计算机网络实验报告

警示

1. 实验心得体会如有雷同，雷同各方当次实验心得体会成绩均以 0 分计。
2. 在规定时间内未上交实验报告的，不得以其他方式补交，当次心得体会成绩按 0 分计。
3. 报告文件以 PDF 文件格式提交。

本报告主要描述学生在实验中承担的工作、遇到的困难以及解决的方法、体会与总结等。

院系	计算机学院	班 级	19 级软工 1 班
学号	19335286		访问控制列表实验
学生	郑有为		

一、本人承担的工作

（1）、操作 PC1，搭建 WWW 服务器，收集结果，分析实验现象，写实验报告

二、遇到的困难及解决方法

1、在搭建实验拓扑结构时，跨路由器的机器无法 ping 通。

解决方案： 这是由于 PC 网关配错的缘故，以 PC1 为例，网关应被设置为 192.168.1.1，而不是 192.168.1.0。而以 0 结尾的 IP 地址表示一个网络地址，在实验拓扑图中可以看到 192.168.1.0 的标识，这指的是路由器左边的所有设备构成的子网的网络地址。一般来说，在网络设计方案中，都会将 IP 地址段的第一个，或者是最后一个 IP 作为网关的 IP。但网关的 IP 可以是其他 IP（1——254）。

2、在配置 HTTP 服务器时先后遇到如下问题：

1. Syntax error on line 39 of :

   /Users/Administrator/Desktop/httpd-2.4.48-win64-VS16/Apache24/conf/httpd.conf:

   ServerRoot must be a valid directory

2. 

解决方案： 进入 conf 文件夹配置 httpd.conf 文件，首先是修改路径：

```
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path.  If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used.  If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
Define SRVROOT "C:\Users\Administrator\Desktop\httpd-2.4.48-win64-VS16\Apache24"

ServerRoot "${SRVROOT}"

```

然后增加一行服务器网址 IP 配置：

```
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80
ServerName localhost:80
#
```

3、在路由器配置路由器时间出现语法错误。

解决方案： 月份需用阿拉伯数字输入而不是英文缩写。

4. 在访问 WWW 服务器，抓包的时候，出现如下情况：

50	3.067012	192.168.1.254	10.1.1.100	TCP	54 1419 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
52	3.090803	192.168.1.254	10.1.1.100	HTTP	421 GET /favicon.ico HTTP/1.1
53	3.091972	10.1.1.100	192.168.1.254	HTTP	470 HTTP/1.1 404 Not Found (text/html)
56	3.141984	192.168.1.254	10.1.1.100	TCP	54 1418 → 80 [ACK] Seq=368 Ack=413 Win=525056 Len=0
135	8.092540	10.1.1.100	192.168.1.254	TCP	64 80 → 1418 [FIN, ACK] Seq=413 Ack=368 Win=525568 Len=0

908	475.214162	192.168.1.2	10.1.1.100	TCP	54 22145 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
909	475.214797	192.168.1.2	10.1.1.100	HTTP	508 GET / HTTP/1.1
910	475.215105	192.168.1.2	10.1.1.100	TCP	66 22146 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
911	475.215295	10.1.1.100	192.168.1.2	TCP	66 80 → 22146 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
912	475.215349	192.168.1.2	10.1.1.100	TCP	54 22146 → 80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
913	475.215529	10.1.1.100	192.168.1.2	HTTP	459 HTTP/1.1 200 OK (text/html)
915	475.265785	192.168.1.2	10.1.1.100	TCP	54 22145 → 80 [ACK] Seq=455 Ack=406 Win=525056 Len=0
929	480.216470	10.1.1.100	192.168.1.2	TCP	60 80 → 22145 [FIN, ACK] Seq=406 Ack=455 Win=525568 Len=0

我们可以看到两个 HTTP 报文，第一个是 Manager 向 WWW 服务器发出请求（GET /favicon.ico HTTP/1.1），第二个 WWW 服务器向 Manager 发送（404 Not Found（text/html））,在实验报告整合时我们才发现这个问题，但我在 PC1 上抓包的时候 WWW 服务返回的包的内容是（HTTP/1.1 200 OK），但实际上两台 PC 都成功访问了 WWW 服务器网站。

仔细分析上下文的数据包，我们发现 PC1 接收时，GET 的是 GET HTTP/1.1，而不是 GET /favicon.ico HTTP/1.1，前者比后者删了一个 logo 的请求，显然我们临时搭建的网站没有设置图标，这应该是使得服务器返回 404 的原因，至于为什么 PC1 的请求不包含/favicon.ico，可能是多次进入网站，浏览器对数据报文发送的改进。

三、体会与总结

在本次实验中，我们学习了 FTP 服务器和 WWW 服务器的搭建方法，掌握了标准访问列表、扩展访

问列表的规则以及配置方法。

1.标准访问列表规则及配置。

标准 ACL 原理：当一个数据包进入路由器的某一个接口时，路由器首先检查该数据包是否可路由或可桥接。然后路由器检查是否在入站接口上应用了 ACL。若有 ACL，就将该数据包与 ACL 中的条件语句相比较。若数据包被允许通过，就继续检查路由器选择表条目以决定转发到的目的接口。ACL 不过滤由路由器本身发出的数据包，只过滤经过路由器的数据包。然后路由器检查目的接口是否应用了 ACL。若无，数据包就被直接送到目的接口输出。对于非 IP 包，ACL 无法对其尽行控制。

配置：配置 ACL 的关键字包括 access-list-number（访问控制列表号） deny（拒绝） permit（允许） source（IP 源地址） source-wildcard（通配符+掩码）等。配置两步骤：

1. 使用 access-list 命令创建访问控制列表；
2. 使用 ip access-group 命令将列表应用到某端口上。

2.扩展访问列表规则及配置。

扩展访问列表规则在标准 ACL 的基础上增加了目的地址的判定、匹配协议的判定、端口判定、时间域的限制等。

配置：扩展 ACL 的关键字还有 protocol（协议类型指定） destination（目的 IP） destination-wildcard（目的通配符+掩码） operator（源或目的端口比较操作符） operand（用于比较的端口值）规则：access-list *access-list-number* {deny | permit} *protocol* source [*source-wildcard* destination *destination-wildcard*] [operator *operand*] [established]（还没有加入时间限定规则，而我们本次实验做的事基于时间的访问控制列表，有按时间控制访问的功能）时间段定义格式如下：

```
time-range  时间段名称(名字的长度为 1～32 个字符,不能包含空格)
absolute {start time date [end time date]| end time date }    !设置绝对时间区间(可选)
periodic day-of-the-week hh:mm to [day-of-the-week] hh:mm     !设置周期时间(可选)
periodic {weekdays | weekend |daily}hh:mm to hh:mm            !设置周期时间(可选)
```

3.标准访问列表和扩展访问列表的区别。

后者的功能更多，更常用：标准 ACL 只会根据源 IP 允许或拒绝数据包，而扩展 ACL 能够根据源 IP、目的 IP、指定协议、端口和标志允许或拒绝数据包，后者能更加精确地实现流量控制。

访问控制列表号不同：前者从 1-99，后者从 100-199。