新时代　新工匠
职业教育改革创新系列教材

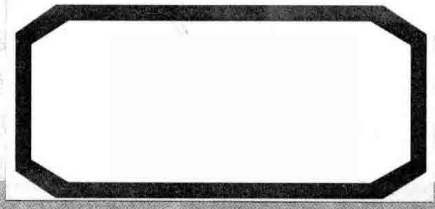
网络信息安全一体化教程

胡定松　黄四清□主　编
周允强　朱国艺□副主编

本书配有电子教学参考资料包

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

新时代　新工匠
职业教育改革创新系列教材



网络信息安全一体化教程

胡定松　黄四清　主　编
周允强　朱国艺　副主编

電子工業出版社
Publishing House of Electronics Industry
北京・BEIJING

内 容 简 介

本书贯彻基于工作过程的课程理念，以“项目式教学”为主要思想，建立以项目为核心、以工作过程为导向、以真实的工作任务为驱动机制的教学过程，采用教、学、做一体化的方式撰写，合理地组织任务，并将每个任务分解为需求分析、方案设计、知识准备、任务实现四个模块，体现教、学、做一体化过程。

全书分为十个项目，内容包括设备安全、VLAN 技术与生成树技术、路由协议、路由重分布与策略路由、访问控制列表、DHCP 与 VRRP、组播、广域网技术、网络安全与 VPN 实现、IPv6 技术与实施。

本书可以作为职业院校、技术院校计算机及相关专业计算机网络课程的实验教材，也可以作为网络培训或相关工程技术人员自学的参考书。

图书在版编目（CIP）数据

网络信息安全一体化教程 / 胡定松，黄四清主编. —北京：电子工业出版社，2017.7

ISBN 978-7-121-32241-9

Ⅰ. ①网… Ⅱ. ①胡… ②黄… Ⅲ. ①计算机网络—信息安全—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2017）第 169097 号

策划编辑：关雅莉
责任编辑：柴　灿
印　　刷：北京七彩京通数码快印有限公司
装　　订：北京七彩京通数码快印有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1 092　1/16　印张：13　字数：382 千字
版　　次：2017 年 7 月第 1 版
印　　次：2017 年 7 月第 1 次印刷
定　　价：28.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254617，luomn@phei.com.cn。

前　言

本书是首批国家级中等职业教育改革与发展示范学校重点建设专业“计算机网络技术”的成果之一，在调研本区域内相关企业岗位的职业能力基础上，深入分析和提取网络技术专业的典型工作任务和岗位技能目标，同时依据毕业生跟踪调查的数据分析，逐步探索、形成新的人才培养方案和专业课程体系，特别是在一体化课程建设方面，取得了预期的目标。

在编写思想上，本书贯彻“基于工作过程”的课程理念，以“项目式教学”为主要思想，建立以项目为核心、以工作过程为导向、以真实的工作任务为驱动机制的教学过程。采用教、学、做一体化的方式进行撰写，合理地组织任务，并将每个任务分解为需求分析、方案设计、知识准备、任务实现四个模块，体现教、学、做一体化的过程。本书侧重于实用性强的网络安全技术，抛开了深奥的理论，以过程化的图片和文字进行表述，直接面向实际工作中的应用环境，使读者更加直观地了解攻击或者防御手法，更加有利于促进计算机专业的学生迅速向网络安全管理人员的角色迈进。本书在内容编排上简单、直观、循序渐进，方便学生积累经验，迅速拉近理论与实践的距离。

本书精选大量的实用案例，循序渐进地介绍了计算机信息安全的基本原理及其应用技术；注重结合经典实例来讲解一些关键技术和应用难点，侧重实用性和启发性。全书分为十个项目，内容包括设备安全、VLAN 技术与生成树技术、路由协议、路由重分布与策略路由、访问控制列表、DHCP 与 VRRP、组播、广域网技术、网络安全与 VPN 实现、IPv6 技术与实施。

