

交换机能够记录所有连接到其端口设备的 MAC 地址,其内部有一张 MAC 地址表。MAC 地址表是标识目的 MAC 地址与交换机端口之间映射关系的表,如图 1-1-24 所示,里

面存放着所有连接到端口设备的 MAC 地址及相应端口号的映射关系。

如图 1－1－24 所示，当交换机被初始化时，其 MAC 地址表是空的，此时如果有数据帧到来，交换机就向除了源端口之外的所有端口转发，并把源端口和相应的 MAC 地址记录在地址表中。以后每收到一个信息都查看地址表，有记录的就按照地址表中对应的地址转发，没有记录的就把信息转发给除源端口之外的所有端口，并记录下端口 MAC 地址的对应信息。直至连接到交换机的所有的计算机都发送过数据之后，交换机的 MAC 地址表最终建立完整。

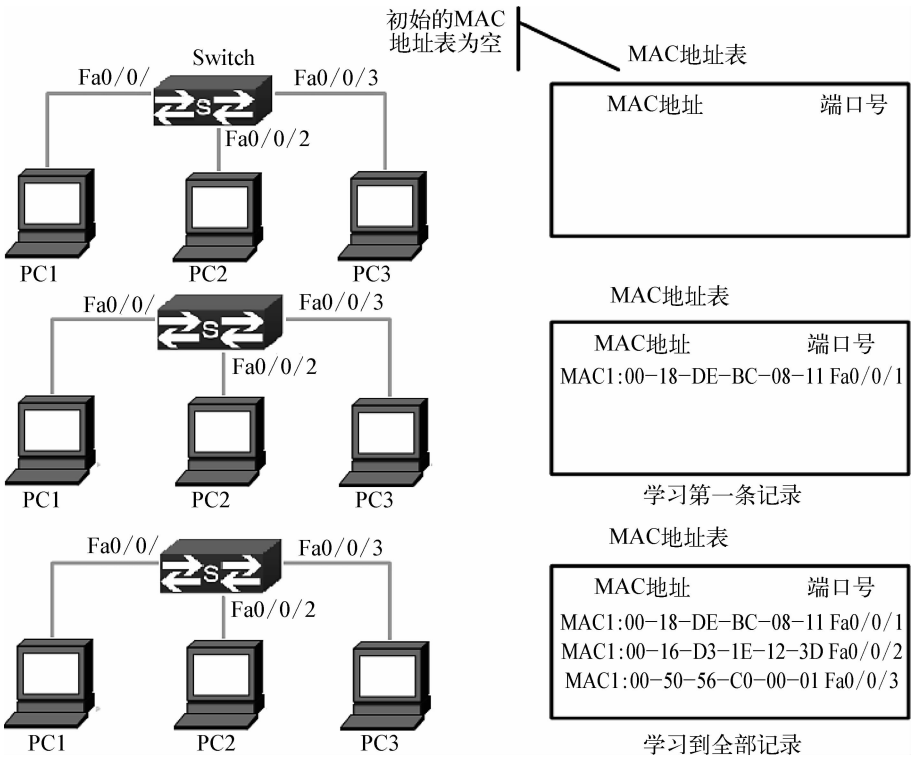

图 1－1－24　交换机 MAC 地址表的学习过程

MAC 地址分为静态 MAC 地址和动态 MAC 地址。静态 MAC 地址由用户配置，具有最高优先级（不能被动态 MAC 地址覆盖）且永久生效；动态 MAC 地址由交换机在转发数据帧的过程中学习，且在有限时间内生效。当交换机接收到需要转发的数据帧时，首先学习数据帧的源 MAC 地址与接收端口之间的关系，并根据目的 MAC 地址查询 MAC 地址表。如果命中相关表项，交换机将数据帧从相应端口转发，否则交换机将数据帧在其所属广播域内广播（泛洪）。如果动态 MAC 地址长时间没有被转发数据帧命中，交换机就将其从 MAC 地址表中删除。对于 MAC 地址表的操作可分为两步：

① MAC 地址的获取。

② 根据 MAC 地址表转发或过滤。

（2）MAC 地址表的获取

MAC 地址表的获取可分为静态配置和动态学习。静态配置即由用户人为地建立 MAC 地址与端口的映射关系；动态学习即由交换机动态地发现 MAC 地址与端口的映射，并定期更

新 MAC 地址表。下面我们将重点介绍 MAC 地址表的动态学习过程。

如图 1－1－25 所示的拓扑环境为 4 台主机连接在神州数码交换机上，其中主机 1 和 2 在同一个物理分段中(即相同的冲突域)，该物理分段与神州数码交换机的端口 5 相连；主机 3 和 4 在同一个物理分段，该物理分段与神州数码交换机的端口 12 相连。

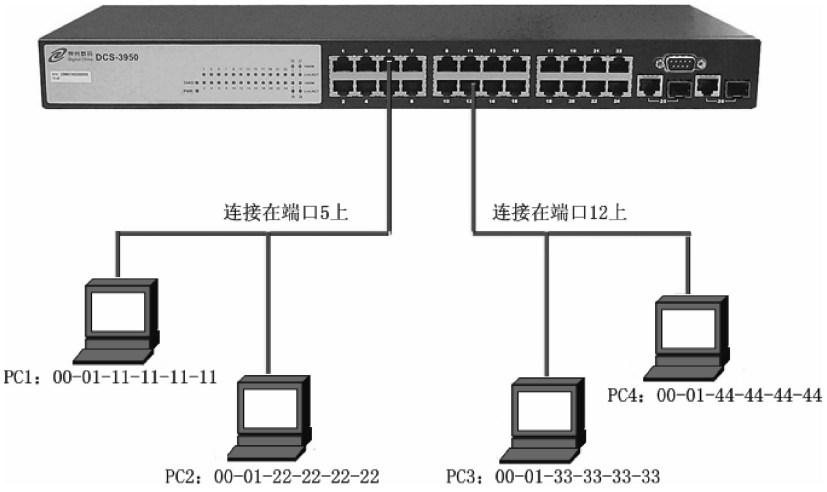

图 1－1－25　MAC 地址表动态学习

初始状态下 MAC 地址表中没有任何学习到的地址映射表项，以主机 1 和主机 3 的相互通信为例，MAC 地址表的学习过程如下：

① 当主机 1 向主机 3 传输信息时，交换机在端口 5 处收到该信息的源 MAC 地址 00－01－11－11－11－11，交换机的 MAC 地址表中就会增加 MAC 地址 00－01－11－11－11－11 和端口 5 映射表项。

② 同时，交换机会检查到该信息的目标 MAC 地址 00－01－33－33－33－33，此时交换机中只有 MAC 地址 00－01－11－11－11－11 和端口 5 的映射表项，没有 00－01－33－33－33－33 对应的端口映射，因此交换机只能将该信息广播给交换机的每个端口。

③ 位于端口 12 的主机 3、4 均收到主机 1 发出的信息，但主机 4 不会给主机 1 回应，因为目标 MAC 地址为 00－01－33－33－33－33，只有主机 3 会给主机 1 回应。这时交换机的 12 号端口收到主机 3 发出的信息，交换机的 MAC 地址表中就又增加了 MAC 地址 00－01－33－33－33－33 和端口 12 映射表项。

④ 目前 MAC 地址表的内容为 MAC 地址 00－01－11－11－11－11 动态对应着端口 5，MAC 地址 00－01－33－33－33－33 动态对应着端口 12。

