

浙大城市学院实验报告

- 课程名称：计算机网络实验
- 实验项目名称：实验十六 防火墙配置实验报告
- 学生姓名：徐彬涵
- 专业班级：软件工程2003
- 学号：32001272
- 实验成绩：
- 指导老师：霍梅梅
- 日期：2022/06/02

一、实验目的

1. 掌握防火墙工作原理；
2. 掌握无状态分组过滤、有状态分组过滤路由器配置；
3. 掌握终端上的防火墙配置

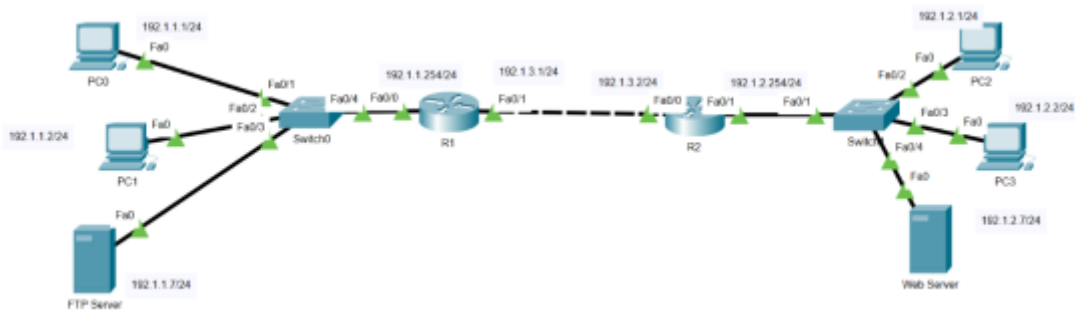
二、实验设备

1. Packet Tracer模拟器软件；
2. Cisco 2911路由器若干台，交换机若干台，PC机若干台，服务器若干台。

三、实验内容

1. 无状态分组过滤器路由器防火墙配置

网络拓扑如下图所示：



- 1) 配置路由器的各个接口的IP地址，子网掩码
- 2) 配置路由器的路由协议（可以用RIP或者OSPF）

R1

```

1 interface FastEthernet0/0
2 ip address 192.1.1.254 255.255.255.0
3 no shutdown
4 interface FastEthernet0/1
5 ip address 192.1.3.1 255.255.255.0
6 no shutdown
7 router rip
8 network 192.1.1.0
9 network 192.1.3.0

