



兰州大学

《计算机网络》实验报告（一）

学院： 信息科学与工程学院

班级： 2018 级计算机科学与技术（数据科学方向）4 班

小组成员： 胡悦、陈宇铭、冯博、钟奕

任课教师： 王忠

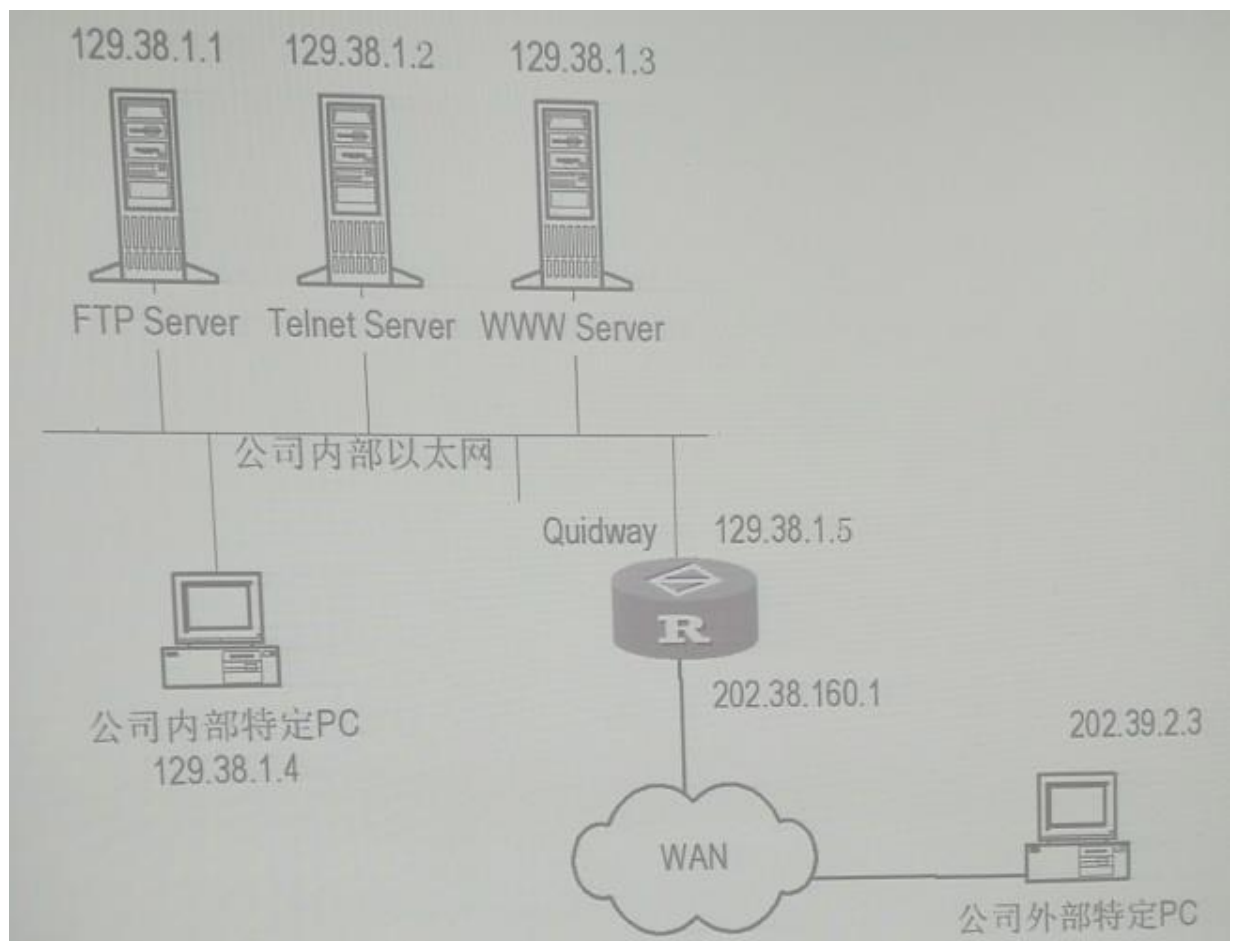
实验小组： 8

实验日期： 2020-11-30

目录

一、 实验任务.....	3
二、 实验要求	3
三、 实验环境.....	4
四、 实验步骤.....	4
1. 在 eNSP 中制作网络拓扑图.....	4
2. IP 地址分配方案	4
2.1 路由器端口地址分配方案.....	4
2.2 主机地址分配方案.....	4
2.3 服务器地址分配方案	5
3. 配置 IP 地址.....	5
3.1 路由器.....	5
3.2 主机	6
3.3 服务器.....	7
4. 配置 RIP 协议.....	10
4.1 公司内部路由器	10
4.2 公司外部路由器	10
5. 测试连通性.....	10
5.1 查看路由表.....	10
5.2 使用 ping、tracert 命令.....	11
5.3 测试服务器连通性.....	12
6. 配置访问规则	15
6.1 分析	15
6.2 对于公司外部，只允许外部特定 PC（202.39.2.3）访问公司内部的三个服务 器。16	
6.3 对于公司内部，只有内部特定 PC（129.38.1.4）能访问外部特定 PC （202.39.2.3）。	错误!未定义书签。

