第 3 章　交换机基本配置

在计算机网络体系中，人们日常接触到的设备，如台式计算机、笔记本等都只能算是数据终端设备，而单纯靠这些网络终端设备无法搭建出一个真正的网络架构。因此本章和第 4 章将详细介绍计算机网络体系中最常见的网络连接设备——交换机和路由器，以及通过了解 H3C 设备和完成一些简单的实验，帮助读者更加清晰地认识到这些日常接触不到的设备是如何“默默无闻”地支撑起互联网这座“摩天大楼”的。

本章主要知识结构如图 3.1 所示。

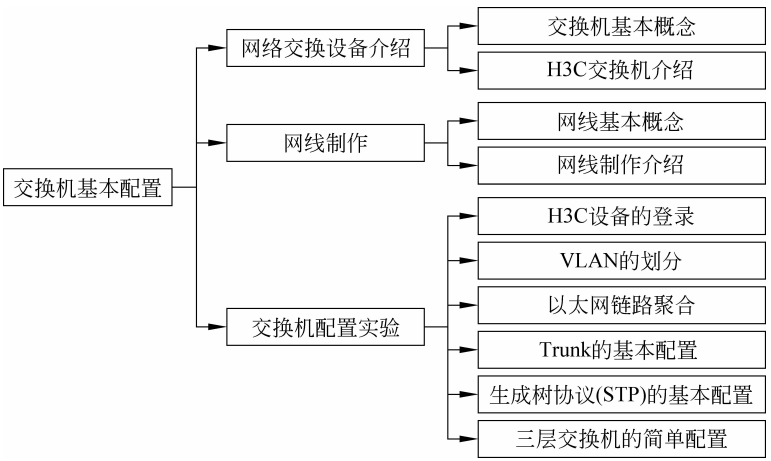

图 3.1　本章主要知识结构

网络交换设备介绍部分，先向读者介绍交换机的基本概念，再介绍 H3C 交换机，让读者能够将一个抽象的概念具体化，对交换设备有一个基本的、初步的认识。

网线制作部分，通过介绍网线技术的发展，并通过图文并茂的形式介绍网线制作方法，使读者特别是使学生读者掌握双绞线的基本制作，在动手实践中了解网线。

交换机配置实验部分，主要是模拟网络工程师在实际工作中最常用到的一些交换机基本配置，通过实验的形式让读者在动手的过程中深入了解交换机的工作原理。

3.1　网络交换设备介绍

3.1.1　交换机基本概念

在正式介绍交换机之前，先看一个简单的图，如图 3.2 所示。

相信读者朋友们对这张图一定不陌生，这就是一个典型的大学四人间宿舍的网络模型，一台带 WiFi 热点功能的“猫”通过网线或者 WiFi 连接着多台网络设备。“猫”的周围这些台式计算机、笔记本或者手机都是我们最常用的设备，在计算机网络中称其为数据终端设备

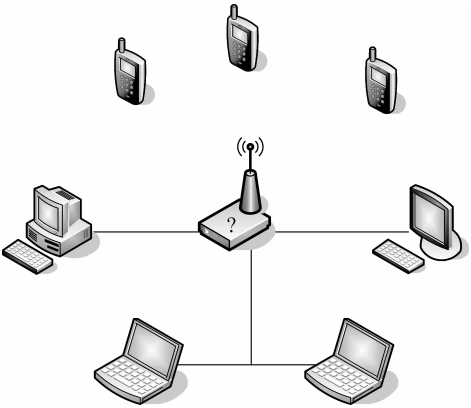

图 3.2　一个常见的网络场景

(Data Terminal Equipment,DTE)。而多数人不感兴趣的那个“猫”,正是本章开始介绍的重点,数据通信设备(Data Circuit-terminating Equipment,DCE)。由于运营商和设备提供商为了加速普及这些网络设备,方便用户使用,大都采用了图形化甚至是“傻瓜式”的安装配置方式,而真正的网络工程师操作的大型骨干网络上的路由交换设备,都是使用最直接的通过 Console 口输入命令行方式管理和维护网络。本书关于路由交换设备的实验,也是以命令行方式进行的。

那么简单介绍了 DTE 和 DCE 之后,下面就来正式介绍一下本章的主角交换机了。

交换机(Switch)是一种用于电信号转发的网络设备。它可以为接入交换机的任意多个网络节点提供独享的电信号通路。按照通信两端传输信息的需要,用人工或设备自动完成的方法,把要传输的信息送到符合要求的相应路由上。交换机根据工作位置的不同,可以分为广域网交换机和局域网交换机。广义的交换机就是一种在通信系统中完成信息交换功能的设备,它应用在数据链路层。交换机有多个端口,每个端口都具有桥接功能,可以连接一个局域网或一台高性能服务器或工作站。实际上,交换机有时也被称为多端口网桥。目前市面上最常见的交换机是以太网交换机。

3.1.2　H3C 交换机介绍

由于交换机是重要的网络设备,一般情况下也只有运营商或中型以上企业才会用到,因此市面上交换机的价格也通常较贵,读者如果只是为了学习需要可以到学校的网络实验室或者是专门的租用机架进行实验。目前,中国市场主要的交换机厂商有美国的思科(CISCO)、瞻博(Juniper)和中国的华为(HUAWEI)、华三(H3C)等。

杭州华三通信技术有限公司(H3C)是一家主要提供 IT 基础架构产品及方案的研究、开发、生产、销售及服务的公司。H3C 不但拥有全线路由器和以太网交换机产品(如图 3.3 所示),还在网络安全、云存储、云桌面、硬件服务器、WLAN、SOHO 及软件管理系统等领域稳健成长。本书编写时进行实验的设备使用的也都是 H3C 的网络设备。本章编写时使用的二层交换机为 H3C 的 3100 系列。该系列交换机

图 3.3　H3C 的 3100 系列以太网交换机

具有 19.2Gb/s 的总线带宽，能为所有端口提供两层线速交换功能，同时支持千兆上行、安全控制、MAC 地址和端口等多元组绑定、广播风暴抑制功能，支持跨交换机的远程端口镜像功能(RSPAN)，可以将接入端口的流量镜像到核心交换机上，是目前市场上比较主流的两层智能交换机设备。

3.2 网线制作

3.2.1 网线基本概念

1. 网线

我们都知道，要想通过有线的方式连接网络，网线是必不可少的。但是网线实际上是一个泛指，广义中的网线是指在局域网中使用的任何一种连接网络的线缆。目前常见的网线主要有双绞线、同轴电缆、光纤三种。现在随着“电力猫”技术的发展，电线也逐渐成为另一种网线，不过由于技术限制仅限于家庭局域网中。而人们日常生活中所说的网线一般都是指双绞线，如图 3.4 所示。

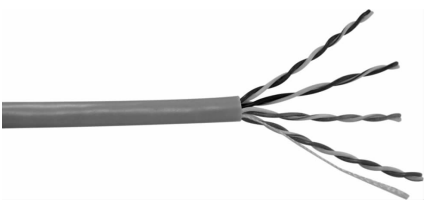

图 3.4 双绞线

2. 双绞线

双绞线是由许多对线并用 RJ-45 水晶头作为端口组成的数据传输线。它的特点就是价格便宜，所以被广泛应用。双绞线是由一对相互绝缘的金属导线绞合而成。采用这种方式，不仅可以抵御一部分来自外界的电磁波干扰，也可以降低多对绞线之间的相互干扰。双绞线过去主要是用来传输模拟信号的，现在同样适用于数字信号的传输，是日常生活中网络布线最常见的线缆。