本书教学学时建议为 72 学时，在教学过程中可参考以下课时分配表。

项目	课程内容	课程分配		
		讲授	实训	合计
项目一	设备安全	2	2	4
项目二	VLAN 技术与生成树技术	2	4	6
项目三	路由协议	2	4	6
项目四	路由重分布与策略路由	4	6	10
项目五	访问控制列表	2	6	8
项目六	DHCP 与 VRRP	2	6	8
项目七	组播	4	8	12
项目八	广域网技术	2	4	6
项目九	网络安全与 VPN 实现	4	4	8
项目十	IPv6 技术实施	2	2	4
合计		26	46	72

本书由中山市中等专业学校胡定松、黄四清担任主编，周允强、朱国艺担任副主编。教材中的项目一～项目四由胡定松编写；项目五、项目六由黄四清编写；项目七、项目八由朱国艺编写；项目九、项目十由周允强编写。全书由胡定松统稿。

感谢神州数码网络（北京）有限公司在编者编写本书过程中给予的大力支持与指导。

由于编者水平所限，加之时间仓促，书中难免存在疏漏和不足之处，敬请广大读者批评指正。

编　者

2017 年 5 月

目　录

项目一 设备安全

教学背景

企事业单位在组网初期部署了设备的接入功能，随着业务的开展，员工和网络设备越来越多，渐渐地给网管人员带来了很多烦恼。由于公司网络没有经过细致规划，公司员工在各个网络接口均能上网，用户接入网络的身份无法确定，经常发现陌生的主机接入，这给公司的信息安全带来了隐患，而网络中随时可能出现的各种攻击行为也严重威胁到了网络安全。为此，需要网络管理员对设备和网络安全做出规划。

任务一　交换机远程管理

需求分析

某学校有 20 台交换机支撑着校园网的运营，这 20 台交换机分别放置在学校的不同位置。网络管理员需要对这 20 台交换机做管理。管理员可以通过带外管理的方式，即通过 Console 口来管理，但管理员需要带着自己的笔记本式计算机，并且带着 Console 线到学校的不同位置调试交换机，十分麻烦。

方案设计

校园网既然是互连互通的，在网络的任何一个信息点都应该能访问其他的信息点，为什么不通过网络的方式来调试交换机呢？通过 Telnet 方式，管理员即可在办公室中调试全校所有的交换机。

所需设备如图 1-1-1 所示。

（1）DCS 二层交换机 1 台。

（2）PC 1 台。

（3）Console 线 1 条。

（4）直通网线 1 条。

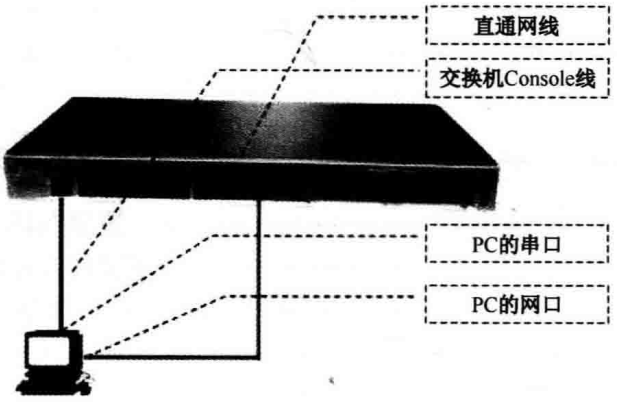


图 1-1-1　交换机远程管理

任务要求如下。

（1）按照拓扑图连接网络。

（2）PC 和交换机的 24 口用网线相连。

（3）交换机的管理 IP 地址为 192.168.1.100/24。

（4）PC 网卡的 IP 地址为 192.168.1.101/24。

知识准备

（1）默认情况下，交换机所有端口都属于 VLAN1，因此通常把 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 个字符。

（3）删除 Telnet 用户时可以在 config 模式下使用 no telnet-user 命令。

（4）使用 Telnet 和 Web 方式调试有以下两个相同的前提条件。

① 交换机开启该功能并设置用户。

② 交换机和主机之间要能连通。

（5）有时候交换机的地址配置正确，主机配置也正确，但就是连不通。排除硬件问题之后可能的原因是主机的 Windows 操作系统开启了防火墙，关闭防火墙即可。

Telnet 方式和 Web 方式都是交换机的带内管理方式。

提供带内管理方式可以使连接在交换机中的某些设备具备管理交换机的功能。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。