⑤ 经过一段时间的主机 1 和主机 3 的通信之后，交换机再也没有接收到从主机 1 或者主机 3 发出的信息，300 s 后交换机的 MAC 地址表将删除上面保存的 MAC 地址映射表项。这里的 300 s 是神州数码交换机缺省的 MAC 地址的老化时间，且神州数码交换机提供老化时间的修改。

(3) 转发和过滤

交换机会根据 MAC 地址表对接收到的数据帧做出转发或过滤的决定。以图 1－1－25 为例，假设当前神州数码交换机 MAC 地址表动态学习到了主机 1 和主机 3 的 MAC 地址，用

户手工配置了主机 2 和主机 4 与端口的映射关系，此时的 MAC 地址表如表 1－1－4 所示。

表 1－1－4　MAC 地址和端口对应表

MAC 地址	端 口 号	获取方式
00－01－11－11－11－11	5	动　态
00－01－22－22－22－22	5	静　态
00－01－33－33－33－33	12	动　态
00－01－44－44－44－44	12	静　态

① 根据 MAC 地址表转发的情况。

如果主机 1 向主机 3 发送信息时，交换机根据 MAC 地址表，将该信息从端口 5 接收到的数据从端口 12 发出。

② 根据 MAC 地址表过滤的情况。

如果主机 1 向主机 2 发送信息，交换机根据 MAC 地址表，检查到主机 2 和主机 1 在同一个物理分段中，交换机将对该信息进行过滤，即不发送帧信息。

另外，交换机能转发三种类型的帧，分别是广播帧、组播帧、单播帧。

下面简单介绍交换机对三种帧的处理：

① 广播帧：交换机能阻隔冲突域，但不能阻隔广播域，在没有设置 VLAN 的情况下连接在交换机的所有设备是处在同一个广播域中的，当交换机接收到广播帧时，它会向所有的端口转发该广播帧。当交换机设置了 VLAN 后，MAC 地址表也会做相应的调整，会增加 VLAN 的信息，此时交换机接收到广播帧后，不会将该广播帧转发给交换机内的所有端口，而是改变为只向属于同一个 VLAN 的所有端口转发。

② 组播帧：当交换机没有设置 IGMP Snooping 的功能时，交换机对组播的处理与广播的处理一样；当交换机设置 IGMP Snooping 功能时，交换机只会向属于该组播组的端口转发该组播帧。

③ 单播帧：在没有设置 VLAN 的情况下，当交换机接收到的单播帧的目标 MAC 地址在 MAC 表中存在，交换机会直接将该单播帧转发到相应的端口；当接收到单播帧的目标 MAC 地址在 MAC 地址表中不存在时，交换机会对该单播帧进行广播；当交换机设置了 VLAN，其只会在同一 VLAN 内转发单播帧；当转发单播帧的目标 MAC 地址在 MAC 地址表中存在，但不属于同一 VLAN，此时交换机只能将该单播帧在它属于的 VLAN 内进行广播。

(4) MAC 地址表配置

① 设置 MAC 地址表中动态学习到的地址映射表项的老化时间。

命令：mac-address-table aging-time

age＞| 0｝

no mac-address-table aging-time

功能：设置 MAC 地址表中动态学习到的地址映射表项的老化时间，本命令的 no 操作为恢复系统的缺省老化时间 300 s。

参数：＜age＞为老化时间，单位为秒，取值范围为 10 s～100 000 s，0 为不老化。

命令模式：全局配置模式。

缺省情况：系统缺省老化时间为 300 s。

使用指南：老化时间设置得过小，交换机中会增加很多不必要广播（影响性能）；老化时间设置得过大，又会使一些早已不用的表项长期存在于 MAC 地址表中，因此用户应该根据实际情况合理地设置老化时间。

当老化时间设置为 0 时，交换机动态学习到地址就不会随着时间而老化，动态学习到的地址将一直保存在 MAC 地址表中。

注意：神州数码交换机的动态 MAC 地址实际老化时间是设置值的 1～1.5 倍，若在此期间没有接收到来自动态 MAC 地址的数据流，这些动态 MAC 地址将被老化。

举例：设置 MAC 地址表动态学习到的 MAC 地址的老化时间为 400 s。

Switch(Config)＃mac-address-table aging-time 400

② 添加或修改静态地址表项和动态地址表项。

命令：mac-address-table static address ＜mac-addr＞ vlan ＜vlan-id＞ interface [Ethernet|port-channel]＜interface-name＞

no mac-address-table [static| dynamic] [address ＜mac-addr＞] [vlan ＜vlan-id＞] [interface ＜interface-name＞]

功能：添加或修改静态地址表项和动态地址表项，此命令的 no 操作为删除静态地址表项和动态地址表项。

参数：static 静态表项，dynamic 动态地址表项，＜mac-addr＞ 要添加或删除的 MAC 地址，＜interface-name＞ 转发 MAC 数据包的端口名称，＜vlan-id＞ 接收 MAC 地址数据包的 VLAN 号。

命令模式：全局配置模式。

缺省情况：当配置 VLAN 接口或三层接口后，系统会生成一个 VLAN 接口或三层接口，与交换机固有的 MAC 地址的静态地址映射表项。

使用指南：在某些特殊用途或者交换机不能动态地学习到 MAC 地址，用户可以使用本命令将 MAC 地址与端口及 VLAN 手工建立映射关系。当端口类型为一个 port-channel 时，该 port-channel 必须是 up 的。

命令 no mac-address-table 为删除交换机 MAC 地址表中存在的所有动态、静态、过滤 MAC 地址表项，系统缺省保留的映射表项除外。

举例：端口 0/0/5 属于 VLAN 200，与 MAC 地址为 00－03－0f－f0－00－18 建立地址映射。

Switch(Config)＃mac-address-table static address 00－03－0f－f0－00－18 vlan 200 interface ethernet 0/0/5

③ 添加或修改过滤地址表项。

命令：mac-address-table blackhole address ＜mac-addr＞ vlan ＜vlan-id＞

no mac-address-table blackhole [address ＜mac-addr＞] [vlan ＜vlan-id＞]

功能：添加或修改过滤地址表项，此命令的 no 操作为删除过滤地址表项。

参数：＜mac-addr＞ 要添加或删除的 MAC 地址，＜vlan-id＞ 接收 MAC 地址数据包的 VLAN 号。

命令模式：全局配置模式。

缺省情况：无过滤表项。

使用指南：配置过滤表项的目的是丢弃指定 MAC 地址的帧，用于过滤不想让其通过的流量，可以过滤源地址和目标地址。过滤表项只与 VLAN 和 MAC 相关，与端口无关。

举例：在 VLAN 200，将 MAC 地址 00－03－0f－f0－00－18 设置为过滤表项。

Switch(Config)＃mac-address-table blackhole address 00－03－0f－f0－00－18 vlan 200

④ 典型配置举例：

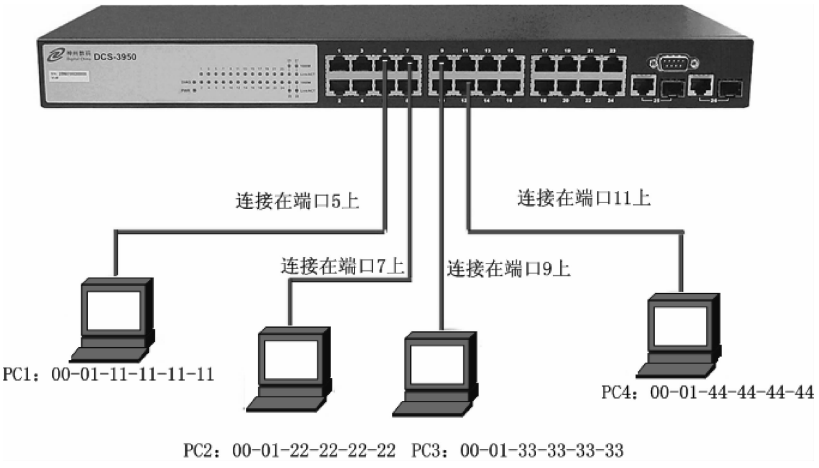

图 1－1－26　MAC 地址表典型配置举例

如图 1－1－26 所示，四台主机分别连接在神州数码交换机的 5、7、9、11 端口，这四台主机都属于缺省 VLAN1。根据实际网络的需要，动态学习功能是打开的。主机 1 保存有机密资料，任何与它不在一个物理分段的主机均不能访问它，主机 2 和主机 3 分别与端口 7 和端口 9 建立静态映射关系。