一、 实验任务



二、 实验要求

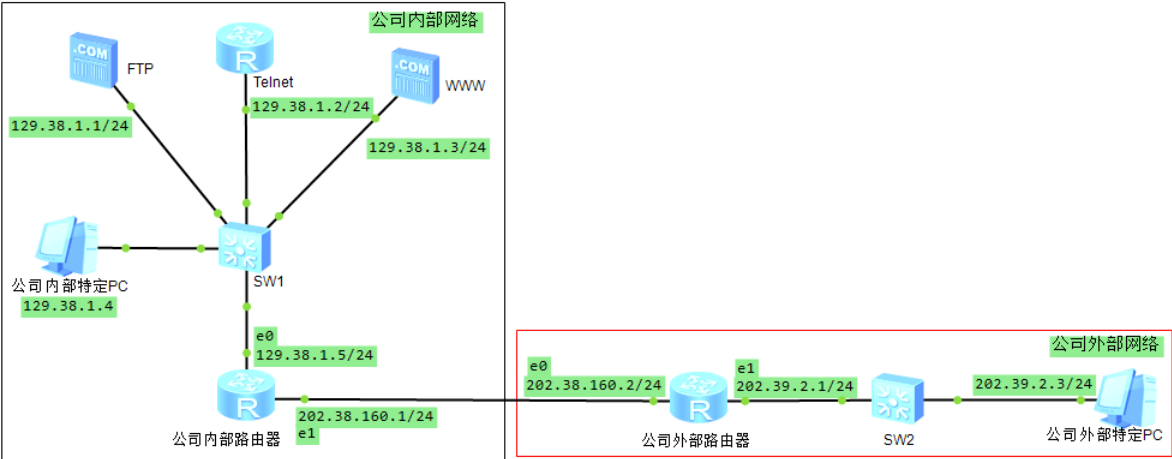
1. 在 eNSP 中设计满足实验任务的网络拓扑结构。
2. 为网络中的所有结点分配对应的 IP 地址。
3. 配置合适的路由协议，使得网络中所有结点都能互相连通。
4. 配置以下访问规则：
 - 4.1 对于公司外部，只允许外部特定 PC（202.39.2.3）访问公司内部三个服务器。
 - 4.2 对于公司内部，只有内部特定 PC（129.38.1.4）能访问外部特定 PC（202.39.2.3）。

三、 实验环境

软件类别	版本号
eNSP	1. 3. 00 V100R003C00
VirtualBox	5. 2. 22 r126460 (Qt5. 6. 2)
Wireshark	3. 0. 0
WinPcap	4. 1. 3

四、 实验步骤

1. 在 eNSP 中制作网络拓扑图



2. IP 地址分配方案

2.1 路由器端口地址分配方案

路由器	e0	e1
公司内部路由器	129.38.1.5/24	202.38.160.1/24
公司外部路由器	202.38.160.2/24	202.39.2.1/24

2.2 主机地址分配方案

主机	IP	网关
公司内部特定 PC	129.38.1.4/24	129.38.1.5/24
公司外部特定 PC	202.39.2.3/24	202.39.2.1/24

2.3 服务器地址分配方案

服务器	IP	网关
FTP Server	129.38.1.1/24	129.38.1.5/24
Telnet Server	129.38.1.2/24	129.38.1.5/24
WWW Server	129.38.1.3/24	129.38.1.5/24

3. 配置 IP 地址

3.1 路由器

3.1.1 公司内部路由器

在工作区双击公司内部路由器图标，在命令行界面配置公司内部路由器的 e0 端口为 129.38.1.5/24，e1 端口为 202.38.160.1/24

代码如下：

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname gsnb
[gsnb]int g0/0/0
[gsnb-GigabitEthernet0/0/0]ip ad 192.38.1.5 24
[gsnb-GigabitEthernet0/0/0]int g0/0/1
[gsnb-GigabitEthernet0/0/1]ip ad 202.38.160.1 24
[gsnb-GigabitEthernet0/0/1]q
```

3.1.2 公司外部路由器

在工作区双击公司外部路由器图标，在命令行界面配置公司外部路由器的 e0 端口为 202.38.160.2/24，e1 端口为 202.39.2.1/24

代码如下：

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname gswb
[gswb]int g0/0/0
[gswb-GigabitEthernet0/0/0]ip ad 202.38.160.2 24
[gswb-GigabitEthernet0/0/0]int g0/0/1
[gswb-GigabitEthernet0/0/1]ip ad 202.39.2.1 24
[gswb-GigabitEthernet0/0/1]q
```

公司外部特定PC

X

基础配置

命令行

组播

UDP发包工具

串口

主机名:

MAC 地址:

54-89-98-BC-63-8F

IPv4 配置

☒ 静态

☐ DHCP

☐ 自动获取 DNS 服务器地址

IP 地址:

202 . 39 . 2 . 3

DNS1:

0 . 0 . 0 . 0

子网掩码:

255 . 255 . 255 . 0

DNS2:

0 . 0 . 0 . 0

网关:

202 . 39 . 2 . 1

IPv6 配置

☒ 静态

☐ DHCPv6

IPv6 地址:

::

前缀长度:

128

IPv6 网关:

::

应用

3.3 服务器

3.3.1 FTP Server

在工作区双击 FTP 服务器图标，在“配置”界面，IP 地址配置为 129.38.1.1，子网掩码配置为 255.255.255.0，网关配置为 129.38.1.5

The screenshot shows the 'FTP' configuration window with the '基础配置' (Basic Configuration) tab selected. The 'Mac地址' (MAC Address) is set to 54-89-98-C3-4F-8A. The 'IPV4配置' (IPv4 Configuration) section shows the '本机地址' (Local Address) as 129.38.1.1, '子网掩码' (Subnet Mask) as 255.255.255.0, and '网关' (Gateway) as 129.38.1.5. The '域名服务器' (DNS Server) is set to 0.0.0.0. The 'PING测试' (Ping Test) section shows the '目的IPV4' (Destination IPv4) as 0.0.0.0 and the '次数' (Count) as 0. The '本机状态' (Local Status) is '设备启动' (Device Started) and the 'ping 成功: 0 失败: 0' (Ping Success: 0 Failure: 0). A '保存' (Save) button is at the bottom right.

The screenshot shows the 'FTP' configuration window with the '基础配置' (Basic Configuration) tab selected. The '服务' (Service) section shows the '监听端口号' (Listening Port Number) as 21, with '启动' (Start) and '停止' (Stop) buttons. The '配置' (Configuration) section shows the '文件根目录' (File Root Directory) as C:\Users\FishAndWasabi\Desktop. A list of files and folders is shown below, including Cherry助手.lnk, CodeBlocks.lnk, C语言.docx, desktop.ini, Start10.url, Wallpaper Engine: 壁纸引擎.url, Windows, ~\$实验一.docx, ~\$新建 Microsoft Excel 工作表.xlsx, ~WRL3898.tmp, 实验一.docx, 新建 Microsoft Excel 工作表.xlsx, 新建 Microsoft Word 文档 (2).docx, 计算机网络.docx, and 迅雷.lnk.