Web 方式也称 HTTP 方式，和 Telnet 方式一样，管理员在办公室中即可调试全校所有的交换机。

Web 方式比较简单，如果用户不习惯 CLI 的调试，则可以采用 Web 方式调试。

主流的调试界面是 CLI，大家要着重学习 CLI。

本任务使用 DCS-3926S 系列交换机作为演示设备，其软件版本为 DCS-3926S_6.1.12.0，实际使用中由于软件版本不同，功能和配置方法有可能存在差异，请关注相应版本的使用说明。

任务实现

步骤 1：给交换机的默认 VLAN 设置 IP 地址，即管理 IP 地址。

```
DCS-3926S#config
DCS-3926S(Config)#interface vlan 1                    //进入 VLAN 1 接口
02:20:17: %LINK-5-CHANGED: Interface Vlan1, changed state to UP
DCS-3926S(Config-If-Vlan1)#ip address 192.168.1.100 255.255.255.0 //配置地址
DCS-3926S(Config-If-Vlan1)#no shutdown                //激活 VLAN 接口
DCS-3926S(Config-If-Vlan1)#exit
DCS-23926S(Config)#exit
DCS-3926S#
```

验证配置：

```
DCS-3926S#show run
Current configuration:
!
hostname DCS-3926S
!
Vlan 1
vlan 1
!
Interface Ethernet0/0/1
……
Interface Ethernet0/0/24
!
interface Vlan1
interface vlan 1
ip address 192.168.1.100 255.255.255.0        //已经配置好交换机的 IP 地址
!
DCS-3926S#
```

步骤 2：为交换机设置授权 Telnet 用户。

```
DCS-3926S#config
DCS-3926S(Config)#telnet-user dcnu password 0 digital
DCS-3926S(Config)#exit
DCS-3926S#
```

步骤 3：验证配置。

```
DCS-3926S#show run
Current configuration:
!
hostname DCS-3926S
!
telnet-user dcnu password 0 digital
!
Vlan 1
vlan 1
!
Interface Ethernet0/0/1
……
```

```
Interface Ethernet0/0/24
!
interface Vlan1
interface vlan 1
ip address 192.168.1.100 255.255.255.0
!
DCS-3926S#
```