双绞线依照其职能不同，可以分为表 3.1 中的几类。

表 3.1 双绞线的分类

种类名称	用　　途
一类线	报警系统，或只适用于语音传输
二类线	语音传输和极低速率数据传输的令牌网络
三类线	语音、10Mb/s 以太网和 4Mb/s 令牌环路
四类线	基于令牌的局域网和最高 100Mb/s 以太网
五类线	主要用于百兆和千兆以太网络，是最常用的
六类线	适用于传输速率高于 1Gb/s 的以太网
七类线	用于今后的 10Gb/s 以太网

3.2.2 网线制作介绍

在 3.2.1 节中介绍了网线，特别是双绞线的一些基本知识，下面从实际的角度介绍网线的制作。

在图 3.4 上已经看到了双绞线是由 8 种颜色的线缆两两缠绕而成，分别是绿、绿白、蓝、蓝白、橙、橙白、棕、棕白。这些线两两缠绕以屏蔽网络传输过程中的干扰信号。在网线组装过程中，双绞线有两种接法：EIA/TIA-568B 标准和 EIA/TIA-568A 标准。

1. T568A 线序

1	2	3	4	5	6	7	8
绿白	绿	橙白	蓝	蓝白	橙	棕白	棕

2. T568B 线序

1	2	3	4	5	6	7	8
橙白	橙	绿白	蓝	蓝白	绿	棕白	棕

最常见的双绞线连接方式主要有直通线和交叉线，接下来分别介绍这两种线的用途和接法。

直通线，不难理解就是线是直接按照顺序插到接口里的，没有任何“技术含量”。事实上也正是如此，双绞线两头都按照 T568B 线序插入 RJ-45 水晶头组成的线就是直通线。直通线主要用于不同设备之间的连接，比如计算机连接交换机等，直通线的线序如图 3.5 所示。

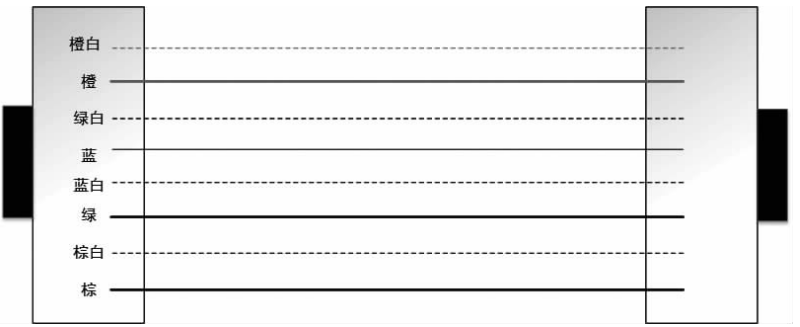

图 3.5　直通线的线序

交叉线，这也是一个能够顾名思义的名称，显然听起来就是这 8 股线要有交叉的部分。事实上，交叉线的一头按照 T568A 标准，另一头按照 T568B 标准接线，这样就完成了交叉线的制作。交叉线主要用于同种设备之间的连接，比如两台交换机或者两台 PC 之间。交叉线的线序如图 3.6 所示。

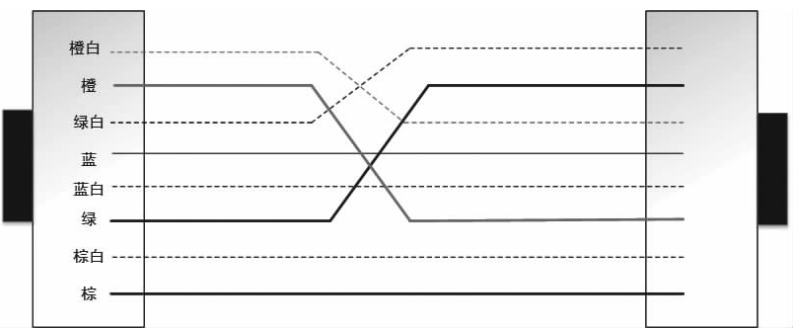

图 3.6　交叉线的线序

除了这两种最常见的接线方式之外，双绞线还有第三种接线方法，称为反转线。简单来

说是将线缆的一端采用 T568A 或 T568B 作线标准，另一端把 T568A 或 T568B 的顺序刚好从第一根到最后一根反过来。反转线通常用于实现从主机到路由器控制台串行通信(COM)端口的连接，也就是路由交换设备上的 Console 口。在通过计算机配置网络交换设备的时候通常都是利用反转线连接 Console 口完成对设备的操作。

3.3 交换机配置实验

3.3.1 H3C 设备的登录

当用户使用 Console 口、AUX 口、异步串口(包括工作在异步方式的同/异步串口，即 Serial 接口和专用异步串口，即 Async 接口)、Telnet 或者 SSH 方式登录设备的时候，系统会分配一个用户界面(也称为 Line)用来管理、监控设备和用户间的当前会话。每个用户界面有对应的用户界面视图，在用户界面视图下网络管理员可以配置一系列参数，比如用户登录时是否需要认证、是否重定向到别的设备以及用户登录后的级别等，当用户使用该用户界面登录的时候，将受到这些参数的约束，从而达到统一管理各种用户会话连接的目的。

目前 H3C 设备支持的登录方式有以下几种。

(1) Console 口本地配置。

(2) AUX 口本地或远程配置。

(3) 异步串口本地或远程配置。

(4) Telnet 或 SSH 本地或远程配置。

而与这些配置方式对应的是 4 种类型的用户界面。

(1) Console 用户界面：用来管理和监控通过 Console 口登录的用户。Console 口端口类型为 EIA/TIA-232 DCE。

(2) AUX 用户界面：用来管理和监控通过 AUX 口登录的用户。AUX 口(Auxiliary Port，辅助端口)端口类型为 EIA/TIA-232 DTE，通常用于通过 Modem 拨号访问。

(3) TTY(True Type Terminal，实体类型终端)用户界面：用来管理和监控通过 TTY 方式登录的用户。TTY 方式是指异步串口的登录方式。

(4) VTY(Virtual Type Terminal，虚拟类型终端)用户界面：用来管理和监控通过 VTY 方式登录的用户。VTY 口属于逻辑终端线，用于对设备进行 Telnet 或 SSH 访问。