配置步骤如下：

A. 设置主机 1 的 MAC 地址 00－01－11－11－11－11 为过滤地址。

Switch(Config)＃mac-address-table blackhole address 00－01－11－11－11－11 vlan 1

B. 主机 2 和主机 3 分别与端口 7 和端口 9 建立静态映射关系。

Switch(Config)＃mac-address-table static address 00－01－22－22－22－22 vlan 1 interface ethernet 0/0/7

Switch(Config)＃mac-address-table static address 00－01－33－33－33－33 vlan 1 interface ethernet 0/0/9

五、实训操作

1. 使用超级终端配置交换机

① 初始界面呈现 1 台台式电脑或笔记本电脑、交换机、DB－9 串口的 Console 配置线、交换机电源线、插座，电脑已经开机，交换机没有接通电源也没有连接 Console 线。

② 鼠标拖拽交换机电源，正确连接插座与交换机，交换机电源指示灯闪烁(最终成绿色)。

③ 鼠标拖拽 DB－9 串口的 Console 配置线，正确连接交换机和电脑。

④ 进入超级终端，设置恰当的名称，正确选择连接时使用的接口（具体是哪一个 COM 口），正确设置选定接口的属性，出现终端的配置界面，顺利进入 CLI 的界面。

2. 使用 Telnet 配置交换机

① 初始界面呈现 1 台台式电脑或笔记本电脑、交换机、DB－9 串口的 Console 配置线、交换机电源线、插座、1 根网线，电脑已经开机，交换机已经接通电源但没有连接 Console 线。

② 正确连接电脑与交换机之间的 Console 线，正确设置超级终端并成功进入交换机的 CLI 界面。

③ 用网线正确连接电脑和交换机，交换机对应的以太网口指示灯显示正常（绿色），正确设置电脑的 IP 地址为 10.1.128.252/24。

④ 使用超级终端正确配置交换机的管理地址为 10.1.128.251/24。

⑤ 测试电脑与交换机之间的网络通信，确保相互之间能 ping 通。

⑥ 使用超级终端正确配置可登录到交换机 Telnet 客户端的用户名、权限和口令，使之能够使用交换机的 Telnet 服务。

⑦ 打开电脑，正确运行 Telnet，输入用户名和口令，成功登录到交换机。

3. 交换机 MAC 地址表的配置

① 初始界面拓扑结构如图 1－1－27 所示。

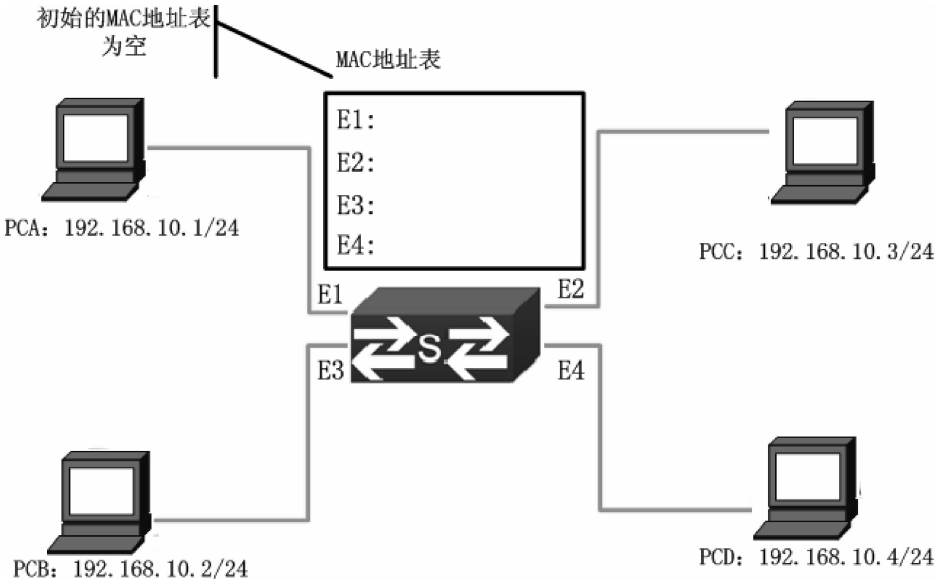

图 1－1－27　交换机 MAC 地址学习及配置

界面呈现 4 台台式电脑或笔记本电脑、交换机、DB－9 串口的 Console 配置线、插座、4 根网线，电脑已经开机，交换机已经接通电源但没有连接 Console 线。

② 在主机 A 与交换机之间正确连接 Console 配置线，创建超级终端名为 DCS3950 并正确设置相关属性，成功进入交换机 CLI 配置界面。

③ 根据拓扑结构图正确连接主机 A 与交换机之间的网线。检查交换机相应接口指示灯的

状态是否为绿色，若不是绿色，更换完好的网线再检查，直到接口指示灯为绿色。

④ 正确设置主机 A 电脑的 IP 地址，使用 ipconfig /all 命令检查并记录主机 A 的 IP 地址及 MAC 地址。如图 1－1－28 所示，方框标识的就是计算机的 MAC 地址。