步骤 4：配置主机的 IP 地址，主机的 IP 地址要与交换机的 IP 地址在一个网段，如图 1-1-2 所示。

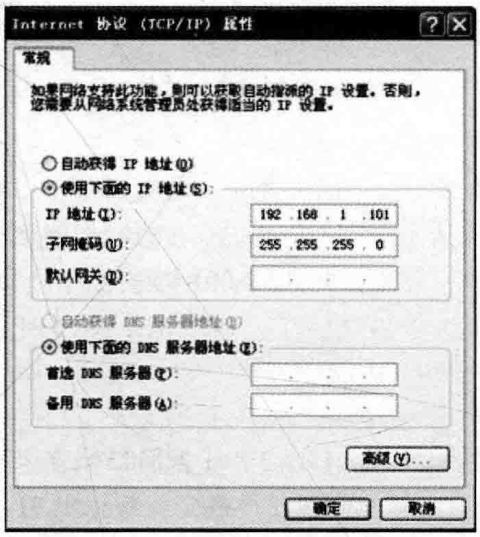


图 1-1-2　配置主机 IP 地址

步骤 5：验证配置。在主机的命令行窗口中使用 ipconfig 命令查看 IP 地址配置情况，如图 1-1-3 所示。

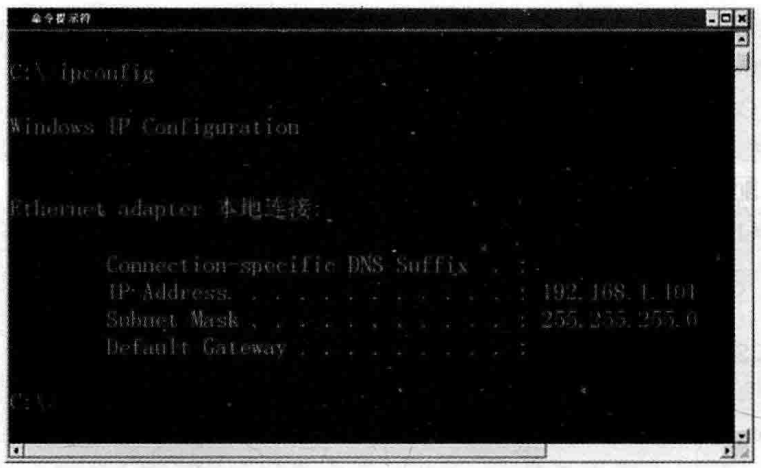


图 1-1-3　查看主机 IP 地址

步骤 6：验证主机与交换机是否连通。

```
DCS-3926S#ping 192.168.1.101
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 192.168.1.101, timeout is 2 seconds.
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1ms
DCS-3926S#
//出现 5 个"!"表示已经连通
```

步骤 7：使用 Telnet 方式登录。登录 PC，选择“开始”→“运行”选项，弹出“运行”对话框，如图 1-1-4 所示，运行 Windows 自带的 Telnet 客户端程序，并且指定 Telnet 的目的地址，需要输入正确的登录名和口令，登录名是 dcnu，口令是 digital。

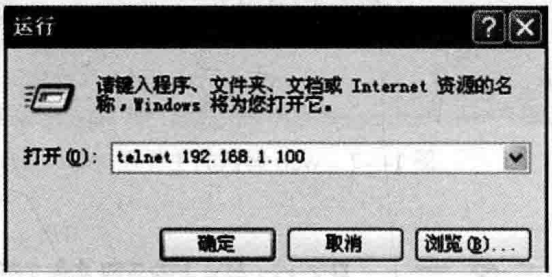


图 1-1-4　运行 Telnet 命令

步骤 8：启动交换机的 Web 服务。

```
DCS-3926S#config
DCS-3926S(Config)#ip http server                    //开启 HTTP 功能
web server is on                                    //表明已经成功启动
DCS-3926S(Config)#
```

步骤 9：设置交换机授权 HTTP 用户。

```
DCS-3926S(Config)#web-user admin password 0 digital    //设置密码
DCS-3926S(Config)#
```

步骤 10：使用 HTTP 方式登录。登录 PC，选择“开始”→“运行”选项，弹出“进行”对话框，如图 1-1-5 所示，指定目标。需要输入正确的登录名和口令，登录名是 admin，口令是 digital，如图 1-1-6 所示。