接下来，通过实验依次实现各种方式对 H3C 设备的访问。

1. 通过 Console 口登录设备

1) Console 口的连接设置

接好相关线缆，然后在“开始”菜单中，选择“附件”→“通信工具”→“超级终端”，设置好区号后就可以进入“新建连接”对话框，如图 3.7 所示。

任意填写名称后(如 telnet)单击“确定”按钮，就进入了一个选项配置，选择 COM1 口登录 Console，如图 3.8 所示。

最后，在“COM1 属性”对话框中把每秒位数调整为“9600”，关闭数据流控制。单击“确定”按钮继续，如图 3.9 所示。

此时，在名为“telnet”的连接中，如果之前的物理链路没有问题，就可以显示交换机管理界面，如图 3.10 所示。

图 3.7　新建连接

图 3.8　选择区号和连接端口

图 3.9　配置 COM1 属性

图 3.10　利用 Console 直接登录设备

接下来从 2)开始,学习一下如何利用 Console 口在命令行配置 H3C 设备登录的各种认证方式。

2) Console 口的认证机制——None 方式

原理:None 方式意味着下次使用 Console 口在本地登录设备时,不需要进行用户名和密码认证,任何人都可以通过 Console 口登录到设备上,这种情况可能会带来安全隐患。

配置步骤:

```
<H3C>system-view                                    //进入全局模式
[H3C]user-interface console 0                       //进入 console 0 口配置
```

```
[H3C-ui-console0]authentication-mode none          //设置认证模式为 none
[H3C-ui-console0]quit                              //退回普通模式
[H3C]quit                                          //退回初始状态
```

配置过程如图 3.11 所示。

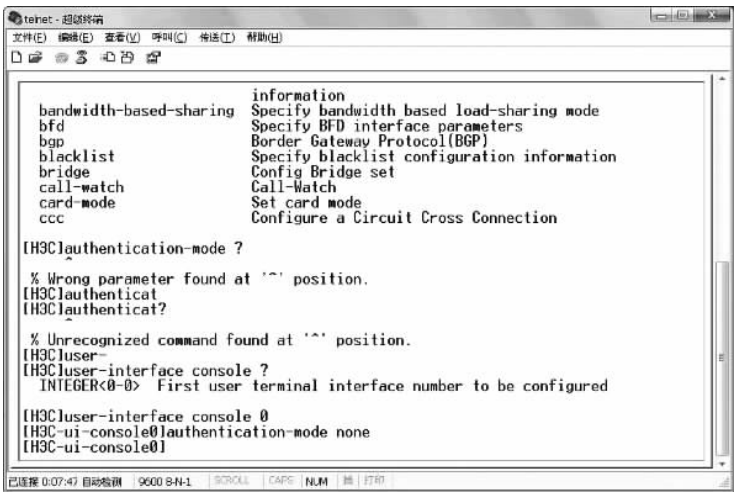

图 3.11　None 方式配置过程

再次登录的时候，就会发现系统在重启之后可以直接登录设备，如图 3.12 所示。但我们可以发现这显然对于企业用户来说是不安全的。

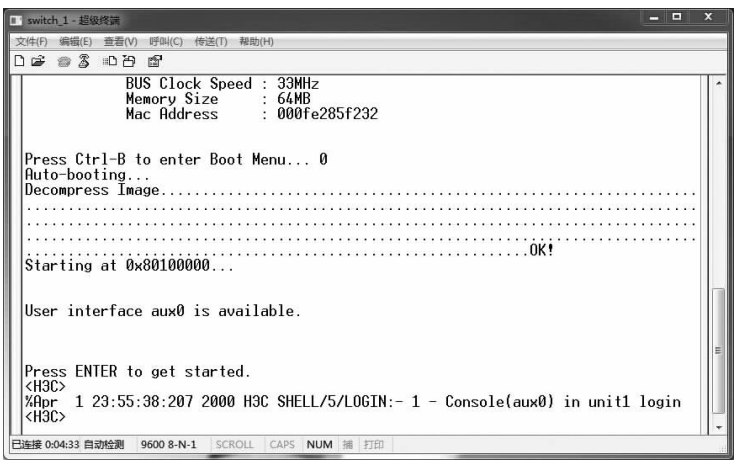

图 3.12　None 方式登录结果

3）Console 口的认证机制——Password 方式

原理：Password 方式意味着下次使用 Console 口本地登录设备时，需要进行密码认证、只有密码认证成功，用户才能登录到设备上。配置认证方式为 Password 后，需要管理员妥善保存密码。

配置步骤：

```
<H3C>system-view                                          //进入全局模式
[H3C]user-interface console 0                             //进入 console 0 口配置
[H3C-ui-console0]authentication-mode password             //设置认证模式为 password
[H3C-ui-console0]set authentication password cipher 111111      //设置密码为 111111
[H3C-ui-console0]quit                                     //退回普通模式
[H3C]quit                                                 //退回初始状态
```

配置过程如图 3.13 所示。

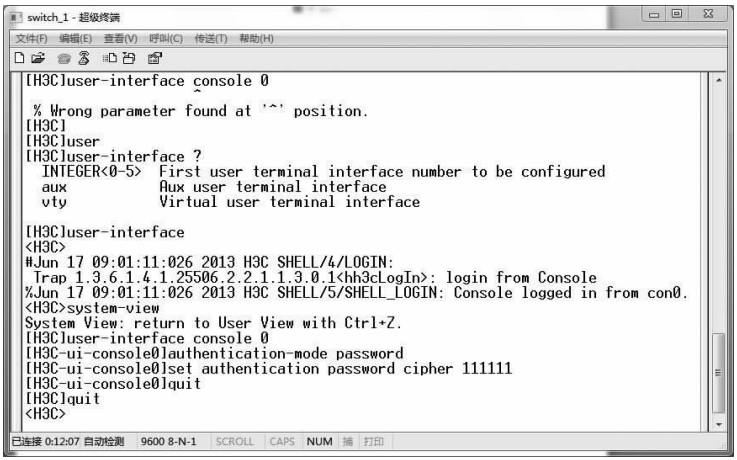

图 3.13　Password 方式配置过程

再次登录时，就会发现设备要求我们输入密码了，输入密码的时候终端上不显示任何内容，回车后如果正确则直接进入系统，如图 3.14 所示。

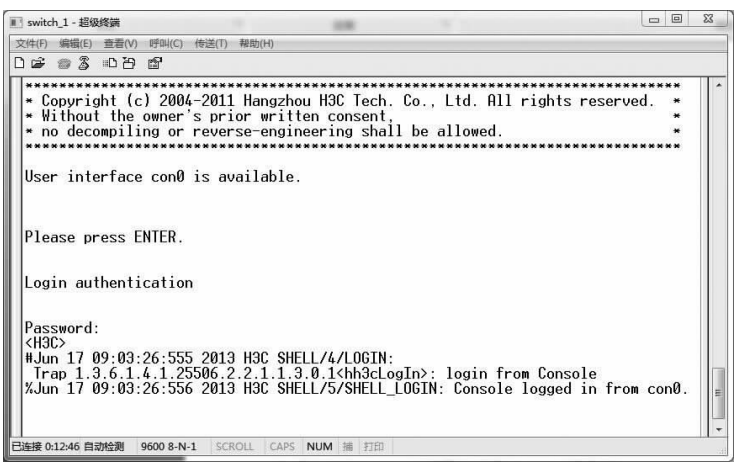

图 3.14　Password 方式登录结果

4）Console 口的认证机制——Scheme 方式

原理：Scheme 方式意味着下次使用 Console 口登录设备时需要进行用户名和密码认证，用户名或密码错误，均会导致登录失败。用户认证又分为本地认证和远程认证，如果采用本地认证，则需要配置本地用户及相应参数；如果采用远程认证，则需要在远程认证服务