3.3.2 Telnet Server

① 配置 IP

在工作区双击路由器 Telnet 图标，在命令行界面配置路由器 Telnet 的 e0 端口为

129.38.1.2/24

代码如下：

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname telnet
[telnet]int g0/0/0
[telnet-GigabitEthernet0/0/0]ip ad 129.38.1.2 24
[telnet-GigabitEthernet0/0/0]q
```

② 配置 Telnet

将路由器 Telnet 配置为 Telnet 服务器，权限等级为 Level 1。

代码如下：

```
<telnet>sys
Enter system view, return user view with Ctrl+Z.
[telnet]telnet server enable
Error: TELNET server has been enabled
[telnet]user-interface vty 0 4
[telnet-ui-vty0-4]authentication-mode password
Please configure the login password (maximum length 16)
:123456
[telnet-ui-vty0-4]user privilege level 1
[telnet-ui-vty0-4]q
```

③ 验证

在公司内部路由器中登录

代码如下：

```
<gsnb>telnet 129.38.1.2
Press CTRL_] to quit telnet mode
Trying 129.38.1.2 ...
Connected to 129.38.1.2 ...
Login authentication
Password: 123456
<gsnb>
```


3.3.3 WWW Server

在工作区双击 WWW 服务器图标，在“配置”界面，IP 地址配置为 129.38.1.3，子网掩码配置为 255.255.255.0，网关配置为 129.38.1.5

The screenshot shows the 'WWW' configuration window with the '基础配置' (Basic Configuration) tab selected. The 'Mac地址' (MAC Address) is set to 54-89-98-36-2B-85. The 'IPV4 配置' (IPv4 Configuration) section shows the '本机地址' (Local Address) as 129.38.1.3, '子网掩码' (Subnet Mask) as 255.255.255.0, '网关' (Gateway) as 129.38.1.5, and '域名服务器' (DNS Server) as 0.0.0.0. The 'PING测试' (Ping Test) section shows the '目的IPV4' (Destination IPv4) as 0.0.0.0 and '次数' (Count) as 1. The '本机状态' (Local Status) is '设备启动' (Device Started) and 'ping 成功: 0 失败: 0' (Ping Success: 0 Failure: 0). A '保存' (Save) button is at the bottom right.

The screenshot shows the 'WWW' configuration window with the '服务器信息' (Server Information) tab selected. The '服务' (Service) section shows the '端口号' (Port Number) as 80, with '启动' (Start) and '停止' (Stop) buttons. The '配置' (Configuration) section shows the '文件根目录' (File Root Directory) as C:\Users\FishAndWasabi\Desktop. A list of files and folders is shown below, including Cherry助手.lnk, CodeBlocks.lnk, C语言.docx, desktop.ini, Start10.url, Wallpaper Engine: 壁纸引擎.url, Windows, ~\$实验一.docx, ~\$新建 Microsoft Excel 工作表.xlsx, ~\$WRL3898.tmp, 实验一.docx, 新建 Microsoft Excel 工作表.xlsx, 新建 Microsoft Word 文档 (2).docx, 计算机网络.docx, and 迅雷.lnk.

4. 配置 RIP 协议

4.1 公司内部路由器

在工作区双击公司内部路由器图标, 在命令行界面配置 RIP 协议

代码如下:

```
[gsnb]rip 1
[gsnb-rip-1]version 2
[gsnb-rip-1]network 129.38.0.0
[gsnb-rip-1]network 202.38.160.0
[gsnb-rip-1]q
```

4.2 公司外部路由器

在工作区双击公司外部路由器图标, 在命令行界面配置 RIP 协议

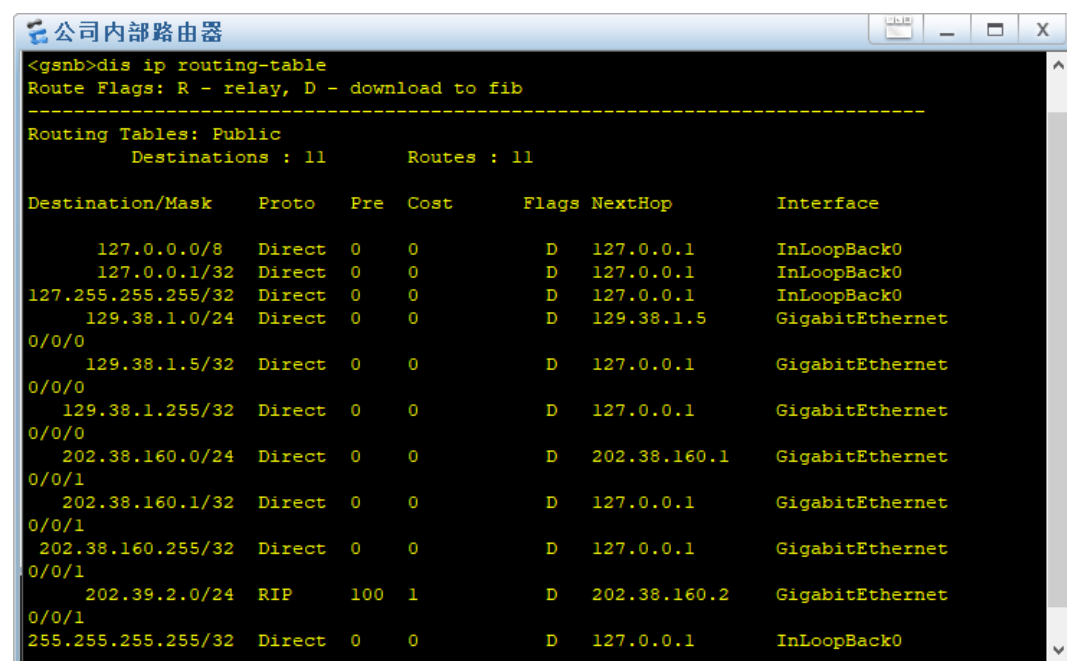
代码如下:

```
[gswb]rip 1
[gswb-rip-1]version 2
[gswb-rip-1]network 202.38.160.0
[gswb-rip-1]network 202.39.2.0
[gswb-rip-1]q
```

5. 测试连通性

5.1 查看路由表

5.1.1 公司内部路由器



```
公司内部路由器
<gsnb>dis ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 11          Routes : 11