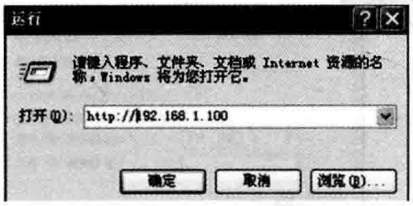


图 1-1-5　运行 HTTP 命令

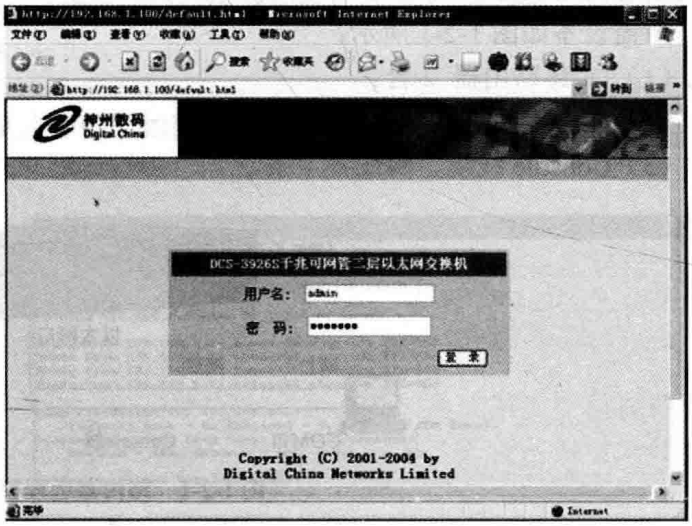


图 1-1-6　输入用户名和密码

步骤 11：图 1-1-7 所示为交换机的 Web 调试的主界面。

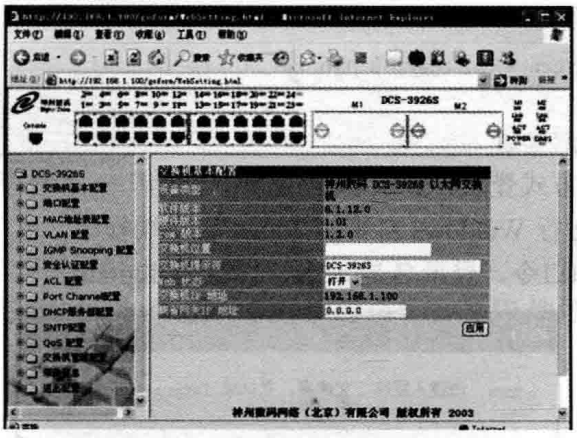


图 1-1-7　Web 调试的主界面

任务二　路由器远程管理

需求分析

小张是公司的网络管理员，有时需要到不同的地方对设备进行调试，但每次都要通过计算机连接到网络设备的 Console 口进行调试，这样管理非常麻烦，小张想使用远程管理的方法来对公司的设备进行管理，这样既方便又高效。

方案设计

小张通过 Console 口管理设备，需要带着笔记本式计算机或专门设置一台台式计算机，并带着 Console 线来调试网络设备，十分麻烦。通过 Telnet 方式，小张可以坐在办公室中调试公司的所有网络设备。

所需设备如图 1-2-1 所示。

（1）DCR 路由器 2 台。

（2）PC 1 台。

（3）Console 线缆、网线各 1 条。

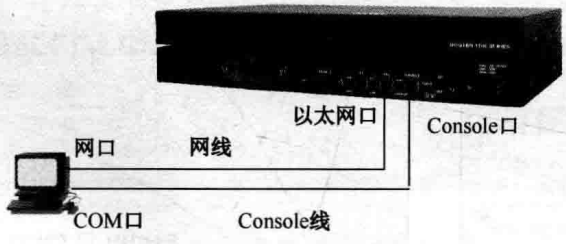


图 1-2-1　路由器远程管理

任务要求：DCR-1702 的 Console 口与 PC 的 COM 口使用 Console 线连接；F0/0 与 PC 的网卡使用交叉双绞线连接，并分别配置 192.168.2.1 和 192.168.2.2 的 C 类 IP 地址。

知识准备

（1）超级终端中的配置是对路由器的操作，此时的 PC 只是输入输出设备。

（2）在使用 Telnet 和 Web 方式管理时，先测试连通性。

任务实现

步骤 1：设置路由器以太网接口 IP 地址并验证连通性。

```
Router>enable                                          //进入特权模式
Router #config                                         //进入全局配置模式
Router-A_config#interface f0/0                         //进入接口模式
Router-A_config_f0/0#ip address 192.168.2.1 255.255.255.0   //设置 IP 地址
Router-A_config_f0/0#no shutdown
Router-A_config_f0/0#^Z
Router-A#show interface f0/0                           //验证
FastEthernet0/0 is up, line protocol is up             //接口和协议都必须 up
address is 00e0.0f18.1a70
  Interface address is 192.168.2.1/24
  MTU 1500 bytes, BW 100000 kbit, DLY 10 usec
  Encapsulation ARPA, loopback not set
Keepalive not set
  ARP type: ARPA, ARP timeout 04:00:00
  60 second input rate 0 bits/sec, 0 packets/sec!
  60 second output rate 6 bits/sec, 0 packets/sec!
  Full-duplex, 100Mb/s, 100BaseTX, 1 Interrupt
    0 packets input, 0 bytes, 200 rx_freebuf
    Received 0 unicasts, 0 lowmark, 0 ri, 0 throttles
    0 input errors, 0 CRC, 0 framing, 0 overrun, 0 long
    1 packets output, 46 bytes, 50 tx_freebd, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 0 deferred, 0 err600
    0 lost carrier, 0 no carrier 0 grace stop 0 bus error
0 output buffer failures, 0 output buffers swapped out
```