器上配置用户名和密码。配置认证方式为 Scheme 后，管理员需要妥善保存用户名及密码。

配置步骤：

```
<H3C>system-view                                    //进入全局模式
[H3C]user-interface console 0                       //进入 console 口配置
[H3C-ui-console0]authentication-mode scheme         //设置认证模式为 scheme
[H3C-ui-console0]quit                               //退回普通模式
[H3C]local-user tjutscce                            //设置用户名 tjutscce
[H3C-luser-tjutscce]password simple tjutscce        //设置用户名对应密码 tjutscce
[H3C-luser-tjutscce]service-type terminal           //无用户服务类型
[H3C-luser-tjutscce]quit                            //退回普通模式
[H3C]quit                                           //退回初始状态
```

配置过程如图 3.15 所示。

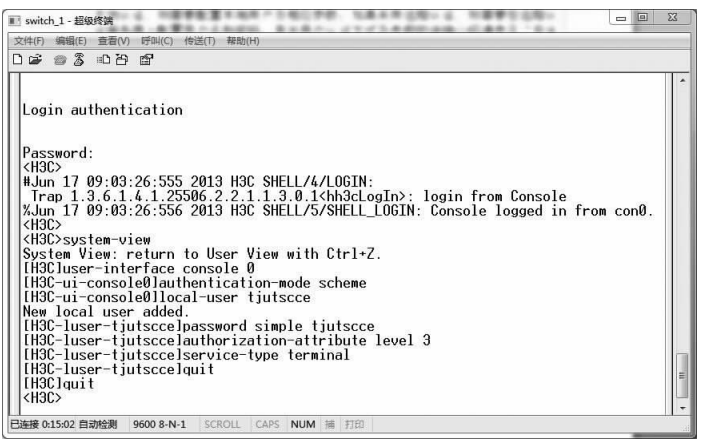

图 3.15　Scheme 方式配置过程

再次登录时，系统会要求我们依次输入用户名和密码，将预先设好的用户名“tjutscce”和密码“tjutscce”输入进去，就能成功登录了，如图 3.16 所示。这个方法要比 Password 方

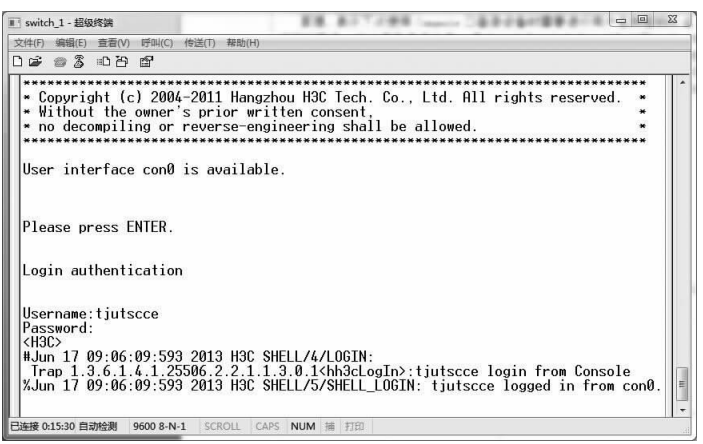

图 3.16　Scheme 方式登录结果

式更加安全，同时还可以通过 authorization-attribute level 命令行为用户设置等级，图 3.15 中的 level 3 为管理员级，意味着当用户登录输入完成用户名和密码认证通过后自动进入系统配置模式。

2. 通过 Telnet 登录设备

默认情况下，H3C 设备不允许用户直接通过 Telnet 方式登录设备。如需采用 Telnet 方式登录，需要管理员先通过 Console 口本地登录设备，再对服务器进行配置，使之支持 Telnet 登录。

1）Telnet 登录主机的基本配置

我们知道，Console 口是无所谓 IP 地址这个概念的，因此它使用之前提到的“小众”的反转线来连接网络设备，而 Telnet 要求主机和交换机处于同一个局域网内的时候才能正常连接，因此要先将主机的本地 IP 地址调整为和设备一样的 IP 地址。

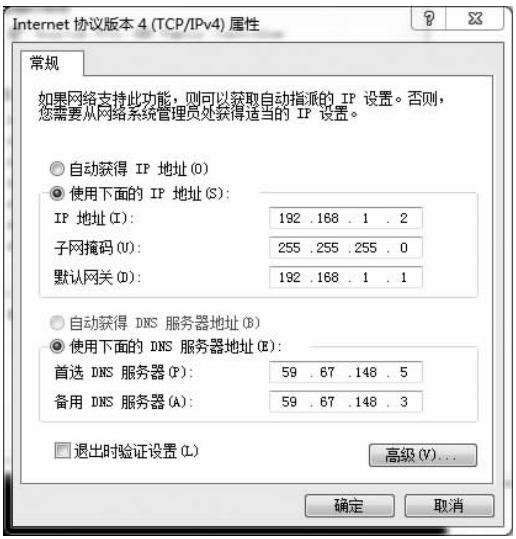

图 3.17　配置主机 IP 地址

本实验中局域网采用 C 类地址通用私有地址网段 192.168.1.0/24。因此需要先将主机的 IP 地址设为 192.168.1.X/24。以 192.168.1.2/24 为例，先进入 Windows 下本地连接的“Internet 协议版本 4”属性，将 IP 地址设为 192.168.1.2，子网掩码设为 255.255.255.0，默认网关设为 192.168.1.1，如图 3.17 所示。

之后，进入 Windows 的命令控制台(CMD)中，输入命令行 telnet 19.168.1.1 回车，结果竟然是不能成功！显然，这是因为之前提到的 H3C 设备为了安全起见默认关掉了 Telnet 连接，因此要先利用 Console 口进入设备将交换机的 Telnet 服务打开。

2）Telnet 登录的认证机制——None 方式

与 Console 默认的 None 模式相同，Telnet 登录在开启的时候也默认开启 None 模式，本实验在开启的同时也向读者演示 None 认证方式的命令行如何配置。

配置步骤：

```
<H3C>system-view                                    //进入全局模式
[H3C]user-interface vty 0                           //进入 vty 口进行配置
[H3C-ui-vty0]telnet server enable                   //启动 telnet 服务
[H3C-ui-vty0]authentication-mode none               //认证方式设为 none 方式
[H3C-ui-vty0]user privilege level 3                 //telnet 登录后的等级为管理级别 3 级
[H3C-ui-vty0]quit                                   //退回普通模式
[H3C]quit                                           //退回初始状态
```