Destination/Mask    Proto    Pre  Cost           Flags NextHop         Interface
-----
      127.0.0.0/8     Direct   0     0             D    127.0.0.1         InLoopBack0
      127.0.0.1/32     Direct   0     0             D    127.0.0.1         InLoopBack0
127.255.255.255/32   Direct   0     0             D    127.0.0.1         InLoopBack0
      129.38.1.0/24   Direct   0     0             D    129.38.1.5         GigabitEthernet
0/0/0
      129.38.1.5/32    Direct   0     0             D    127.0.0.1         GigabitEthernet
0/0/0
      129.38.1.255/32  Direct   0     0             D    127.0.0.1         GigabitEthernet
0/0/0
      202.38.160.0/24  Direct   0     0             D    202.38.160.1       GigabitEthernet
0/0/1
      202.38.160.1/32  Direct   0     0             D    127.0.0.1         GigabitEthernet
0/0/1
      202.38.160.255/32 Direct   0     0             D    127.0.0.1         GigabitEthernet
0/0/1
      202.39.2.0/24    RIP      100    1             D    202.38.160.2       GigabitEthernet
0/0/1
255.255.255.255/32   Direct   0     0             D    127.0.0.1         InLoopBack0
```

5.1.2 公司外部路由器

```
公司外部路由器
[gswb]dis ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 11          Routes : 11

Destination/Mask    Proto   Pre  Cost   Flags NextHop         Interface
-----
127.0.0.0/8         Direct  0    0       D  127.0.0.1         InLoopBack0
127.0.0.1/32        Direct  0    0       D  127.0.0.1         InLoopBack0
127.255.255.255/32   Direct  0    0       D  127.0.0.1         InLoopBack0
129.38.1.0/24       RIP     100  1       D  202.38.160.1      GigabitEthernet
0/0/0
202.38.160.0/24     Direct  0    0       D  202.38.160.2      GigabitEthernet
0/0/0
202.38.160.2/32     Direct  0    0       D  127.0.0.1         GigabitEthernet
0/0/0
202.38.160.255/32   Direct  0    0       D  127.0.0.1         GigabitEthernet
0/0/0
202.39.2.0/24       Direct  0    0       D  202.39.2.1        GigabitEthernet
0/0/1
202.39.2.1/32       Direct  0    0       D  127.0.0.1         GigabitEthernet
0/0/1
202.39.2.255/32     Direct  0    0       D  127.0.0.1         GigabitEthernet
0/0/1
255.255.255.255/32   Direct  0    0       D  127.0.0.1         InLoopBack0
```

5.2 使用 ping、tracert 命令

5.2.1 ping

公司内部特定 PC -> 公司外部特定 PC

```
PC>ping 202.39.2.3
Ping 202.39.2.3: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 202.39.2.3: bytes=32 seq=2 ttl=126 time=78 ms
From 202.39.2.3: bytes=32 seq=3 ttl=126 time=62 ms
From 202.39.2.3: bytes=32 seq=4 ttl=126 time=79 ms
From 202.39.2.3: bytes=32 seq=5 ttl=126 time=78 ms

--- 202.39.2.3 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss

    round-trip min/avg/max = 0/74/79 ms
```

公司外部特定 PC -> 公司内部特定 PC

```
PC>ping 129.38.1.4

Ping 129.38.1.4: 32 data bytes, Press Ctrl_C to break
From 129.38.1.4: bytes=32 seq=1 ttl=126 time=78 ms
From 129.38.1.4: bytes=32 seq=2 ttl=126 time=78 ms
From 129.38.1.4: bytes=32 seq=3 ttl=126 time=78 ms
From 129.38.1.4: bytes=32 seq=4 ttl=126 time=63 ms
From 129.38.1.4: bytes=32 seq=5 ttl=126 time=78 ms

--- 129.38.1.4 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 63/75/78 ms
```

5.2.2 tracert

公司内部特定 PC -> 公司外部特定 PC

```
PC>tracert 202.39.2.3

tracert to 202.39.2.3, 8 hops max
(ICMP), press Ctrl+C to stop
 1  129.38.1.5    46 ms  32 ms  47 ms
 2  202.38.160.2  46 ms  32 ms  47 ms
 3  202.39.2.3   78 ms  78 ms  94 ms
```

公司外部特定 PC -> 公司内部特定 PC