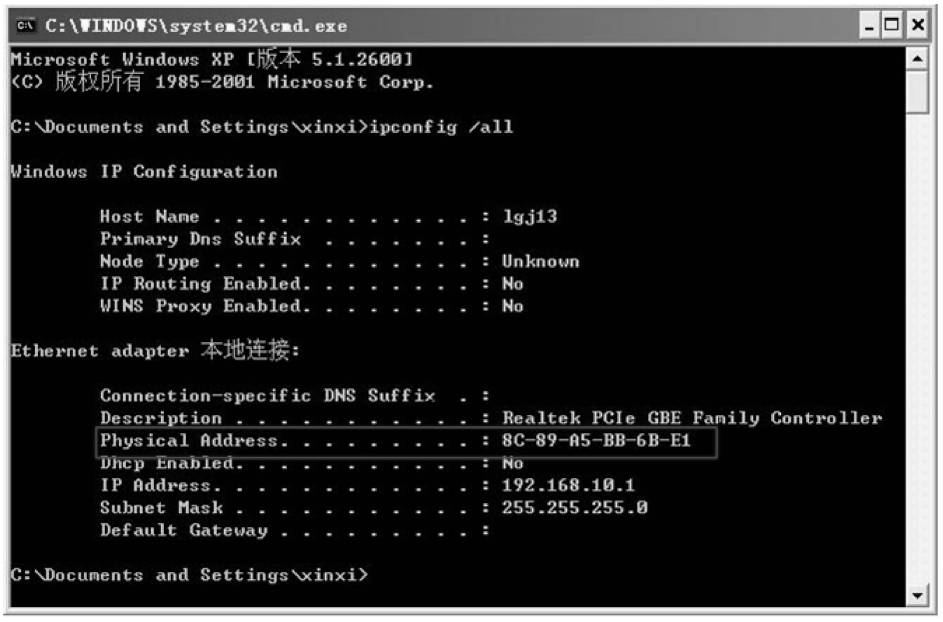

图 1－1－28　查看电脑的 IP 地址及 MAC 地址

⑤ 在交换机中使用命令 show mac-address-table 查看交换机的 MAC 地址表，如图 1－1－29 所示。

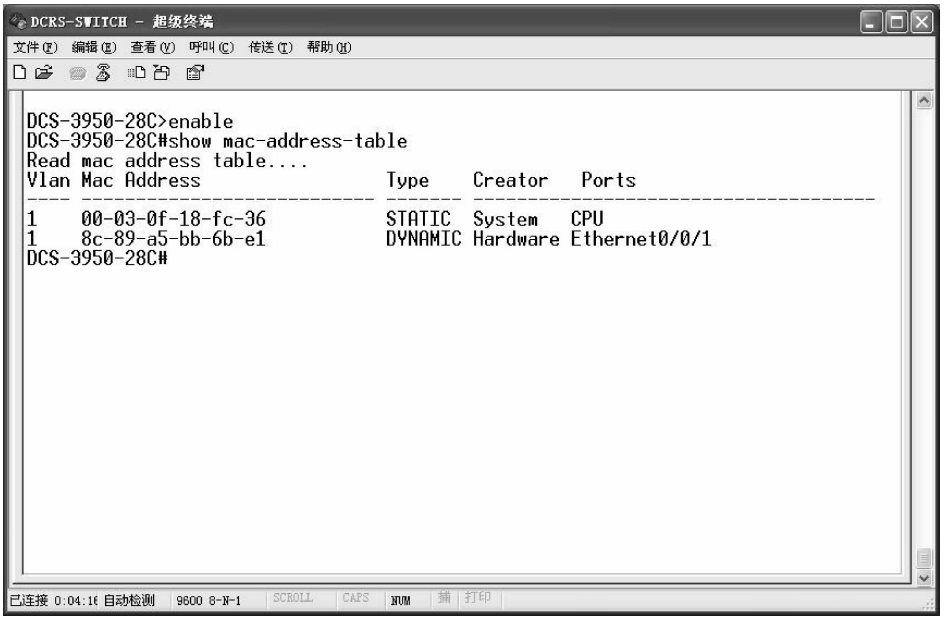

图 1－1－29　查看主机 A 接入交换机后的 MAC 地址表

⑥ 参照第④和第⑤步，分别将主机 B、C、D 接入到交换机并分别查看接入后交换机的 MAC 地址表情况（截图）。

⑦ 将主机 A 与交换机 1 号接口改成静态映射并查看结果。

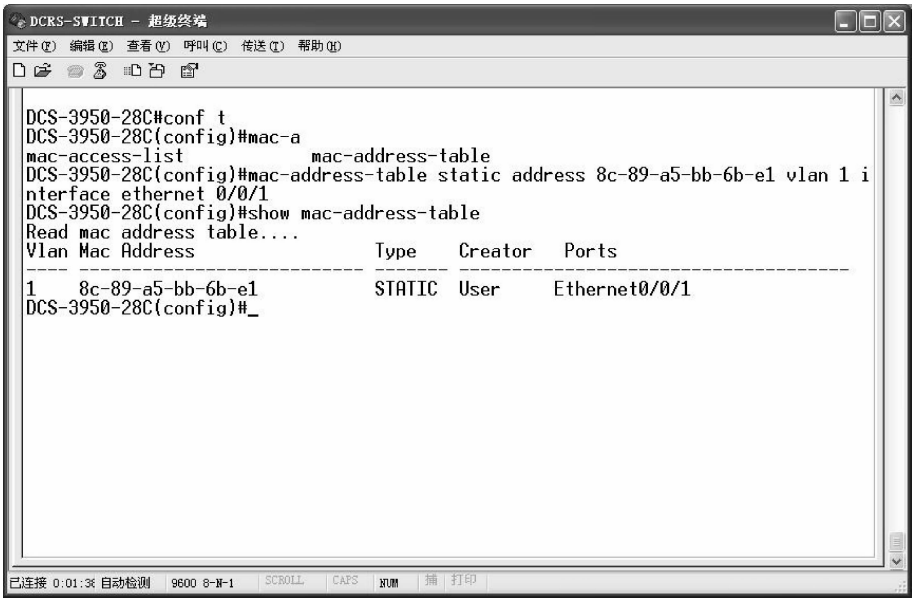

图 1－1－30　建立静态映射

六、知识拓展

拓展内容：ARP 攻击及防范

1. ARP 攻击现象

故障现象 1：小周家里本身有一台台式主机，随后又购买了一台 IBM 的笔记本电脑。两台电脑都通过路由器进行共享上网，开始还挺正常的，可后来总出现一些异常的状况，比如笔记本先开机后，台式机再开机就会引发局域网断开的情况。

故障现象 2：小周所在的某学校现有电脑约 1 100 台，其中 320 台是教师用机，其他的机器为学生用机。一般情况下，只有教师用机可以上网，学生机只有在上计算机课时，才会开机上网，网络运行一直顺畅。半个月以前，局域网频繁断网，文件共享速度、网络打印速度、网络传输速度突然变得缓慢，甚至失去响应。

以上两种现象都是 ARP 攻击后出现的典型现象，ARP 攻击具体表现为局域网内一些正在上网的电脑主机频繁掉线或是断线。产生该故障原因大多是由于局域网内有电脑使用 ARP 病毒欺骗程序（比如 QQ 盗号软件等），这些程序发送 ARP 数据包，致使被攻击的电脑不能上网。

2. ARP 攻击原理分析

局域网是通过 ARP 协议来完成 IP 地址转换为第二层物理地址（即 MAC 地址）的。ARP 协议对网络安全具有重要的意义。通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量，使网络阻塞或者实现“man in the middle”（中间人攻击）进行

ARP 重定向和嗅探攻击。

用伪造源 MAC 地址发送 ARP 响应包，对 ARP 高速缓存机制进行攻击。

每个主机都用一个 ARP 高速缓存存放最近 IP 地址到 MAC 硬件地址之间的映射记录。MS Windows 高速缓存中的每一条记录（条目）的生存时间一般为 60 s，起始时间从被创建时开始算起。

默认情况下，ARP 从缓存中读取 IP－MAC 条目，缓存中的 IP－MAC 条目是根据 ARP 响应包动态变化的。因此，只要网络上有 ARP 响应包发送到本机，即会更新 ARP 高速缓存中的 IP－MAC 条目。

攻击者只要持续不断地发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存中的 IP－MAC 条目，造成网络中断或中间人攻击。

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 地址和 MAC 地址存储在 ARP 缓存中。因此，B 向 A 发送一个自己伪造的 ARP 应答，而这个应答中的数据为发送方 IP 地址是 192.168.10.3（C 的 IP 地址），MAC 地址是 DD－DD－DD－DD－DD－DD（C 的 MAC 地址本来应该是 CC－CC－CC－CC－CC－CC，这里被伪造了）。当 A 接收到 B 伪造的 ARP 应答，就会更新本地的 ARP 缓存（A 不知道被伪造了）。