配置过程如图 3.18 所示。

配置完成后就可以在 Windows 下的“运行”对话框中输入“cmd”回车就能进入

Windows 的命令控制台了，如图 3.19 所示。

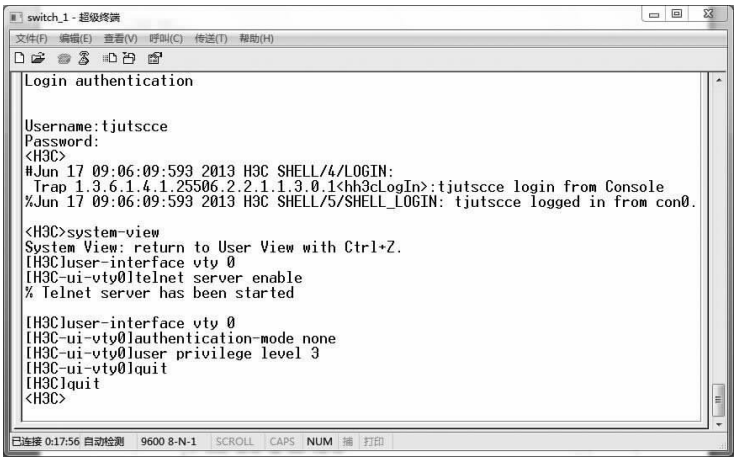

图 3.18　None 方式配置过程

图 3.19　进入命令控制台

在进入 Windows 的命令控制台后再输入命令行 telnet 192.168.1.1 回车，就能成功进入 H3C 交换机的管理界面了，如图 3.20 所示。

图 3.20　None 方式登录结果

3）Telnet 登录的认证机制——Password 方式

配置步骤：

```
<H3C>system-view                                    //进入全局模式
[H3C]user-interface vty 0                           //进入 vty 口进行配置
[H3C-ui-vty0]telnet server enable                   //启动 telnet 服务
[H3C-ui-vty0]authentication-mode password           //认证方式设为 password 方式
[H3C-ui-vty0]set authentication password simple 111111          //设置密码为 111111
[H3C-ui-vty0]user privilege level 3                 //telnet 登录后的等级为管理级别 3 级
[H3C-ui-vty0]quit                                   //退回普通模式
[H3C]quit                                           //退回初始状态
```

配置过程如图 3.21 所示。

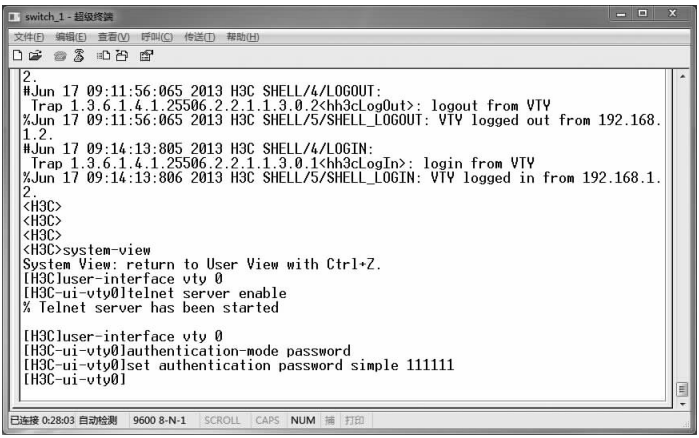

图 3.21　Password 方式配置过程

在进入 Windows 的命令控制台后再输入命令行 telnet 192.168.1.1 回车，我们就被要求和 Console 口下的 Password 登录一样需要输入密码了，当然密码的输入也不会有任何显示，回车后通过认证进入管理界面，如图 3.22 所示。

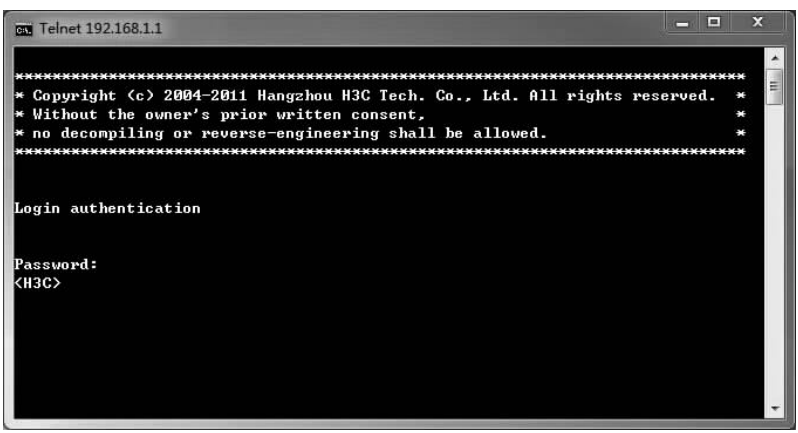

图 3.22　Password 方式登录结果

4）Telnet 登录的认证机制——Scheme 方式

配置步骤：

```
<H3C>system-view                                    //进入全局模式
[H3C]user-interface vty 0                           //进入 vty 口进行配置
[H3C-ui-vty0]telnet server enable                   //启动 telnet 服务
[H3C-ui-vty0]authentication-mode scheme             //认证方式设为 scheme 方式
[H3C-ui-vty0]quit                                   //退回到全局模式
[H3C]local-user tjutscce                            //新建一个用户名为 tjutscce
[H3C-luser-tjutscce]password simple tjutscce        //设置用户名对应的密码为 tjutscce
[H3C-luser-tjutscce]service-type telnet             //设置服务类型为 telnet 服务
[H3C-luser-tjutscce]user privilege level 3          //telnet 登录后的等级为管理级别 3 级
[H3C-luser-tjutscce]quit                            //退回普通模式
[H3C]quit                                           //退回初始状态
```

配置过程如图 3.23 所示。

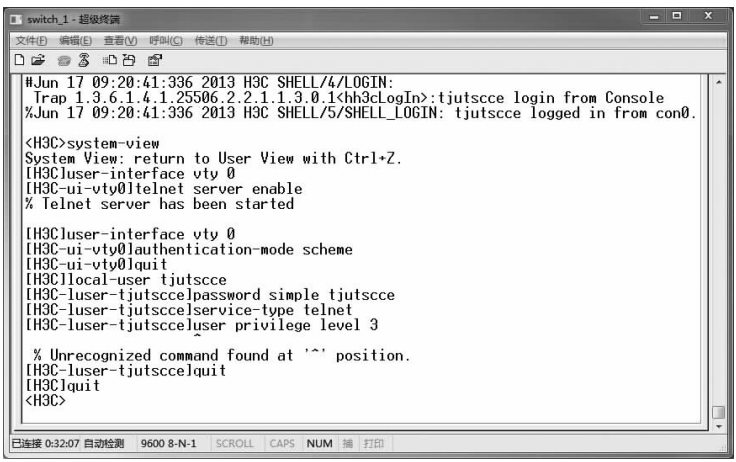

图 3.23　Scheme 方式配置过程

在进入 Windows 的命令控制台后再输入命令行 telnet 192.168.1.1 回车，我们就被要求和 Console 口下的 Scheme 登录一样需要输入用户名和密码了，输入完成回车后通过认证进入管理界面，如图 3.24 所示。

图 3.24　Scheme 方式登录结果

3. 通过 SSH 登录设备

原理：SSH 是 Secure Shell(安全外壳)的简称。用户通过一个不能保证安全的网络环境远程登录到设备时，SSH 可以利用加密和强大的认证功能提供安全保障，保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。设备支持 SSH 功能，用户可以通过 SSH 方式登录到设备上，对设备进行远程管理和维护。

默认情况下，用户可以直接通过 Console 口本地登录设备，登录时认证方式为 None(不需要用户名和密码)，登录用户级别为 3。但是这样的登录就失去了 SSH 的安全性，为了体现安全性，本实验使用 RSA 算法进行密钥加密登录，保证安全。