```
PC>tracert 129.38.1.4

tracert to 129.38.1.4, 8 hops max
(ICMP), press Ctrl+C to stop
 1  202.39.2.1    32 ms  46 ms  47 ms
 2  202.38.160.1  32 ms  46 ms  47 ms
 3  129.38.1.4   78 ms  79 ms  78 ms
```

5.3 测试服务器连通性

为了方便进行测试服务器,将公司外部特定 PC 换成客户端公司外部特定 Client。
在工作区双击 Client 客户端图标,在“配置”界面,IP 地址配置为 202.39.2.3,
子网掩码配置为 255.255.255.0,网关配置为 202.39.2.1

5.3.1 FTP Server

Client2

基础配置 客户端信息 日志信息

Mac地址: 54-89-98-33-1D-EE (格式:00-01-02-03-04-05)

IPv4配置

本机地址: 202 . 39 . 2 . 3 子网掩码: 255 . 255 . 255 . 0

网关: 202 . 39 . 2 . 1 域名服务器: 0 . 0 . 0 . 0

PING测试

目的IPv4: 129 . 38 . 1 . 4 次数: 3 发送

本机状态: 设备启动 ping 成功: 3 失败: 0

保存

Client2

基础配置 客户端信息 日志信息

FtpClient

HttpClient

服务器地址: 129 . 38 . 1 . 1 用户名: 1

端口号: 21 密码: 1

登录 登出

提示

文件下载成功。

确定

文件传输格式 类别

文件名称	大小(B)
Program Files (x86)	
uninstall.log	1817
Users	
新建 Microsoft Word...	0
计算机网络.docx	0
迅雷.lnk	1161

只显示小于1M的文件

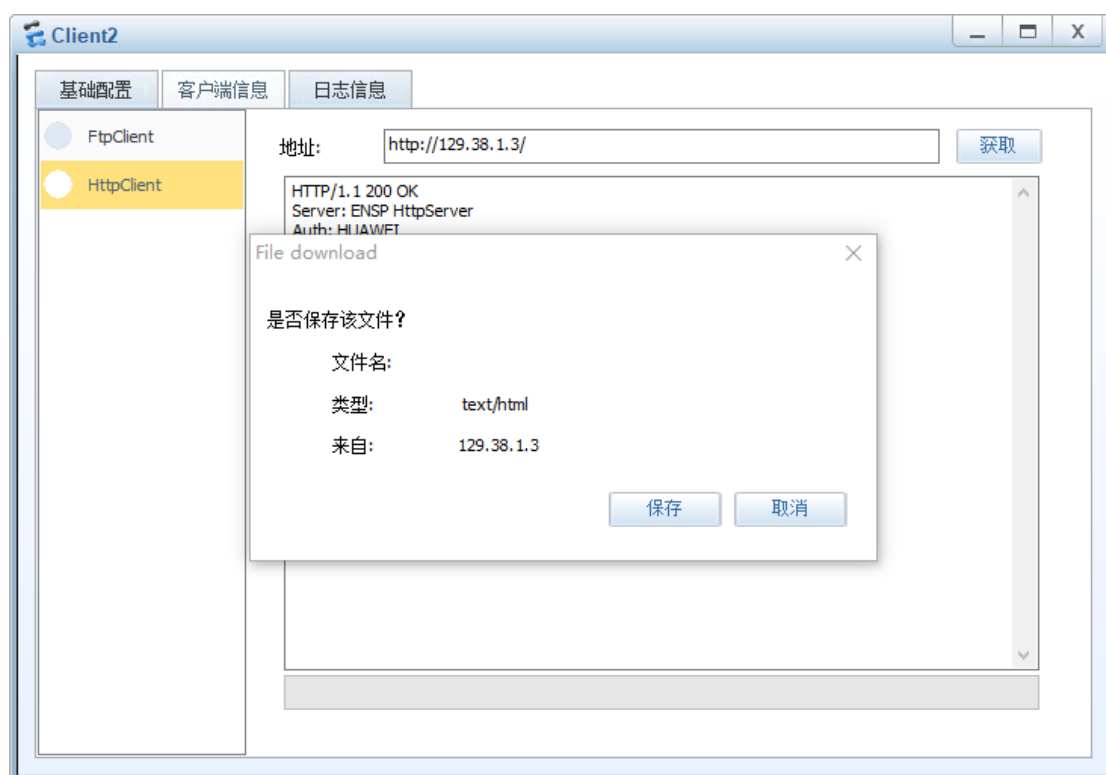
5.3.2 Telnet Server

在公司外部路由器中登录

代码如下：

```
<gswb>telnet 129.38.1.2
Press CTRL_] to quit telnet mode
Trying 129.38.1.2 ...
Connected to 129.38.1.2 ...
Login authentication
Password: 123456
<gswb>
```

5.3.3 WWW Server



6. 配置访问规则

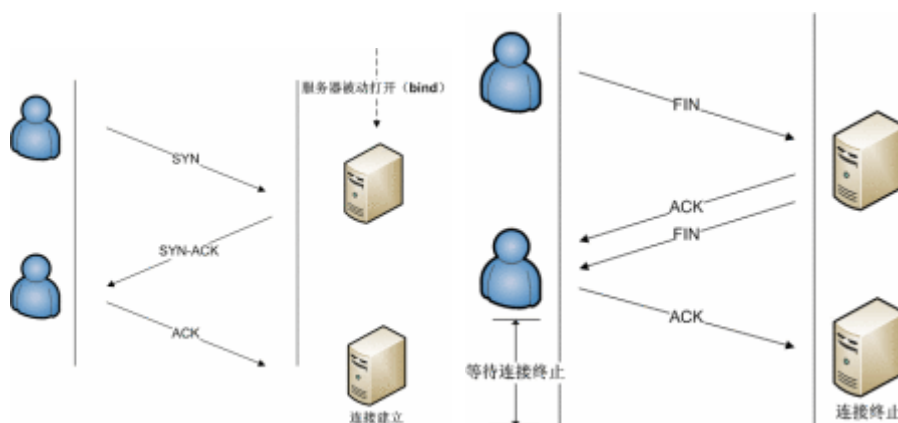
为了方便进行测试服务器，在公司外部网络中添加客户端 Client2。在工作区双击 Client2 客户端图标，在“配置”界面，IP 地址配置为 202.39.2.2，子网掩码配置为 255.255.255.0，网关配置为 202.39.2.1

6.1 分析

根据实验要求，可得该实验存在单向 ACL 的情况，即公司内部仅有公司内部特定 PC 可以访问公司外部网络，公司内部的三台服务器无法访问公司外部网络，即不能访问公司外部特定 PC，而公司外部特定 PC 可以访问公司内部的三台服务器，即公司内部的三台服务器无法给公司外部特定 PC 的请求以相应。因此，若简单地设计 ACL 规则，可能会导致公司外部特定 PC 可以访问公司内部的三台服务器却无法得到回应的问题。查询网上资料得，目前主流方法是通过自反 ACL 进行控制（只有 S7700 系列, 9700 系列, 12700 系列的交换机支持自反 ACL 特性，路由器不支持，原理是加入计时器限时允许返回的报文传输以实现单向网络访问控制）。经查询，目前 eNSP 不支持该功能。

故我们尝试通过控制数据传输过程中的具体标志实现实验目标。

① 对于公司外部，只允许外部特定 PC (202.39.2.3) 访问公司内部的三个服务器。三台服务器分别为 FTP Server、Telnet Server 及 WWW Server。若外部主机要对服务器实现访问（此处不讨论 ping 的问题），则其均需要使用 TCP 传输协议进行三次握手，进而建立连接。以下为建立连接和断开连接的过程：



因此可以通过规定 TCP 协议报文头中的标志位 (FLAG) 的进出规则来实现对服务器的服务访问进行限制。我们的策略是在公司内部网络的出口（即公司内部路由器 e0 端口的 INBOUND 方向）实行白名单机制，允许报文头为 ACK（建立连接）和报文头为 FIN（断开

连接)且源 IP 和目的 IP 符合要求的 TCP 协议数据报文通行, 以此实现实验目的。

ack	指定TCP报文中SYN Flag的类型为ack(010000)。
fin	指定TCP报文中SYN Flag的类型为fin(000001)。
psh	指定TCP报文中SYN Flag的类型为psh(001000)。
rst	指定TCP报文中SYN Flag的类型为rst(000100)。
syn	指定TCP报文中SYN Flag的类型为syn(000010)。
urg	指定TCP报文中SYN Flag的类型为urg(100000)。

来自 eNSP 命令参考

② 对于公司内部, 只有内部特定 PC (129.38.1.4) 能访问外部特定 PC (202.39.2.3)。

在该实验要求中, 我们认为访问为 ping, 即能够访问为 ping 通。根据资料, ping 使用 ICMP (Internet 控制报文协议) 给目标 IP 地址发送一个数据包并接收返回的同样大小的数据包, 因此可以通过限制 icmp 协议的去包或回包限制报文的传输。我们的策略是在公司内部网络的入口 (即公司内部路由器 e1 端口的 INBOUND 方向), 实行白名单机制, 允许报文类型为 Echo-reply (回文) 且源 IP 和目的 IP 符合要求的 ICMP 协议数据报文通行, 以此实现实验目的。

icmp-name	icmp-type	icmp-code
Echo	8	0
Echo-reply	0	0

来自 eNSP 命令参考

6.2 配置规则

6.2.1 公司内部路由器 e0 端口规则

代码如下:

