天津理工大学**实验报告**

**学院名称: 计算机科学与工程学院**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** |  | **学号** |  | **专业** | |  |
| **班级** |  | **实验项目** | **实验1、2、3、4、5、6、7、8、9、10** | | | |
| **课程名称** | | **网络综合实验** | | **课程代码** | **0682036** | |
| **实验时间** | | **2018年 月 日** | | **实验地点** |  | |
| **批改意见** | | | | **成绩** |  | |
| **教师签字:** | | | | | | |
| **实验目的：**  了解网络的组建，端口扫描，服务器配置，交换机配置，路由器配置和目前网络的先进技术。提高学生理论与实践相结合的能力。  **实验内容：**  **实验1 简单局域网组建**  主要内容：制作网线，用单交换机组建网络，用2台或以上的交换机组建网络，配置IP地址，调通网络。  **实验2 端口扫描**  主要内容：利用端口扫描工具，扫描远程主机端口开放情况**。**  **实验3 Web服务器的配置与管理**  主要内容：配置WEB服务器，发布网站。  **实验4 FTP服务器的配置与管理**  主要内容：利用Windows自带的FTP服务建立FTP服务器，利用Serv-U建立FTP服务器，配置客户端。  **实验5 交换机配置**  主要内容：交换机的访问方法，常用命令，VLAN的划分。  **实验6 路由器基本配置**  主要内容：路由器的访问方法，常用路由命令。静态路由和动态路由的配置。  **实验7 NAT配置**  主要内容：配置NAT，配置端口映射。  **实验8 L2TP VPN配置**  主要内容：利用L2TP的方法配置VPN，以及客户端的配置。  **实验9 协议分析**（按单独的那个指导书进行）  **实验10 路由配置综合实验**  **附加实验 路由器的基本配置（用机柜完成）**  用机柜完成连线，并用超级终端完成路由器的基本配置。 | | | | | | |

**实验过程：**

**实验1 简单局域网组建**

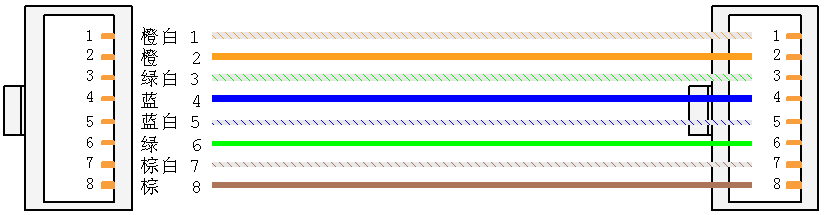
一．实验目的:

主要内容：制作网线，用单交换机组建网络，用 2 台或以上的交换机组建网络，配置 IP 地址，调通网络

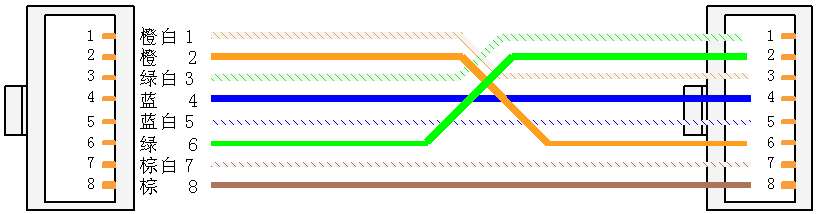
二．实验原理：

双绞线有两种接法：EIA/TIA 568B标准和EIA/TIA 568A标准。   
　　T568A线序   
　　 1 2 3 4 5 6 7 8   
　　绿白 绿 橙白 蓝 蓝白 橙 棕白 棕   
  