配置步骤：

```
<H3C>system-view                                    //进入全局模式
[H3C]public-key local create RSA                    //生成本地 RSA 密钥对
[H3C]ssh serverenable                               //启动 SSH 服务功能
[H3C]user-interface vty 0
[H3C-ui-vty0]authentication-mode scheme             //认证方式设为 scheme 方式
[H3C-ui-vty0]protocol inbound ssh                   //使配置的用户界面只支持 SSH 协议
[H3C-ui-vty0]local-user tjutscce                    //创建可登录用户 tjutscce
[H3C-luser-tjutscce]password simple tjutscce        //为用户设置对应的密码 tjutscce
[H3C-luser-tjutscce]service-type ssh                //设置 vty 用户服务类型为 ssh 方式
[H3C-luser-tjutscce]user privilege level 3          //telnet 登录后的等级为管理级别 3 级
[H3C-luser-tjutscce]quit                            //退回普通模式
[H3C]quit                                           //退回初始状态
```

配置过程如图 3.25 所示。

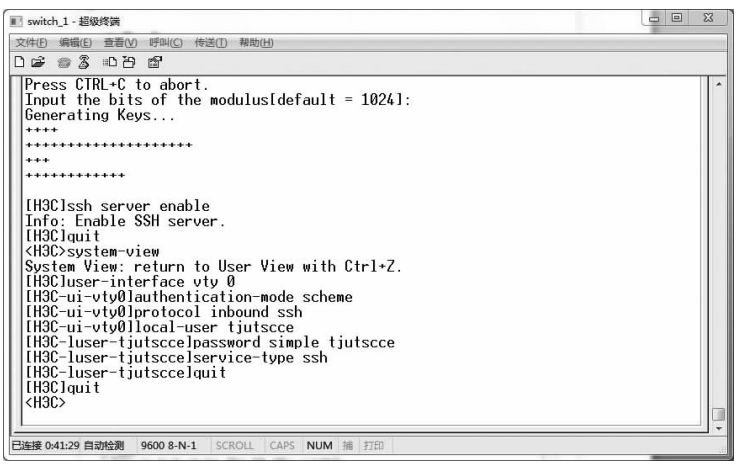

图 3.25　SSH 登录方式配置过程

这里要用专门进行 SSH 登录的软件进行连接。启动软件后，在 Connect to Remote Host 对话框中依次填写 IP 地址、登录名、端口号和选择认证方式，按照之前的设置分别正确填入后单击 Connect 按钮即可，如图 3.26 所示。

之后弹出来的界面就是要求输入登录密码，将之前设置的“tjutscce”也输入进去，继续，如图 3.27 所示。

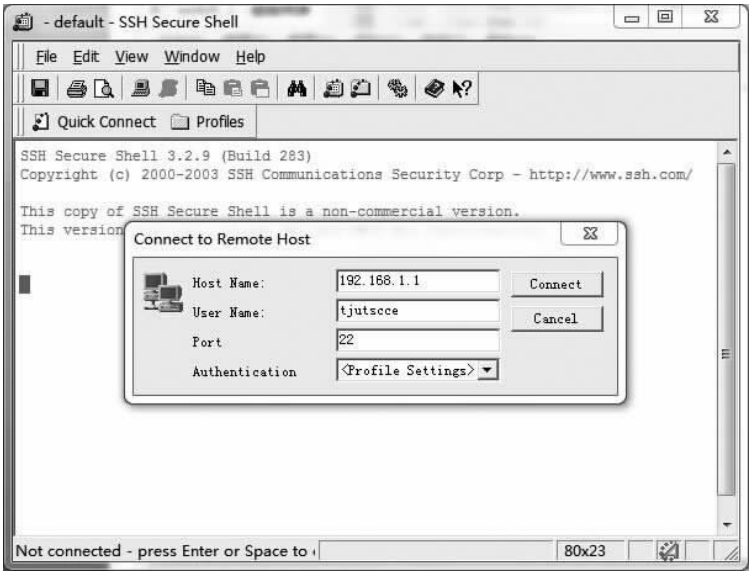

图 3.26　SSH 方式登录过程 1

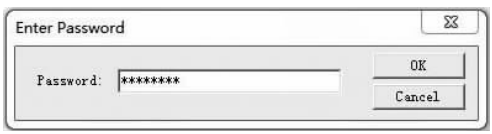

图 3.27　SSH 方式登录过程 2

全部完成后如果一切正常，就可以正确进入交换机的登录配置界面了，如图 3.28 所示。

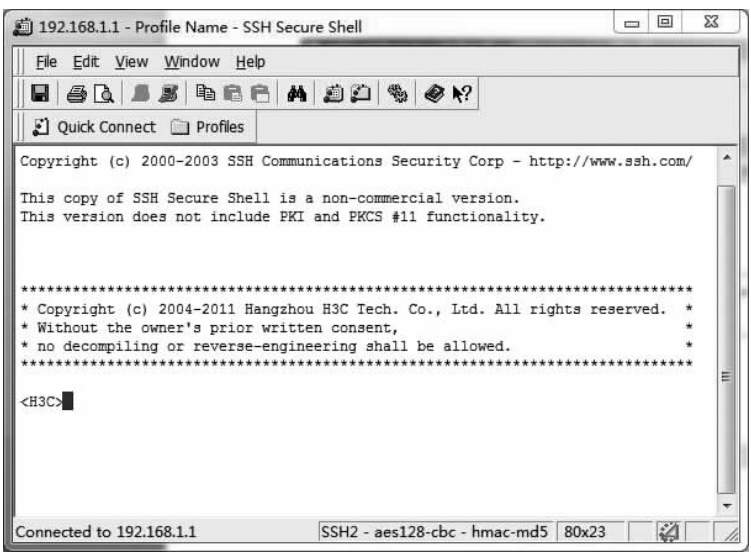

图 3.28　SSH 方式登录结果

4. 通过 HTTP 登录设备

这种方式的管理类似于人们常见的家庭路由器用的那种图形界面，利用 HTTP 让管理员通过浏览器管理计算机。

配置步骤：

```
<H3C>system-view                                    //进入全局模式
[H3C]ip http enable                                 //启动 HTTP 服务模式
[H3C]local-user tjutscce                            //创建可登录用户 tjutscce
[H3C-luser-tjutscce]password simple tjutscce        //为用户设置对应的密码 tjutscce
[H3C-luser-tjutscce]service-type telnet             //设置用户服务类型为 telnet 方式
[H3C-luser-tjutscce]quit                            //退回普通模式
[H3C]quit                                           //退回初始状态
```