```

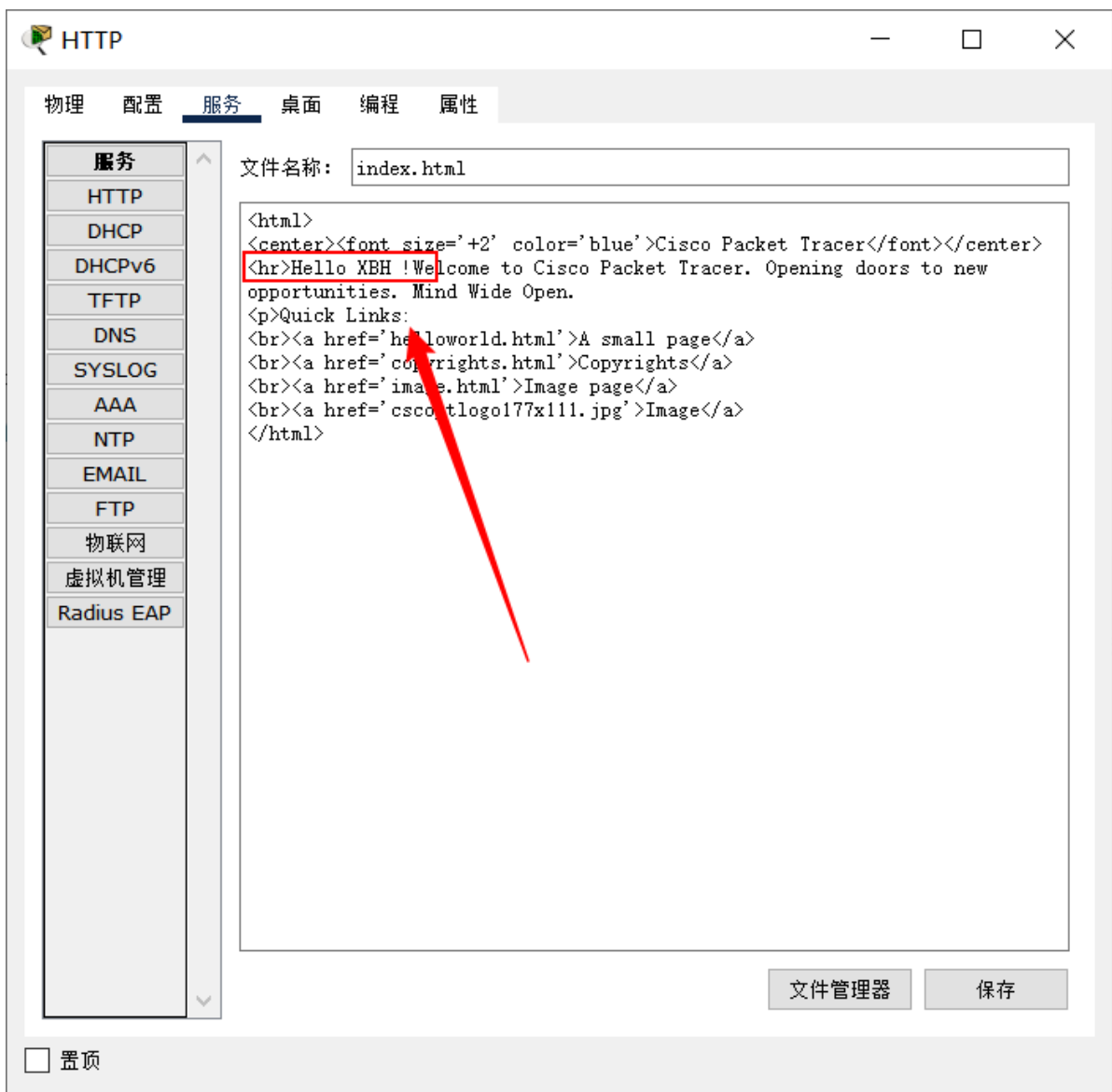
R2

```

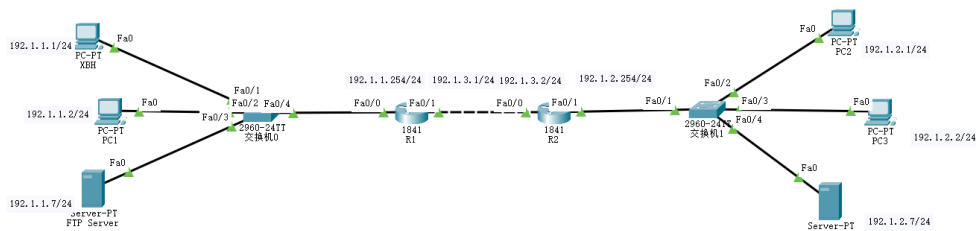
1 interface FastEthernet0/0
2 ip address 192.1.3.2 255.255.255.0
3 no shutdown
4 interface FastEthernet0/1
5 ip address 192.1.2.254 255.255.255.0
6 no shutdown
7 router rip
8 network 192.1.2.0
9 network 192.1.3.0