当攻击源大量向局域网中发送虚假的 ARP 信息后，就会造成局域网中的机器 ARP 缓存崩溃。

交换机上同样维护着一个动态的 MAC 缓存，首先，交换机内部有一个对应的列表，交换机的端口对应 MAC 地址表 Port n <-> Mac 记录着每一个端口下面存在哪些 MAC 地址，这个表开始是空的，交换机从来往数据帧中学习。因为 MAC－PORT 缓存表是动态更新的，那么让整个 交换机的端口表都改变，对交换机进行 MAC 地址欺骗的 Flood，不断发送大量假 MAC 地址的数据包，交换机就更新 MAC－PORT 缓存，如果能通过这样的办法把以前正常的 MAC 和 Port 对应的关系破坏了，那么交换机就会进行泛洪发送给每一个端口，让交换机基本变成一个 HUB，向所有的端口发送数据包，要进行嗅探攻击的目的一样能够达到，这样也将造成交换机 MAC－PORT 缓存的崩溃，如下为交换机中的日志所示：

Internet 172.20.156.10 000b.cd85.a193 ARPA VLAN256
Internet 172.20.156.50 000b.cd85.a193 ARPA VLAN256
Internet 172.20.156.254 0000b.cd85.a193 ARPA VLAN256
Internet 172.20.156.53 0000b.cd85.a193 ARPA VLAN256
Internet 172.20.156.33 0000b.cd85.a193 ARPA VLAN256
Internet 172.20.156.13 0000b.cd85.a193 ARPA VLAN256
Internet 172.20.156.15 0000b.cd85.a193 ARPA VLAN256
Internet 172.20.156.14 0000b.cd85.a193 ARPA VLAN256

仔细观察以上日志，你会发现来自不同 IP 地址的信息采用的是同一个 MAC 地址，这就是 ARP SPOOFING（ARP 地址欺骗攻击）。

3. ARP 欺骗过程

假设一个只有三台电脑组成的局域网，该局域网由交换机（Switch）连接，其中一个电脑名叫

A，代表攻击方；一台电脑叫 S，代表源主机，即发送数据的电脑；另一台电脑名叫 D，代表目的主机，即接收数据的电脑。这三台电脑的 IP 地址分别为 192.168.0.2、192.168.0.3、192.168.0.4，MAC 地址分别为 MAC_A、MAC_S、MAC_D，其网络拓扑环境如图 1－1－31 所示。

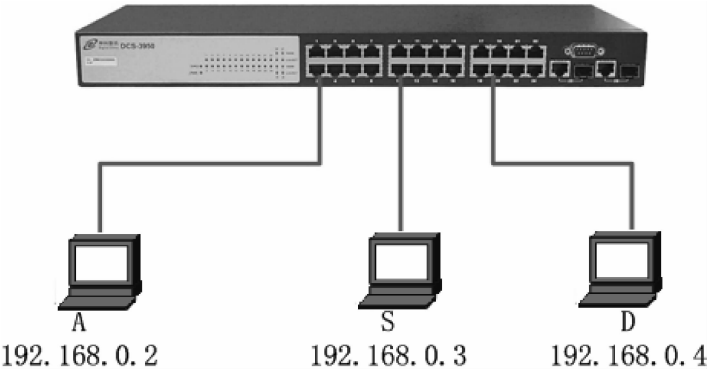

图 1－1－31　ARP 攻击拓扑图

现在，S 电脑要给 D 电脑发送数据了，在 S 电脑内部，上层的 TCP 和 UDP 的数据包已经传送到了最底层的网络接口层，数据包即将要发送出去，但这时还不知道目的主机 D 电脑的 MAC 地址（MAC_D）。这时候，S 电脑要先查询自身的 ARP 缓存表，查看里面是否有 192.168.0.4 这台电脑的 MAC 地址，如果有，就将封装在数据包的外面，直接发送出去即可。如果没有，这时 S 电脑要向全网络发送一个 ARP 广播包，大声询问："我的 IP 是 192.168.0.3，硬件地址是 MAC_S，我想知道 IP 地址为 192.168.0.4 的主机的硬件地址是多少？"这时，全网络的电脑都收到了该 ARP 广播包，包括 A 电脑和 D 电脑。A 电脑一看其要查询的 IP 地址不是自己的，就将该数据包丢弃不予理会。而 D 电脑一看 IP 地址是自己的，则回答 S 电脑："我的 IP 地址是 192.168.0.4，我的硬件地址是 MAC_D"。需要注意的是，这条信息是单独回答的，即 D 电脑单独向 S 电脑发送的，并非刚才的广播。现在 S 电脑已经知道目的电脑 D 的 MAC 地址了，它可以将要发送的数据包上贴上目的地址 MAC_D，发送出去了。同时它还会动态更新自身的 ARP 缓存表，将 192.168.0.4－MAC_D 这一条记录添加进去，这样，等 S 电脑下次再给 D 电脑发送数据的时候，就不用发送 ARP 广播包了，这就是正常情况下的数据包发送过程。

这样的机制看上去很完美，似乎整个局域网也应该天下太平，相安无事。但是，上述数据发送机制有一个致命的缺陷，即它是建立在对局域网中电脑全部信任的基础上的，那么这样就很危险了，因为局域网中并非所有的电脑都安分守己，往往有非法者的存在。比如在上述数据发送中，当 S 电脑向全网询问 IP 地址为 192.168.0.4 的主机的硬件地址是多少后，D 电脑回应了自己的正确 MAC 地址，但同时 A 电脑也进行回话了，告知其 IP 地址是 192.168.0.4，其硬件地址是 MAC_A，此时它竟然冒充自己是 D 电脑的 IP 地址，而 MAC 地址则写成自己的。由于 A 电脑不停地发送这样的应答数据包，本来 S 电脑的 ARP 缓存表中已经保存了正确的记录（即 192.168.0.4－MAC_D），但是由于 A 电脑不停地应答，这时 S 电脑并不知道 A 电脑发送的数据包是伪造的，导致 S 电脑又重新动态更新自身的 ARP 缓存表，并将其记录成 192.168.0.4－MAC_A。很显然，这是一个错误的记录（这步也叫 ARP 缓存表中毒），这样就

导致以后凡是S电脑要发送给D电脑，也就是IP地址为192.168.0.4这台主机的数据，都将会发送给MAC地址为MAC_A的主机，这样，A电脑就劫持了由S电脑发送给D电脑的数据，这就是ARP欺骗的过程。

如果A电脑再做得“过分”一些，它不冒充D电脑，而是冒充网关，那后果会怎么样呢？我们都知道，如果一个局域网中的电脑要连接外网，也就是登录互联网的时候，都要经过局域网中的网关转发一下，所有收发的数据都要先经过网关，再由网关发向互联网。在局域网中，网关的IP地址一般为192.168.0.1。如果A电脑向全网不停地发送ARP欺骗广播，告知其IP地址是192.168.0.1，其硬件地址是MAC_A，这时局域网中的其他电脑并没有察觉到异常，因为局域网通信的前提条件是信任任何电脑发送的ARP广播包，这样局域网中的其他电脑都会更新自身的ARP缓存表，记录下192.168.0.1-MAC_A这样的记录。这样，当它们发送给网关，也就是IP地址为192.168.0.1这台电脑的数据，结果都会发送到MAC_A这台电脑中，这样，A电脑就将监听整个局域网发送给互联网的数据包。