步骤 2：设置 PC 的 IP 地址并测试连通性，如图 1-2-2 和图 1-2-3 所示。

图 1-2-2　设置主机 IP 地址

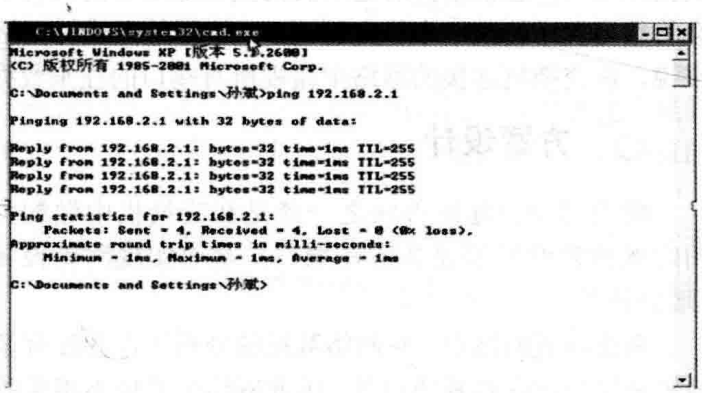


图 1-2-3　测试连通性

步骤 3：设置本地数据库中的用户名，本例使用用户名 dcnu 和密码 dcnu。

```
Router-A_config#username dcnu password dcnu //设置本地用户名和密码
Router-A_config#
```

步骤 4：创建一个新的登录验证方法，名为 login_fortelnet，此方法将使用本地数据库验证。

```
Router-A_config#aaa authentication login login_fortelnet local
//创建 login_fortelnet 验证，采用 local
Router-A_config#
```

步骤 5：进入 Telnet 进程管理配置模式，配置登录用户使用 login_fortelnet 的验证方法进行验证。

```
Router-A_config#line vty 0 4
Router-A_config_line#login authentication login_fortelnet  //在接口下应用
Router-A_config_line#
```

步骤 6：经过配置，Telnet 登录路由器时的过程如下所示。

```
C:\>telnet 192.168.2.1
Connecting to remote host...
Press 'q' or 'Q' to quit connection.
User Access Verification
Username:dcnu
Password:
2004-1-1 04:21:34 User dcnu logged in from 192.168.2.1 on vty 1
                    Welcome to DCR Multi-Protocol 1700 Series Router
Router1700>
```

任务三　交换机端口监听

需求分析

集线器无论接收到什么数据，都会将数据按照广播的方式在各个端口发送出去，这个方式虽然造成了网络带宽的浪费，但网管设备对网络数据的收集和监听是很有效的；交换机在收到数据帧之后，会根据目的地址的类型决定是否需要转发数据，而且如果不是广播数据，则它只会将数据发送给某一个特定的端口，这样的方式对网络效率的提高很有好处，但对于网管设备来说，在交换机连接的网络中监视所有端口的往来数据似乎变得更困难了。

方案设计

解决这个问题的办法之一就是在交换机中做配置，使交换机将某一端口的流量在必要的时候镜像给网管设备所在端口，从而实现网管设备对某一端口的监视。这个过程被称为“端口镜像”。

在交换式网络中，对网络数据的分析工作并没有像人们预想的那样变得更加快捷，由于交换机是进行定向转发的设备，因此网络中其他不相关的端口将无法收到其他端口的数据，如网管的协议分析软件安装在一台接在端口 1 中的机器上，而如果想分析端口 2 与端口 3 设备之间

的数据流量就变得几乎不可能了。

本任务使用 DCS-3926S 系列交换机作为演示设备，其软件版本为 DCS-3926S_6.1.12.0，实际使用中由于软件版本不同，其功能和配置方法有可能存在差异，请关注相应版本的使用说明。