```

- 3) 配置主机和服务器的IP地址、子网掩码、网关，配置服务器的HTTP、FTP服务；
（在HTTP服务页面上显示自己的名字）



4) 测试全网连通性



5) 配置路由器R1和R2的无状态分组过滤规则

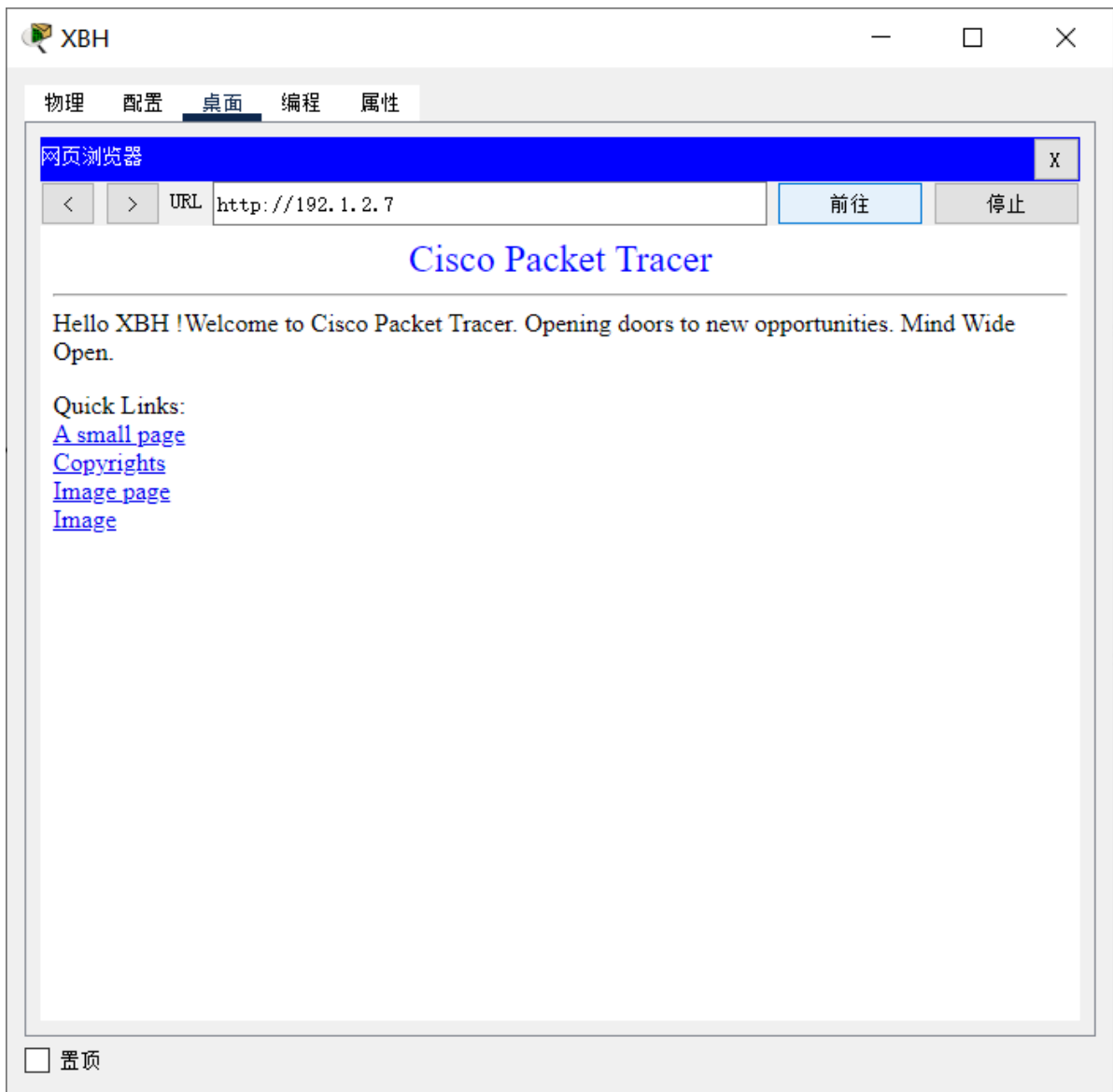
R1

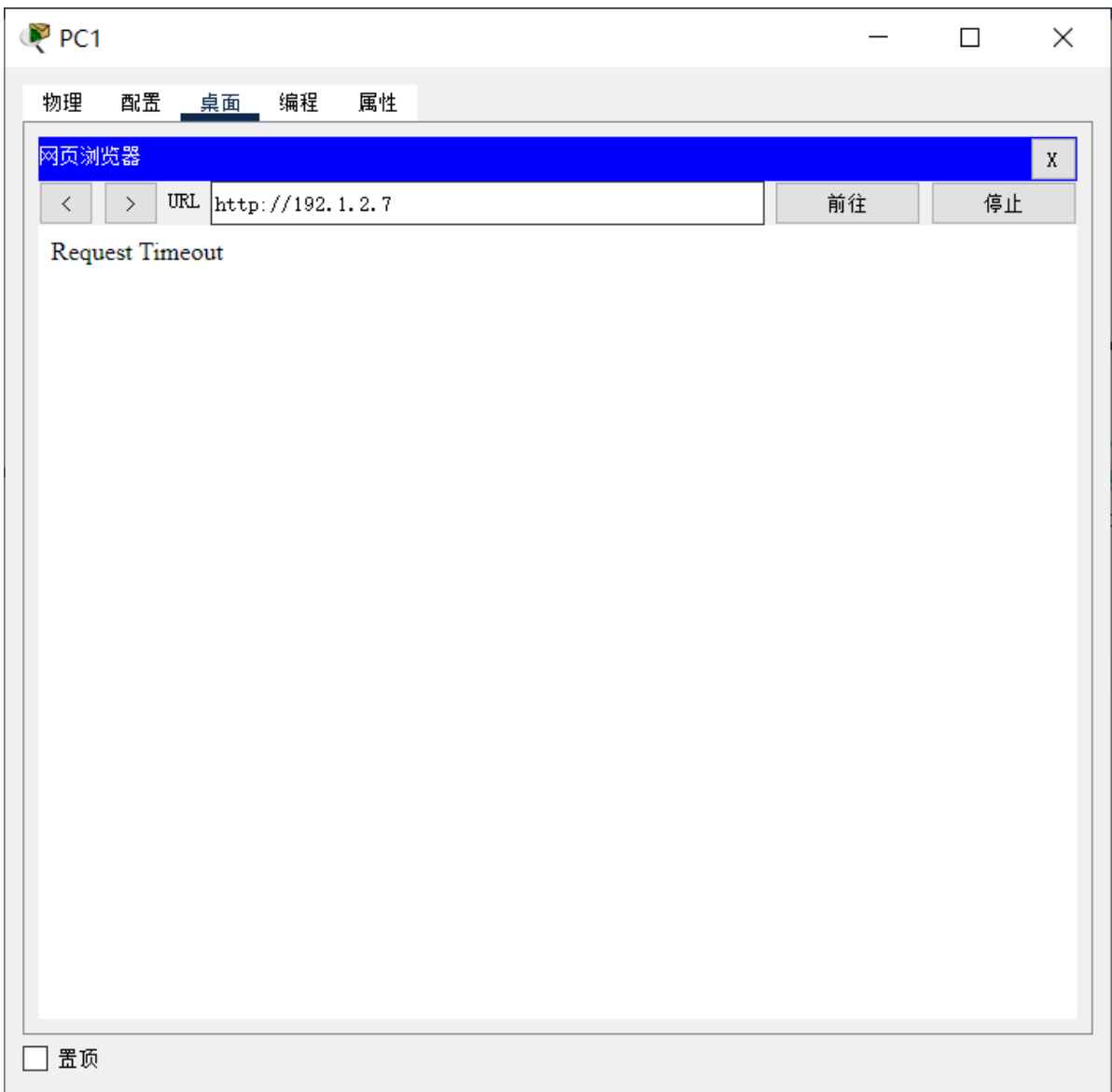
```
1 interface FastEthernet0/0
2 ip access-group 101 in
3 duplex auto
4 speed auto
5 interface FastEthernet0/1
6 duplex auto
7 speed auto
8 access-list 101 permit tcp host 192.1.1.1 host 192.1.2.7 eq www
9 access-list 101 permit tcp host 192.1.1.7 eq ftp host 192.1.2.1
10 access-list 101 permit tcp host 192.1.1.7 gt 1024 host 192.1.2.1
11 access-list 101 deny ip any any
12
```