4. ARP攻击常用防御方法

(1) 交换机内绑定用户IP/MAC地址

交换机内绑定用户MAC地址的操作可参考图1-1-30。

(2) 将确定的攻击源MAC地址添加为过滤地址

例如，设置主机1的MAC地址00-01-11-11-11-11为过滤地址。

Switch(Config)#mac-address-table blackhole address 00-01-11-11-11-11 vlan 1

通过以上配置过滤表项的目的是丢弃指定主机1地址的帧，用于过滤不让其流量通过。

(3) 客户机上做网关的ARP静态绑定

其涉及的命令有如下三条：

① Arp -a：列出本机缓存的所有ARP信息。

② Arp -dip 地址：清除缓存信息。

③ Arp -s ip地址 mac地址：建立静态绑定。

具体操作参见下面的例子：

首先在笔记本电脑桌面中依次单击“开始”→“运行”选项，在弹出的“运行”对话框内输入“CMD”命令并按回车键后，就可打开CMD命令提示对话框。随后从光标闪烁的位置处，输入“Arp -a”命令并按回车键，就可获取路由器的IP地址及MAC地址信息，如图1-1-32所示。

Interface后面的192.168.11.114地址，是本机在局域网内的IP地址，而Internet Address下的192.168.11.254地址，则是路由器所使用的IP(即网关地址)，右侧Physical Address下的a4-0c-c3-4f-61-c2则是路由器的MAC地址。我们将以上这些获取到的信息记录下来，然后运行Ipconfig /all命令，来获取本地计算机网卡的MAC地址，这里是8C-89-A5-BB-6B-E1，如图1-1-33所示。

得到了以上信息，接下来我们需要绑定路由器及本地IP地址，来防范ARP病毒的地址欺骗。打开“记事本”文档，在其文本处输入如下命令：

```
@echo off
Arp -s 192.168.11.254 a4-0c-c3-4f-61-c2
Arp -s 192.168.11.114 8C-89-A5-BB-6B-E1
```

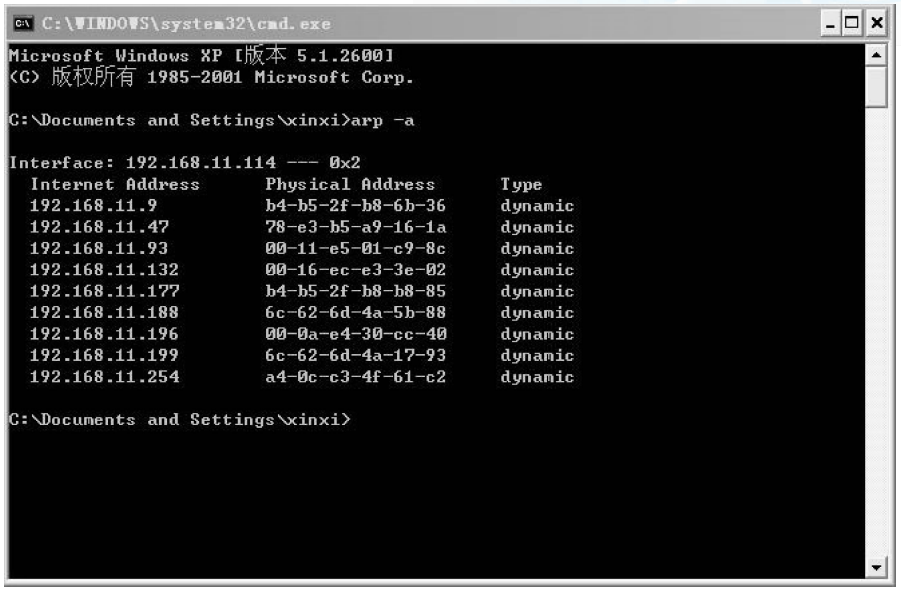

图 1－1－32　获取 IP 地址和 MAC 地址

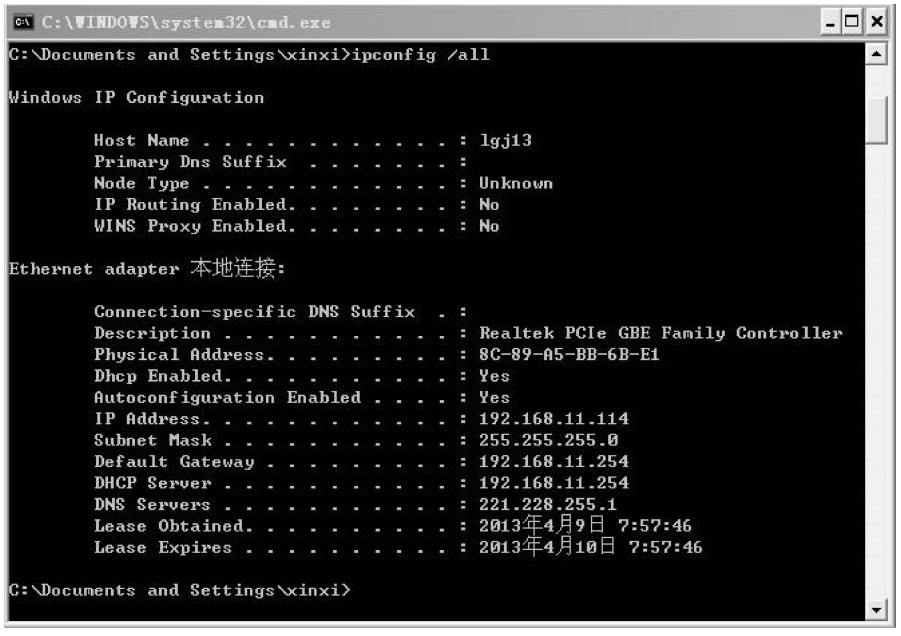

图 1－1－33　获取网卡的 MAC 地址

操作完毕后，将其保存为“.bat”格式的批处理文件，名称可以随意书写，然后将其放入到“启动”文件夹，这样每次开机就会先运行一下我们所编写绑定路由器（网关）及本地 IP 地址的命令，从而可以防范 ARP 病毒的地址欺骗。使用同样的方法，在台式机上绑定其路由器以及本地 IP 地址，再利用杀毒软件进行全面杀毒，将 ARP 病毒从主机内赶走即可。

当然不排除绑定以上地址信息后，病毒仍然有地址欺骗的行为，并且还会引发断网的异常状况。因此我们需要利用路由器实现更深层的绑定，才能彻底解决地址欺骗。其他一些 ARP

攻击的防御方法，我们将在后续的内容中进行学习。

练一练

尝试在一台电脑中完成网关的 ARP 静态绑定，网关地址自己设定。

七、思考与练习

1. 通常我们所学的交换机工作在 ISO/OSI 模型七层的_____层。
2. 交换机中 POE 和 SPF 的接口含义分别是_____、_____。
3. Telnet 的中文含义是_____，通过使用它来对交换机进行_____管理。
4. 配置超级终端的端口属性是_____。
5. 交换机的基本功能包括_____、_____和环路避免。
6. 配置交换机 IP 地址的操作步骤是：_____；_____；_____。
7. MAC 地址使用_____位十六进数表示，若用 X 表示 MAC 地址中的数值，则通常情况下如何表示 MAC 地址_____。
8. 交换机的地址学习就是基于 MAC 地址的学习，初始状态下交换机中 MAC 地址表为空，为了建立 MAC 地址表，交换机会通过传输一种特殊的广播帧，一般称这个过程为_____。
9. 交换机会根据_____对接收到的数据帧做出转发或过滤的决定，使用_____命令可以查看交换机中的 MAC 地址表。
10. 在交换机中可以通过_____命令查看当前交换机的配置信息。
11. 保存交换机的配置信息可使用_____命令。
12. 若要清除交换机的配置，其操作的命令和顺序：_____；_____；_____。
13. 保存交换机的配置信息可使用_____命令。
14. 简述交换机建立 MAC 地址表的过程。
15. 简述交换机在进行转发和过滤时，何时会发采用单播？何时会采用广播？
16. 简述防止交换机 ARP 攻击的常用防御方法及相关命令。