```
<gsnb>sys
Enter system view, return user view with Ctrl+Z.
[gsnb]acl name test1 advanced
[gsnb-acl-adv-test1]rule permit tcp source 129.38.1.0 0.0.0.3
destination 202.39.2.3 0 tcp-flag ack
[gsnb-acl-adv-test1] rule permit tcp source 129.38.1.0 0.0.0.3
destination 202.39.2.3 0 tcp-flag fin
[gsnb-acl-adv-test1] rule permit ip source 129.38.1.4 0
destination 202.39.2.3 0
[gsnb-acl-adv-test1] rule deny ip
```


6.2.1 公司内部路由器 e1 端口规则

代码如下：

```
<gsnb>sys
Enter system view, return user view with Ctrl+Z.
[gsnb]acl name test2 advanced
[gsnb-acl-adv-test2] rule permit icmp source 202.39.2.3 0
destination 129.38.1.4 0 icmp-type echo-reply
[gsnb-acl-adv-test2] rule permit ip source 202.39.2.3 0
destination 129.38.1.0 0.0.0.3
[gsnb-acl-adv-test2] rule deny ip
```

6.3 绑定端口

6.3.1 公司内部路由器 e0 端口

代码如下：

```
[gsnb-acl-adv-test1] int g0/0/0
[gsnb-GigabitEthernet0/0/0] traffic-filter inbound acl name test1
```

6.3.2 公司内部路由器 e1 端口

代码如下：

```
[gsnb-acl-adv-test2] int g0/0/1
[gsnb-GigabitEthernet0/0/1] traffic-filter inbound acl name test2
```

6.4 检验

为了方便进行测试服务器

- ① 将公司外部特定 PC 换成客户端公司外部特定 Client。在工作区双击 Client 客户端图标，在“配置”界面，IP 地址配置为 202.39.2.3，子网掩码配置为 255.255.255.0，网关配置为 202.39.2.1。
- ② 将公司内部特定 PC 换成客户端公司内部特定 Client。在工作区双击 Client 客户端图标，在“配置”界面，IP 地址配置为 129.38.1.4，子网掩码配置为 255.255.255.0，网关配置为 129.38.1.5。
- ③ 在公司外部网络中添加 FTP 服务器。在工作区双击 FTP 服务器图标，在“配置”界面，IP 地址配置为 202.39.2.2，子网掩码配置为 255.255.255.0，网关配置为 202.39.2.1。
- ④ 在公司外部网络中添加“外部-PC2”客户端。在工作区双击“外部-PC2”客户端图标，在“配置”界面，IP 地址配置为 202.39.2.4，子网掩码配置为 255.255.255.0，网关配置为 202.39.2.1。

⑤ 在公司内部网络中添加“内部-PC2”客户端。在工作区双击“内部-PC2”客户端图标，在“配置”界面，IP 地址配置为 129.38.1.6，子网掩码配置为 255.255.255.0，网关配置为 129.38.1.5。

6.4.1 公司内部特定 PC

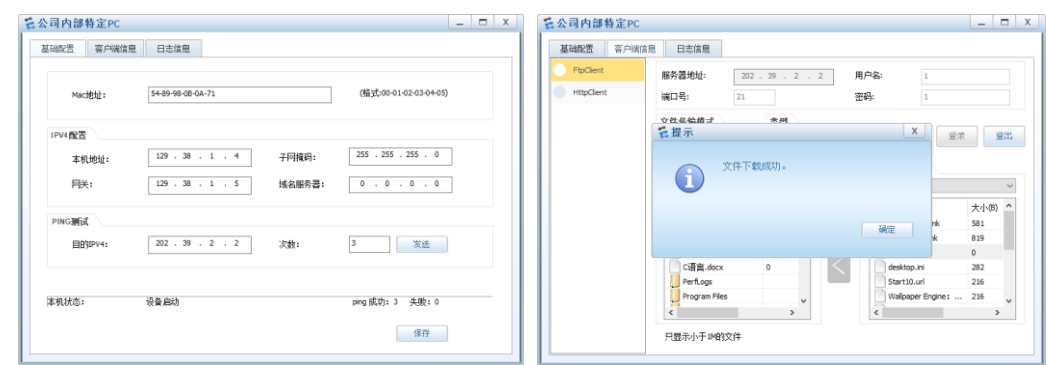
① 在访问规则添加前

访问公司外部特定 PC

```
PC>tracert 202.39.2.3

tracert to 202.39.2.3, 8 hops max
(ICMP), press Ctrl+C to stop
 1  129.38.1.5    16 ms  46 ms  47 ms
 2  202.38.160.2  32 ms  46 ms  47 ms
 3  202.39.2.3   32 ms  46 ms  47 ms
```

访问公司外部网络的 FTP 服务器



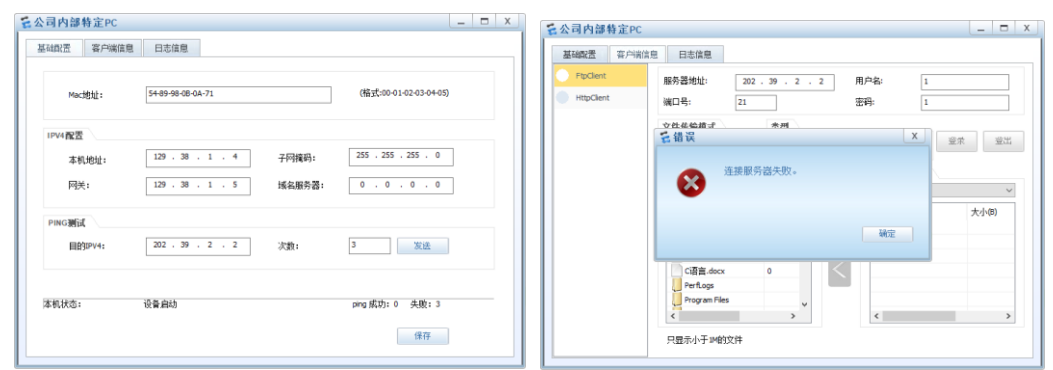
② 在访问规则添加后

访问公司外部特定 PC