　　T568B线序   
　　 1 2 3 4 5 6 7 8   
　　橙白 橙 绿白 蓝 蓝白 绿 棕白 棕

直通线：两头都按T568B线序标准连接。



交叉线：一头按T568A线序连接，一头按T568B线序连接。



本节我们采用直通线的连接方法。

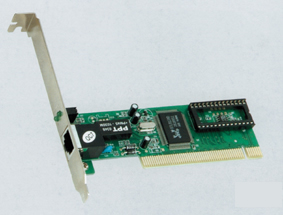
三．实验过程：

1.所需设备

* + 带有RJ-45连接头的UTP电缆



* + 带有RJ-45接口的以太网卡

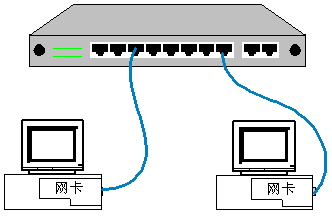


* + 10M/100M集线器或交换机



2.以太网组网步骤

* 制作UTP电缆
* 安装以太网卡
* 将计算机接入网络



3. 设置IP地址

在桌面上右键单击“网上邻居”出现下面的窗口：

//img//

右键单击“本地连接”，在出现的弹出式菜单中点击“属性”，出现下面的窗口

//img//

双击“Internet协议”，出现“Internet属性”窗口，在里面填上IP地址

//img//

4.设置文件夹共享

在要共享的文件夹上右键单击，在出现的弹出式菜单中选择“共享…”选项。

//img//

点击完“共享”选项后出现该文件夹的属性窗口。

//img//

选择“共享该文件夹”单选钮后点击“确定”按钮，该文件夹处于共享状态。如下图所示，在该文件夹上出现一个“手”托着文件夹

//img//

5.使用文件共享

双击桌面上的“网上邻居”，出现“网上邻居”窗口。

//img//

双击“临近的计算机”出现当前工作组窗口。

//img//

双击需要访问的计算机，出现该计算机上的共享资源。

//img//

双击“software”共享文件夹，出现该文件夹下的资源。

//img//

此时可以对该文件夹下的资源进行访问。

6. 映射网络驱动器

//img//

在“资源管理器”中点击菜单栏中的“工具”按钮，出现“映射网络驱动器”窗口，在文件夹文本框中输入共享资源，或从浏览中选择。

//img//

点击“完成”按钮，完成网络驱动器的映射，以后访问网络资源就和访问本地驱动器一样。选择网络驱动器“H”盘出现下面的窗口

//img//

四．实验结果：

通过实验室中制作网线后检验，将水晶头插到网线测试仪的两个端口上，看 指示灯的变化，显示 8 个灯均亮，测试通过。

**实验2 端口扫描**

一．实验目的

1）掌握漏洞的概念及产生原因

2）掌握操作系统体系结构的安全隐患

3）掌握漏洞对系统的影响

4）学习一种漏洞扫描器的方法

二．实验原理

一般来说，基于网络的漏洞扫描工具可以看作为一种漏洞信息收集工具，他根据不同漏洞的特性，构造网络数据包，发给网络中的一个或多个目标机，以判断某个特定的漏洞是否存在。(实际上是进行一次没有危害的攻击！)

三．实验过程：

1. 安装Nmap，与平常软件安装无异。

2. 运行Nmap的GUI界面。如下：

//img//

3. Nmap用法示例：

(1) 进行ping扫描，打印出对扫描做出响应的主机,不做进一步测试(如端口扫描或者操作系统探测)：

nmap -sP 192.168.1.0/24

(2) 仅列出指定网络上的每台主机，不发送任何报文到目标主机：

nmap -sL 192.168.1.0/24

(3) 探测目标主机开放的端口，可以指定一个以逗号分隔的端口列表(如-PS22，23，25，80)：

nmap -PS 192.168.1.234

(4) 使用UDP ping探测主机：

nmap -PU 192.168.1.0/24

(5) 使用频率最高的扫描选项：SYN扫描,又称为半开放扫描，它不打开一个完全的TCP连接，执行得很快：

nmap -sS 192.168.1.0/24

(6) 当SYN扫描不能用时，TCP Connect()扫描就是默认的TCP扫描：

nmap -sT 192.168.1.0/24

(7) UDP扫描用-sU选项,UDP扫描发送空的(没有数据)UDP报头到每个目标端口:

nmap -sU 192.168.1.0/24

(8) 确定目标机支持哪些IP协议 (TCP，ICMP，IGMP等):

nmap -sO 192.168.1.19

(9) 探测目标主机的操作系统：

nmap -O 192.168.1.19

nmap -A 192.168.1.19

四．实验结果：

1. 进行ping扫描，打印出对扫描做出响应的主机,不做进一步测试

//img//

2. 仅列出指定网络上的每台主机，不发送任何报文到目标主机

//img//

3. 探测目标主机开放的端口，可以指定一个以逗号分隔的端口列表(如-PS22，23，25，80)：

//img//

4. 使用UDP ping探测主机：

//img//

5. 使用频率最高的扫描选项：SYN扫描,又称为半开放扫描，它不打开一个完全的TCP连接，执行得很快：

//img//

6. 当SYN扫描不能用时，TCP Connect()扫描就是默认的TCP扫描

//img//

7. UDP扫描用-sU选项,UDP扫描发送空的(没有数据)UDP报头到每个目标端口

//img//

8. 确定目标机支持哪些IP协议 (TCP，ICMP，IGMP等):

//img//

9. 探测目标主机的操作系统：

//img//

**实验3 Web服务器的配置与管理**

实验过程：

遇到的问题及解决的方法：

**实验4 FTP服务器的配置与管理**

实验过程：

遇到的问题及解决的方法：

**实验5 交换机配置**

实验过程：

遇到的问题及解决的方法：

**实验6 路由器基本配置**

实验过程：

遇到的问题及解决的方法：

**实验7 NAT配置**

实验过程：

遇到的问题及解决的方法：

**实验8 L2TP VPN配置**

实验过程：

**实验9 协议分析**（按单独的那个指导书进行）

**实验10 路由配置综合实验**

遇到的问题及解决的方法：

**附加实验 路由器的基本配置（用机柜完成）**

实验过程：

遇到的问题及解决的方法