任务二　接入互联网

一、任务描述

在熟悉并掌握二层接入技术的基础上，小王和小李开始着手如何将公司的内网接入到 Internet 中。考虑到分公司近三年的发展规划，人员的规模将控制在 20 人之内，公司本着节约成本角度出发，首先让他们考察一下目前主流的电信宽带接入技术，由他们决定采用什么样的接

入方式更适合公司的要求，其次再对接入设备进行选型，并选择性价比高的无线宽带路由器。

二、任务目标

1. 了解主流宽带接入技术。
2. 掌握宽带的基础知识。
3. 掌握 IP 私有地址的使用。
4. 掌握无线路由器的工作原理。
5. 掌握无线路由器的配置方法。

三、任务使用设备清单

1. TP-Link 150 M 无线宽带路由器(TL-WR746N)，如图 1-2-1 所示。

2. 笔记本电脑一台。

图 1-2-1　宽带路由器

四、任务相关知识和技能储备

1. 认识带宽的相关知识

(1) 数据传输速率

数据传输速率是描述数据传输系统的重要技术指标之一。数据传输速率在数值上等于每秒钟传输构成数据代码的二进制比特数，单位为比特/秒，记作 bit/s 或者 bps。

在实际应用中，常用的数据传输速率单位还有 kbps、Mbps 和 Gbps，其中，

1 Mbps=1 024 kbps=128 kBps（注意 B 的大小写）

1 Gbps=1 024 Mbps=128 MBps（注意 B 的大小写）

1 Mbps=1 024 bps×1 024 bps

注意

有的资料中将传输速率单位的换算关系定义为 1 000，即 1 Mbps=1 000 kbps，这主要出于计算的方便，因为这样计算产生的误差在实际速率中并不明显。

想一想

你的硬盘中存放的电影一般是多大？硬盘数据的存储单位是什么？

(2) 宽带的传输速度

在现代网络技术中，人们总是以“带宽”来表示信道的数据传输速率，“带宽”与“速率”几乎成了同义词。

在计算机科学中，bit 是表示信息的最小单位，叫作二进制位，用 0 和 1 表示。Byte 叫作字节，由 8 个位(8 bit)组成一个字节(1 Byte)，用于表示计算机中的一个字符。Byte 与 bit 之间可以进行换算，其换算关系为 1 Byte=8 bit。在实际应用中一般使用简称，即 1 bit 简写为 1b(注意是小写英文字母 b)，1 Byte 简写为 1 B(注意是大写英文字母 B)。

在计算机网络或者是网络运营商中，一般宽带速率的单位用 bps(或 b/s)表示，bps 表示比特每秒即表示每秒钟传输多少位信息，是 bit per second 的缩写。所谓的 1 M 带宽的意思是指 1 Mbps。

(3) 宽带速率计算的方法

带宽与速率是不一样的，带宽表示传输能力，而速率是实际数据流通的速度。带宽的单位是 bit/s(bps)而速率单位是 Byte/s(Bps)。

在网络传输过程中的带宽和速率的关系为带宽/8 ＝传输速率。

理论上来说，2 M 即 2 Mb/s，宽带速率是 256 kB/s，即 2 048 kb/s，实际速率大约为 103 kB/s～200 kB/s。实际速率小于理论速率的原因是受用户计算机性能、网络设备质量、资源使用情况、网络高峰期、网站服务能力、线路衰耗、信号衰减等多种因素的影响而造成的。4 M即 4 Mb/s，宽带理论速率是 512 kB/s，实际速率为 200 kB/s～440 kB/s。

练一练

100 M 局域网的传输速率的理论值是多少？千兆以太网的网络理论传输速率是多少？如何测试你所在实训室的实际网络传输带宽及速率？提示：搭建一个简单的 FTP，使用 FTP 客户端软件 FLASHFXP 下载文件来查看速率。

2. 重拾 IP 地址的基础知识

(1) IP 地址的分类

由于网络中拥有的计算机有可能不一样多，有的网络可能拥有较多的计算机，也有的网络拥有较少的计算机，于是人们按照网络规模的大小，把 32 位地址信息设成五种定位划分的方式，这五种划分方法分别对应于 A 类、B 类、C 类、D 类、E 类 IP 地址，如表 1－2－1 所示。

表 1－2－1　IP 地址的分类

类　　型	IP 地址范围	保 留 IP
A 类	1.0.0.1－126.255.255.254	127.X.X.X
B 类	128.0.0.1－191.255.255.254	169.254.X.X
C 类	192.0.0.1－223.255.255.254	
D 类	224.0.0.1－239.255.255.254	
E 类	240.0.0.1－255.255.255.254	

① A 类 IP 地址：0.0.0.0～127.255.255.255。

A 类 IP 地址是指在 IP 地址的四段号码中，第一段号码为网络号码，剩下的三段号码为本地计算机的号码。如果用二进制表示 IP 地址的话，A 类 IP 地址就由 1 字节的网络地址和 3 字节的主机地址组成，网络地址的最高位必须是 0。A 类 IP 地址中网络的标识长度为 7 位，主机的标识长度为 24 位，A 类网络地址数量较少，可以用于主机数达 1 600 多万台的大型网络。

② B 类 IP 地址：128.0.0.0～191.255.255.255

B 类 IP 地址是指在 IP 地址的四段号码中，前两段号码为网络号码。B 类 IP 地址是由 2 字节的网络地址和 2 字节的主机地址组成，网络地址的最高位必须是 10。B 类 IP 地址中网络

的标识长度为 14 位，主机的标识长度为 16 位，B 类网络地址适用于中等规模的网络，每个网络所能容纳的计算机数为 6 万多台。

③ C 类 IP 地址：192.0.0.0～223.255.255.255

C 类 IP 地址是指在 IP 地址的四段号码中，前三段号码为网络号码，剩下的一段号码为本地计算机的号码。如果用二进制表示 IP 地址的话，C 类 IP 地址是由 3 字节的网络地址和 1 字节的主机地址组成，网络地址的最高位必须是 110。C 类 IP 地址中网络的标识长度为 21 位，主机标识的长度为 8 位，C 类网络地址数量较多，适用于小规模的局域网络，每个网络最多只能包含 254 台计算机。

④ D 类 IP 地址：224.0.0.0～239.255.255.255。

D 类 IP 地址是保留的，用作组播地址。

⑤ E 类 IP 地址：240.0.0.0～255.255.255.255。

(2) 私有地址

私有地址是国际互联网代理成员管理局(IANA)在 IP 地址范围内，将一部分地址保留作为私人 IP 地址空间或者专门用于内部局域网使用的地址。

私有地址是指内部网络或主机地址，公有地址是指在因特网上全球唯一的 IP 地址。RFC1918 为私有网络预留出了 3 个 IP 地址块，分别如下：

A 类：10.0.0.0～10.255.255.255

B 类：172.16.0.0～172.31.255.255

C 类：192.168.0.0～192.168.255.255

上述 3 个范围内的地址不会在因特网上被分配，因而可以不必向 ISP 或注册中心申请而在公司或企业内部自由使用。

想一想

在本次接入互联网过程中，如果让你来选择，你会使用哪个段的私有地址段？

3. 了解主流宽带接入技术

(1) ADSL 接入

ADSL 是英文 Asymmetrical Digital Subscriber Loop(非对称数字用户环路)的英文缩写。ADSL 技术是运行在原有普通电话线上的一种新的高速宽带技术，它利用现有的一对电话铜线，为用户提供上下行非对称的传输速率(带宽)。