```
PC>tracert 202.39.2.3

tracert to 202.39.2.3, 8 hops max
(ICMP), press Ctrl+C to stop
 1  129.38.1.5    32 ms  46 ms  47 ms
 2      * * *
 3  202.39.2.3   32 ms  62 ms  63 ms
```

访问公司外部网络的 FTP 服务器



6.4.2 公司内部-PC2

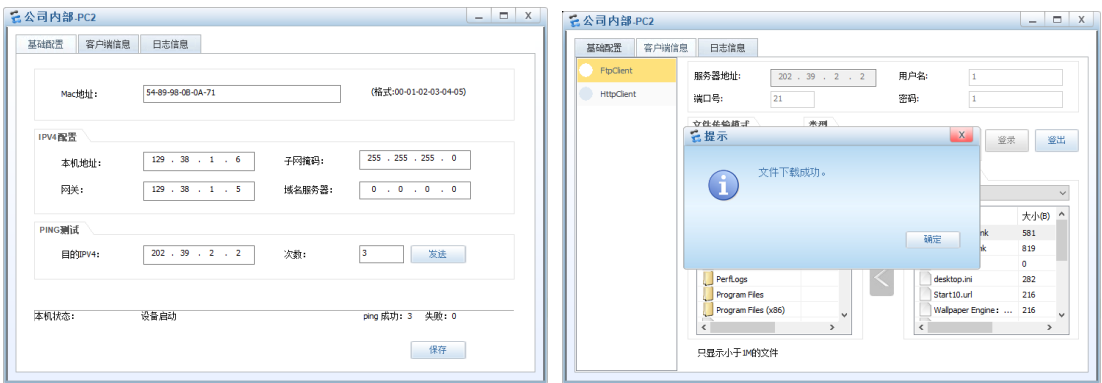
① 在访问规则添加前

访问公司外部特定 PC

```
PC>tracert 202.39.2.3

tracert to 202.39.2.3, 8 hops max
(ICMP), press Ctrl+C to stop
 1  129.38.1.5    31 ms  47 ms  47 ms
 2  202.38.160.2  31 ms  47 ms  47 ms
 3  202.39.2.3   62 ms  63 ms  62 ms
```

访问公司外部网络的 FTP 服务器



② 在访问规则添加后

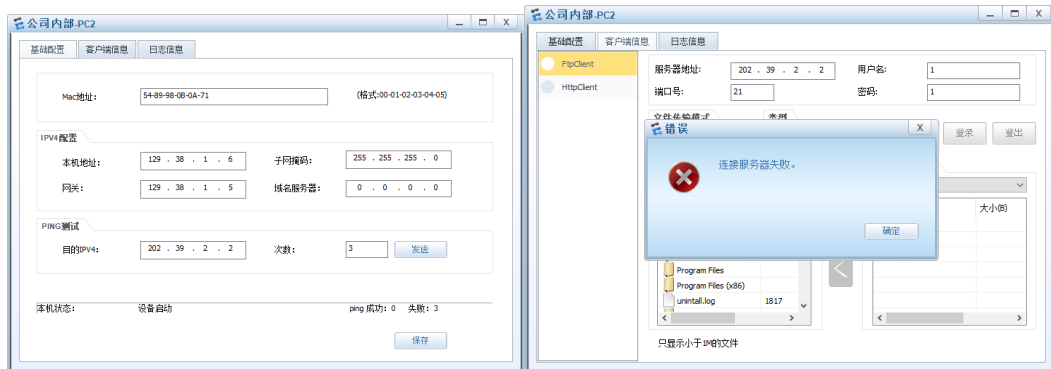
访问公司外部特定 PC

```
PC>tracert 202.39.2.3

tracert to 202.39.2.3, 8 hops max
(ICMP), press Ctrl+C to stop
 1  * * *
 2  * * *
 3  * * *
```

4	*	*	*
5	*	*	*
6	*	*	*
7	*	*	*
8	*	*	*

访问公司外部网络的 FTP 服务器



6.4.3 公司外部特定 PC

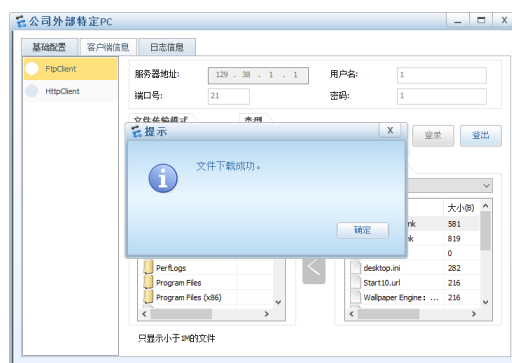
① 在访问规则添加前

访问公司内部特定 PC

```
PC>tracert 129.38.1.4

tracert to 129.38.1.4, 8 hops max
(ICMP), press Ctrl+C to stop
 1  202.39.2.1    32 ms  46 ms  47 ms
 2  202.38.160.1  32 ms  46 ms  47 ms
 3  129.38.1.4   78 ms  79 ms  78 ms
```

访问公司内部 FTP Server 及 WWW Server



访问公司内部 Telnet 服务器

将公司外部特定 PC 换成路由器 C，在命令行界面配置公司外部路由器的 e0 端口为 202.39.2.3/24。

通过路由器 C 登录公司内部 Telnet 服务器