配置过程如图 3.29 所示。

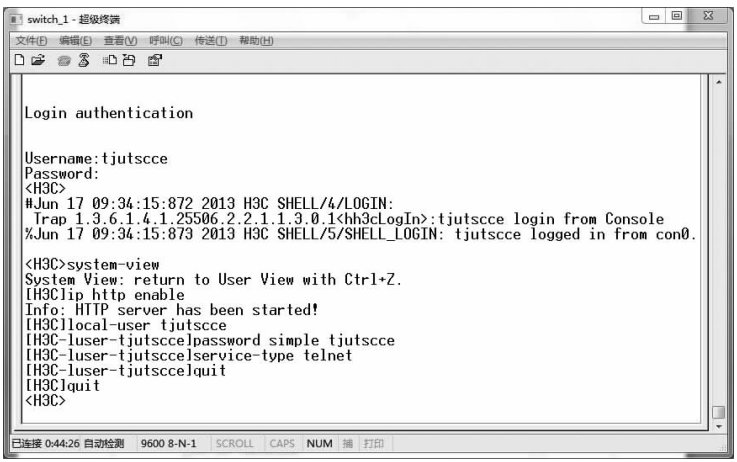

图 3.29　HTTP 方式配置过程

此时打开浏览器输入 http://192.168.1.1 后回车，即可进入如图 3.30 所示的登录界面。

图 3.30　HTTP 方式登录界面

输入正确的用户名和密码后，就能正常登录进控制页面了，如图 3.31 所示。

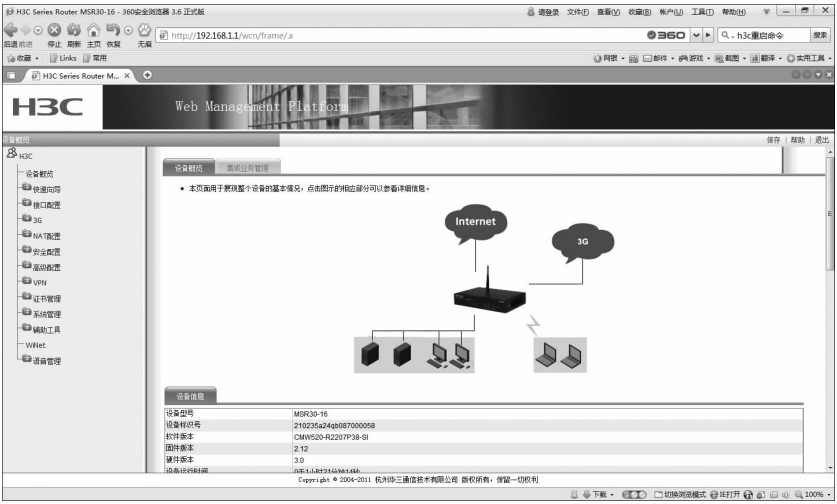

图 3.31　H3C 的 Web 管理界面

3.3.2　VLAN 的划分

1. VLAN 的概念

VLAN(Virtual Local Area Network，虚拟局域网)是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。VLAN 是一种比较新的技术，工作在 OSI 参考模型的第二层和第三层，一个 VLAN 就是一个广播域，VLAN 之间的通信是通过第三层的路由器来完成的。与传统的局域网技术相比较，VLAN 技术更加灵活，它具有以下优点：网络设备的移动、添加和修改的管理开销减少；可以控制广播活动；可提高网络的安全性。

2. 实验拓扑

本实验的拓扑如图 3.32 所示。

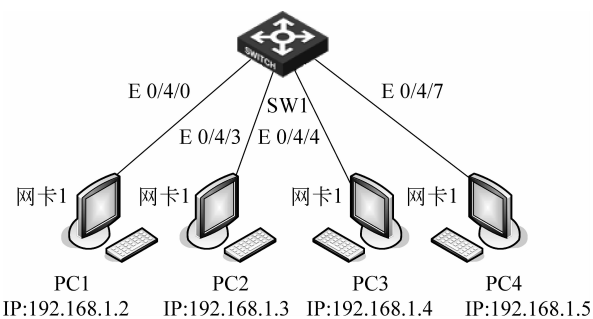

图 3.32　本实验拓扑

3. 实验内容

将交换机的前 4 个端口设置为 VLAN10，将后 5，6，7，8 端口设置为 VLAN11，并验证

虚拟局域网的效果。

4. 实验目标

从图 3.32 的拓扑中可以看到以太网接口 0/4/0 到 0/4/3 这 4 个接口连接着 PC1 和 PC2，以太网接口 0/4/4 到 0/4/7 这 4 个接口连接着 PC3 和 PC4，而 4 个 PC 的 IP 地址都处在 192.168.1.0/24 这个网段内。学过《计算机网络》课程的同学或有一定网络基础的读者应该知道，当交换机在默认情况下由于这 4 台主机处于同一网段，因此它们之间是能相互通信的，即使用 ping 命令可以相互 ping 通。而当我们按照实验内容的要求设置 VLAN10 和 VLAN11 后，这两个 VLAN 对应的交换机端口连接着的设备在 VLAN 内可以相互 ping 通，而不同 VLAN 之间则无法 ping 通。由此可以验证 VLAN 是否设置成功。

5. 实验步骤

首先来验证一下在默认情况下 PC1 是否能够 ping 通 PC4。

打开 PC1 的命令窗口，输入 ping 192.168.1.5 后回车，看一下结果，如图 3.33 所示。

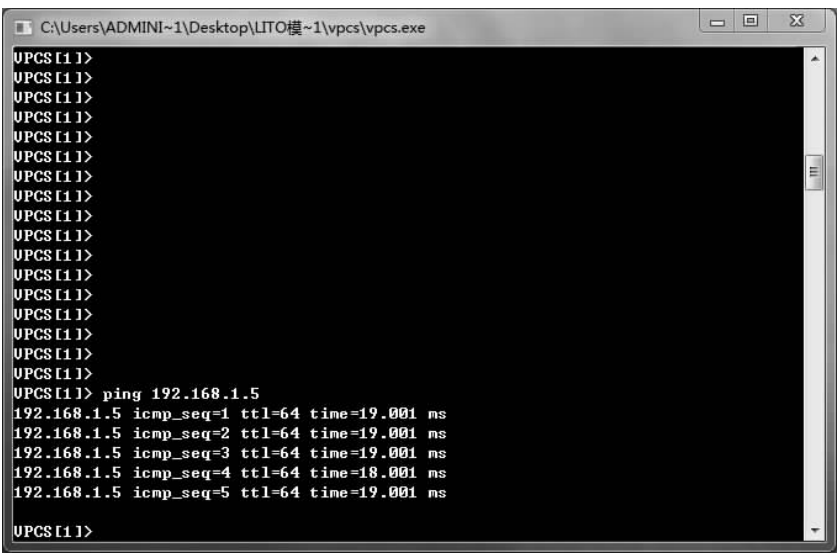

图 3.33　本实验拓扑

如图 3.33 所示，我们可以看到 PC1 是可以 ping 通 PC4 的，其他 PC 之间相互 ping 之后，可以发现交换机已经开始实现同一个局域网内的通信了。那么，我们就开始按照要求，设置 VLAN10 和 VLAN11 组建虚拟局域网，首先从 VLAN10 开始。

配置步骤：

```
<SW1>system-view                                    //进入交换机全局模式
[SW1]vlan 10                                        //创建名为"10"的 vlan
[SW1-vlan10]description 10                          //添加对 vlan 10 的描述
[SW1-vlan10]display vlan                            //查看 vlan 相关信息
[SW1-vlan10]port Ethernet 0/4/0 to Ethernet 0/4/3
                                          //将 0/4/0 口到 0/4/3 口的端口划入 vlan10 中
[SW1-vlan10]quit                                    //退回全局模式
```