非对称主要体现在上行速率(最高 640 kbps)和下行速率(最高 8 Mbps)的非对称性上。上行(从用户到网络)为低速传输，可达 640 kbps；下行(从网络到用户)为高速传输，可达 8 Mbps。

特点：可直接利用现有的电话线，节省安装成本。同时，可满足普通家庭的上网需求。

图 1-2-2 中国电信 ADSL 宽带猫

(2) LAN 接入

以太网宽带接入(FTTB+LAN)是一种光纤加五类网络线的宽带接入方式。它将光纤直接接入小

区和大楼，然后通过五类线与各用户的终端相连，为广大用户提供高速上网和其他宽带数据服务。LAN 具有传输速率高、用户端投资少的特点，可以满足不同层面用户的多种需求。

特点：传输速率高、网络稳定性好、安装方便、用户端投资成本低。

注意：电信的 LAN 与其他运营商的 LAN 有很大的区别。电信 LAN 是采用 VLAN 方式，个人独享 VLAN 及带宽，屏蔽操作系统的各类广播包，具有速度快、保密性好的特点。

(3) EPON 光纤接入

EPON(GPON)光纤上网的线路通过电信专网平台提供了线路的接入层独享的接入方式，真正实现高速光纤上网。与 FTTB+LAN 相比，光纤上网专线真正实现了接入层端口独享，而并不像 FTTB+LAN 仅在大楼交换机处为独享的。

特点：端口独享，由于用户线路直接接入电信局机房，故其网络质量高于 FTTB+LAN。光纤上网专线真正提供了电信高品质的服务。

4. 无线宽带路由器

(1) 无线路由器的选择

随着 IT 业的迅猛发展，无线上网也成为了当下的主流之一，在企业中也不例外，所以，无线路由器也渐渐成为家庭和企业中不可或缺的网络设备之一。

目前市场上的无线路由器种类较多，消费者在选购无线路由器时，应该从哪些方面着手呢?

① 品牌选择：

以下几个参考品牌，根据某电子商务网站的销售进行排行：

A. TP-Link(普联)无线路由器。

B. D-Link(友讯)无线路由器。

C. 巴法络无线路由器。

D. NETGEAR(网件)无线路由器。

E. 华硕无线路由器。

当然，品牌还有很多，不过最终选择什么品牌，还需要根据自己的预算和需求。在这里建议使用大品牌，而杂牌则不需要考虑。小王和小李根据公司状况，最终选择了 TP-Link 无线路由器。

② 参数的选择：

A. 数据传输率。数据传输率和有线网络类似，无线网络的传输速率是指在一定的网络标准之下接收和发送数据的能力。有所不同的是，在无线网络中，数据传输率和网络环境有很大的关系。因为在无线网络中，数据的传输是通过信号进行的，而实际的使用环境或多或少都会对传输信号造成一定的干扰。

B. 信号覆盖范围，即无线路由器的有效工作距离。只有在无线路由器的信号覆盖范围内，与之搭配的计算机才能进行无线连接。室内 100 m，室外 400 m 是无线路由器有效工作距离的理想值，它会随网络环境的不同而变化。通常在室内，50 m 范围内有较好的无线信号；在室外，无线路由器的有效工作距离在 100 m～200 m 之间。

C. 接口。常见的无线路由器一般都有一个 RJ-45 接口，这是一个 WAN 接口，也就是无线路由器连接到外部网络的接口；其余 2～4 个接口为 LAN 接口，用来连接普通局域网；内部有一个网络交换机芯片，专门处理 LAN 接口之间的信息交换。

D. 增益天线。在无线网络中，天线可以达到增强信号的目的，可以把它理解为无线信号

的放大器。根据方向性的不同，天线有全向和定向两种。

E. 硬件参数。作为专业人士，除了需要了解上述的 4 个参数以外，还需要了解无线路由器的 CPU 和内存以及 ROM 的大小。目前在市场中，旗舰级的家用路由器一般会标注 CPU、内存、ROM 的参数。

(2) 无线路由器的工作原理

无线路由器其实是一个简单的 NAT 应用，作为普通用户来说，只需要按照说明书使用即可。但作为计算机专业的学生而言，则需要了解并掌握无线路由器的工作原理。

如图 1－2－3 所示为一个基本的 NAT 应用。

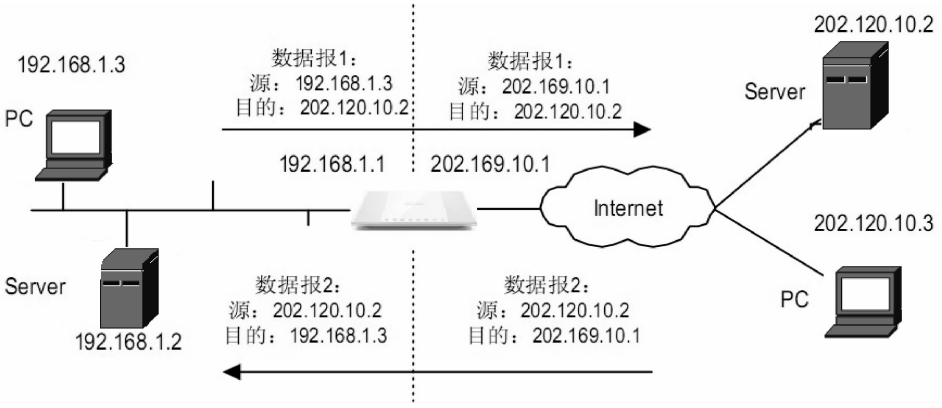

图 1－2－3　无线路由器地址转换的基本过程

无线路由器处于私有网络和公有网络的连接处。当内部 PC(192.168.1.3)向外部服务器(202.120.10.2)发送一个数据报 1 时，数据报将通过无线路由器。NAT 进程查看报头内容，发现该数据报是发往外网的，那么它将数据报 1 的源地址字段的私有地址 192.168.1.3 转换成一个可在 Internet 上选路的公有地址 202.169.10.1，并将该数据报发送到外部服务器，同时在网络地址转换表中记录这一映射。外部服务器给内部 PC 发送应答报文 2(其初始目的地址为 202.169.10.1)，到达无线路由器后，NAT 进程再次查看报头内容，然后查找当前网络地址转换表的记录，用原来的内部 PC 的私有地址 192.168.1.3 替换目的地址。

五、实训操作

在综合考虑各个因素之后，小王和小李最终选择联通 8M 光纤到户。在运营商的工作人员完成了接入之后，他们将对采购的无线路由器进行配置。此次操作他们采用了笔记本电脑对路由器进行配置。

1. 宽带 Modem 与无线路由器进行连接

使用超五类网线将 Modem 的 LAN 口与无线路由器的 WAN 口进行连接，使用的超五类线可以是自制也可以是机制线。通电，此时已经完成了硬件的连接。

2. 笔记本电脑与无线路由器的连接

在笔记本电脑桌面的右下角，双击带 X 的无线网卡，得到图 1－2－4 无线网络的链接界面，在选择界面后会看到 TP-LINK_822968 这个无线信号(专业术语 SSID)。

图 1－2－4　无线网络连接界面

双击该 SSID，得到如图 1－2－5 所示的界面。

图 1－2－5　网线连接界面

连接成功以后，显示如图 1－2－6 所示。接下来，我们就可以对无线路由器进行相应的配置。

图 1－2－6　笔记本电脑与无线路由连接成功