所需设备如图 1-3-1 所示。

（1）DCS 二层交换机 1 台。

（2）PC 3 台。

（3）Console 线 1 条。

（4）直通网线 3 条。

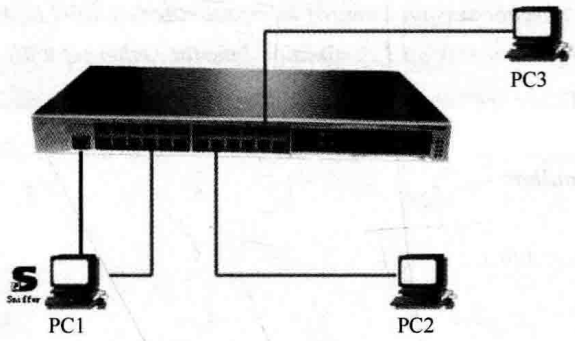


图 1-3-1　交换机端口监听拓扑图

各 PC 网络参数设置见表 1-3-1。

表 1-3-1　各 PC 网络参数设置

设备	IP 地址	子网掩码	端口
PC1	192.168.1.101	255.255.255.0	交换机 e0/0/1
PC2	192.168.1.102	255.255.255.0	交换机 e0/0/2
PC3	192.168.1.103	255.255.255.0	交换机 e0/0/3

知识准备

（1）DCS-3926S 目前只支持一个镜像目的端口，镜像源端口没有使用上的限制，可以有一个，也可以有多个，多个源端口可以处于相同的 VLAN，也可以处于不同的 VLAN。但如果镜像目的端口能镜像到多个镜像源端口的流量，则镜像目的端口必须同时属于这些镜像源端口的所在的 VLAN。

（2）镜像目的端口不能是端口聚合组成员。

（3）镜像目的端口的吞吐量如果小于镜像源端口吞吐量的总和，则目的端口无法完全复制源端口的流量；可减少源端口的个数或复制单向的流量，或者选择吞吐量更大的端口作为目的端口。

端口镜像技术可以将一个源端口的数据流量完全镜像到另一个目的端口进行实时分析。利用端口镜像技术，可以把端口 2 或端口 3 的数据流量完全镜像到端口 1 中进行分析。端口镜像完全不影响镜像端口的工作。

任务实现

步骤 1：交换机全部恢复出厂设置后，配置端口镜像，将端口 2 或者端口 3 的流量镜像到端口 1 中。

```
DCS-3926S(Config)#monitor session 1 source interface ethernet 0/0/2 ?
both                    -- Monitor received and transmitted traffic
rx                      -- Monitor received traffic only
tx                      -- Monitor transmitted traffic only
<CR>
DCS-3926S(Config)#monitor session 1 source interface ethernet 0/0/2 both
DCS-3926S(Config)#monitor session 1 destination interface ethernet 0/0/1
DCS-3926S(Config)#
```

步骤 2：验证配置。

```
DCS-3926S#show monitor
session number : 1
Source ports:    Ethernet0/0/2
RX: No
TX: No
Both: Yes
Destination port: Ethernet0/0/1
------------------------------------------------
DCS-3926S#
```

步骤 3：启动抓包软件，PC2 ping PC3，查看是否可以捕捉到数据包，如图 1-3-2 所示。

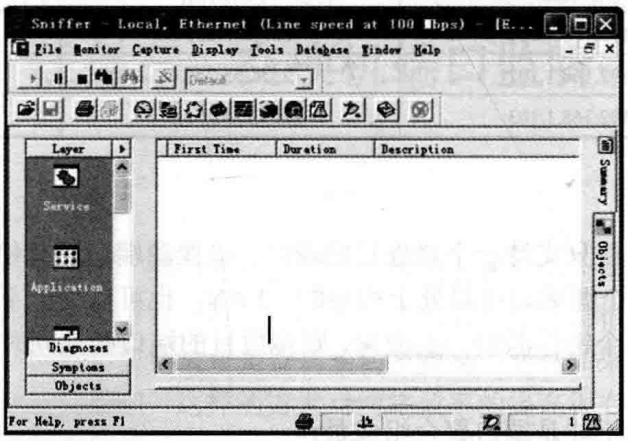


图 1-3-2　抓包软件捕捉数据包

任务四　交换机链路聚合

需求分析

两个实验室分别使用一台交换机提供 20 多个信息点，两个实验室的互连通过一条级联网