```
<C>telnet 129.38.1.2
Press CTRL_] to quit telnet mode
Trying 129.38.1.2 ...
Connected to 129.38.1.2 ...
Login authentication
Password: 123456
<C>
```

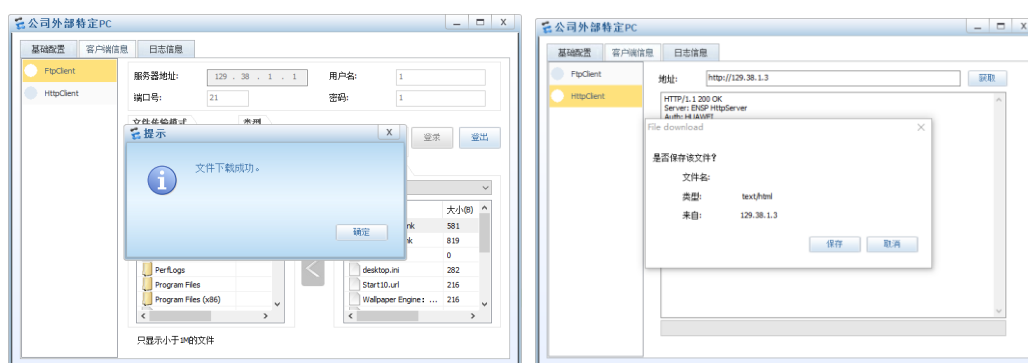
② 在访问规则添加后

访问公司内部特定 PC

```
PC>tracert 129.38.1.4

tracert to 129.38.1.4, 8 hops max
(ICMP), press Ctrl+C to stop
 1  *  *  *
 2  *  *  *
 3  *  *  *
 4  *  *  *
 5  *  *  *
 6  *  *  *
 7  *  *  *
 8  *  *  *
```

访问公司内部 FTP Server 及 WWW Server



访问公司内部 Telnet 服务器

将公司外部特定 PC 换成路由器 C，在命令行界面配置公司外部路由器的 e0 端口为 202.39.2.3/24。

通过路由器 C 登录公司内部 Telnet 服务器

```
<C>telnet 129.38.1.2
Press CTRL_] to quit telnet mode
Trying 129.38.1.2 ...
Connected to 129.38.1.2 ...
```

```
Login authentication
Password: 123456
<gswb>
```

6.4.4 公司内部-PC2

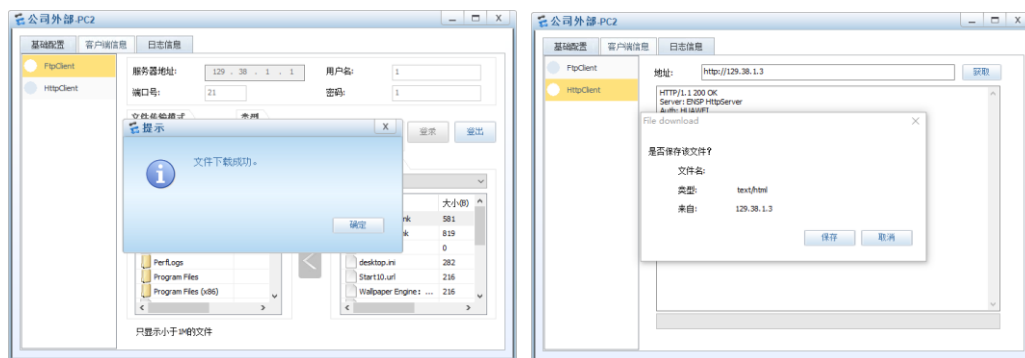
① 在访问规则添加前

访问公司内部特定 PC

```
PC>tracert 129.38.1.4

tracert to 129.38.1.4, 8 hops max
(ICMP), press Ctrl+C to stop
 1  202.39.2.1    32 ms  46 ms  47 ms
 2  202.38.160.1  32 ms  46 ms  47 ms
 3  129.38.1.4   78 ms  79 ms  78 ms
```

访问公司内部 FTP Server 及 WWW Server



访问公司内部 Telnet 服务器

将公司外部-PC2 换成路由器 C2，在命令行界面配置公司外部路由器的 e0 端口为 202.39.2.2/24。

通过路由器 C2 登录公司内部 Telnet 服务器

```
<C2>telnet 129.38.1.2
Press CTRL_] to quit telnet mode
Trying 129.38.1.2 ...
Connected to 129.38.1.2 ...
Login authentication
Password: 123456
<C2>
```

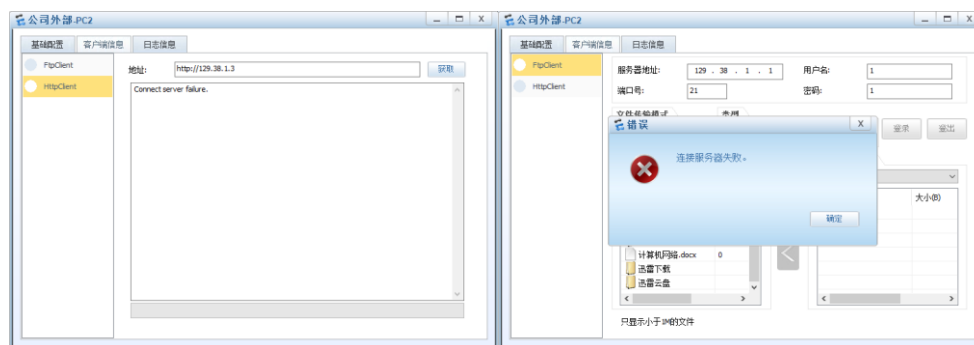
② 在访问规则添加后

访问公司内部特定 PC

```
PC>tracert 129.38.1.4

tracert to 129.38.1.4, 8 hops max
(ICMP), press Ctrl+C to stop
 1      * * *
 2      * * *
 3      * * *
 4      * * *
 5      * * *
 6      * * *
 7      * * *
 8      * * *
```

访问公司内部 FTP Server 及 WWW Server



访问公司内部 Telnet 服务器

将公司外部特定 PC 换成路由器 C2，在命令行界面配置公司外部路由器的 e0 端口为 202.39.2.2/24。

通过路由器 C2 登录公司内部 Telnet 服务器

```
<C2>telnet 129.38.1.2
Press CTRL_] to quit telnet mode
Trying 129.38.1.2 ...
Error: Can't connect to the remote host
<C2>
```

五、 小组签名

陈宇铭	冯博	胡悦	钟奕
-----	----	----	----