配置过程如图 3.34 所示。

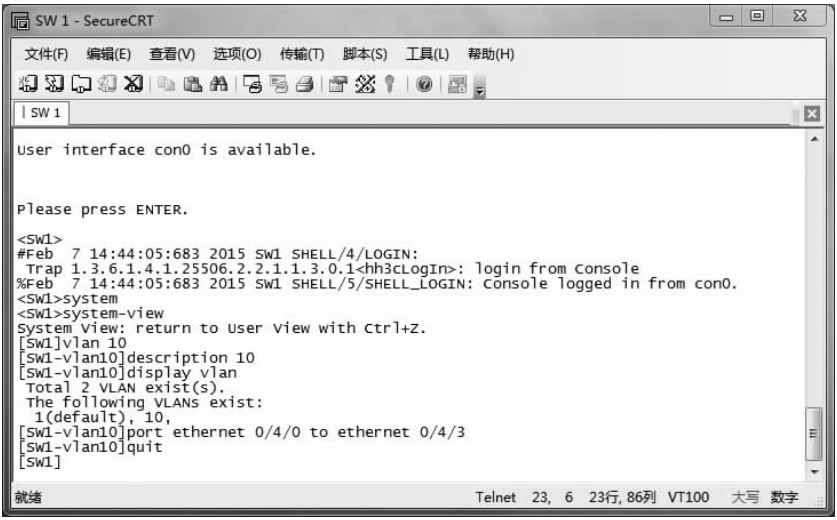

图 3.34 VLAN10 的配置过程

此时,再输入 display vlan 10 看一下现在 VLAN 的情况,如图 3.35 所示。

```
[SW1]display vlan 10
 VLAN ID: 10
 VLAN Type: static
 Route Interface: not configured
 Description: 10
 Name: VLAN 0010
 Broadcast MAX-ratio: 100%
 Tagged   Ports: none
 Untagged Ports:
    Ethernet0/4/0            Ethernet0/4/1            Ethernet0/4/2
    Ethernet0/4/3
```

图 3.35 VLAN10 的详情

从图中可以看到,以太网接口 0/4/0 到接口 0/4/3 已经被划到 VLAN10 下了,下面继续配置 VLAN11。

配置步骤:

```
<SW1>system-view                                    //进入交换机全局模式
[SW1]vlan 11                                        //创建名为"11"的 vlan
[SW1-vlan11]description 11                          //添加对 vlan 11 的描述
[SW1-vlan11]display vlan                            //查看 vlan 相关信息
[SW1-vlan11]port Ethernet 0/4/4 to Ethernet 0/4/7
                                          //将 0/4/4 口到 0/4/7 口的端口划入 vlan11 中
[SW1-vlan11]quit                                    //退回全局模式
```

配置过程如图 3.36 所示。

此时,再输入 display vlan 11 看一下现在 VLAN 的情况,如图 3.37 所示。

现在已经将 VLAN10 和 VLAN11 都配置好了,接下来就来验证一下是否能够像我们预想的结果那样。以 PC1(属于 VLAN10)和 PC3(属于 VLAN11)举例分别 ping 一下 PC2 和 PC4,看一下结果如何。

首先从 PC1 开始,因为 PC2 和它处于同一 VLAN,而 PC4 和它处于不同 VLAN,因此 PC1 应该能 ping 通 PC2,不能 ping 通 PC4。

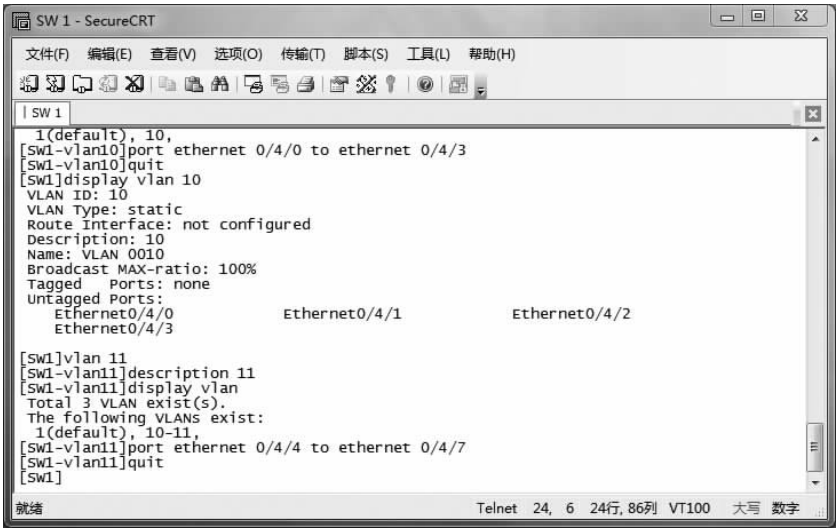

图 3.36 VLAN11 的配置过程

```
[SW1]display vlan 11
 VLAN ID: 11
 VLAN Type: static
 Route Interface: not configured
 Description: 11
 Name: VLAN 0011
 Broadcast MAX-ratio: 100%
 Tagged   Ports: none
 Untagged Ports:
    Ethernet0/4/4            Ethernet0/4/5            Ethernet0/4/6
    Ethernet0/4/7
```

图 3.37 VLAN11 的详情

从图 3.38 可以看到，PC1 是能 ping 通 PC2(192.168.1.3)的，但是不能 ping 通 PC4(192.168.1.5)，接下来看 PC3 去 ping PC2 和 PC4 的结果，如图 3.39 所示。

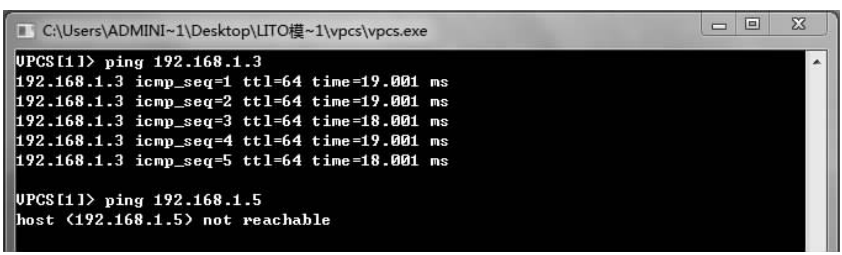

图 3.38 验证 VLAN10 和 VLAN11(1)

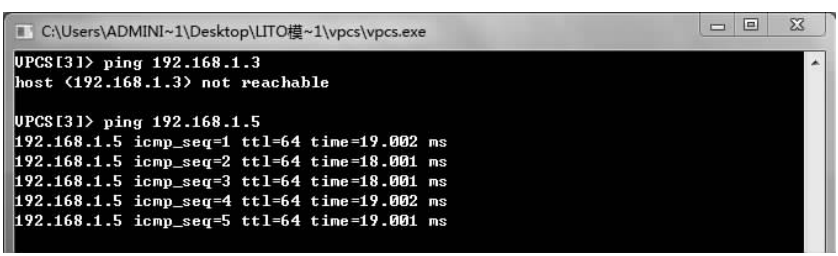

图 3.39 验证 VLAN10 和 VLAN11(2)