R2

```
1 interface FastEthernet0/0
2 duplex auto
3 speed auto
4 interface FastEthernet0/1
5 ip access-group 101 in
6 duplex auto
7 speed auto
8 access-list 101 permit tcp host 192.1.2.7 eq www host 192.1.1.1
9 access-list 101 permit tcp host 192.1.2.1 host 192.1.1.7 eq ftp
10 access-list 101 permit tcp host 192.1.2.1 host 192.1.1.7 gt 1024
11 access-list 101 deny ip any any
```

6) 测试过滤规则效果





PC2

物理

配置

桌面

编程

属性

命令行

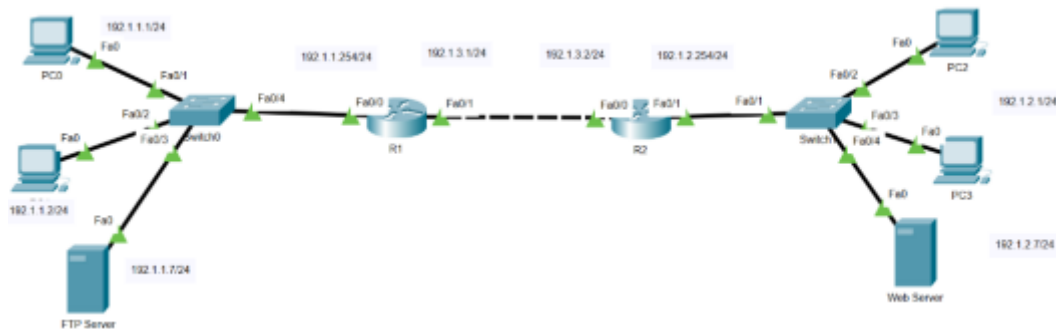
X

C:\>cisco
Invalid Command.

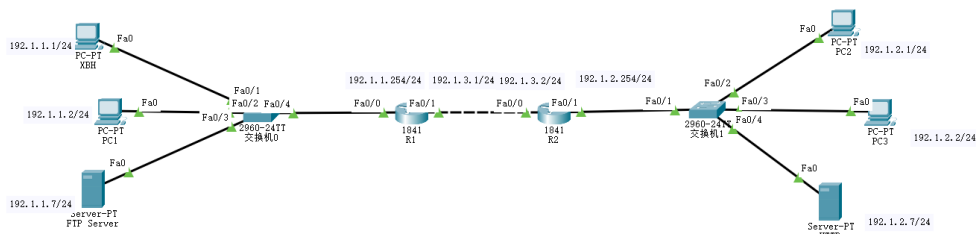
C:\>ftp 192.1.1.7
Trying to connect...192.1.1.7
Connected to 192.1.1.7
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.1.1.7:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
4 : c1841-ipbasek9-mz.124-12.bin 16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
7 : c2600-i-mz.122-28.bin 5571584
8 : c2600-ipbasek9-mz.124-8.bin 13169700
9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
12 : c2800nm-ipbasek9-mz.124-8.bin 15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin 3058048
15 : c2950-i6q412-mz.121-22.EA8.bin 3117390
16 : c2960-lanbase-mz.122-25.EX.bin 4414921

☐ 置顶



- 1) 配置路由器的各个接口的IP地址，子网掩码
- 2) 配置路由器的路由协议（可以用RIP或者OSPF）
- 3) 配置主机和服务器的IP地址、子网掩码、网关，配置服务器的HTTP、FTP服务；
（在HTTP服务页面上显示自己的名字）
- 4) 测试全网连通性



Scenario 0										Realtime
激活	最新状态	源	目的地	类型	颜色	时间(秒)	周期的	编号	编译	删除
成功	成功	PC1	HTTP	ICMP		0.000	N	0	(编辑)	(删除)
成功	成功	PC2	FTP Server	ICMP		0.000	N	1	(编辑)	(删除)
成功	成功	PC1	HTTP	ICMP		0.000	N	2	(编辑)	(删除)

- 5) 配置路由器R1和R2的有状态分组过滤规则

R1

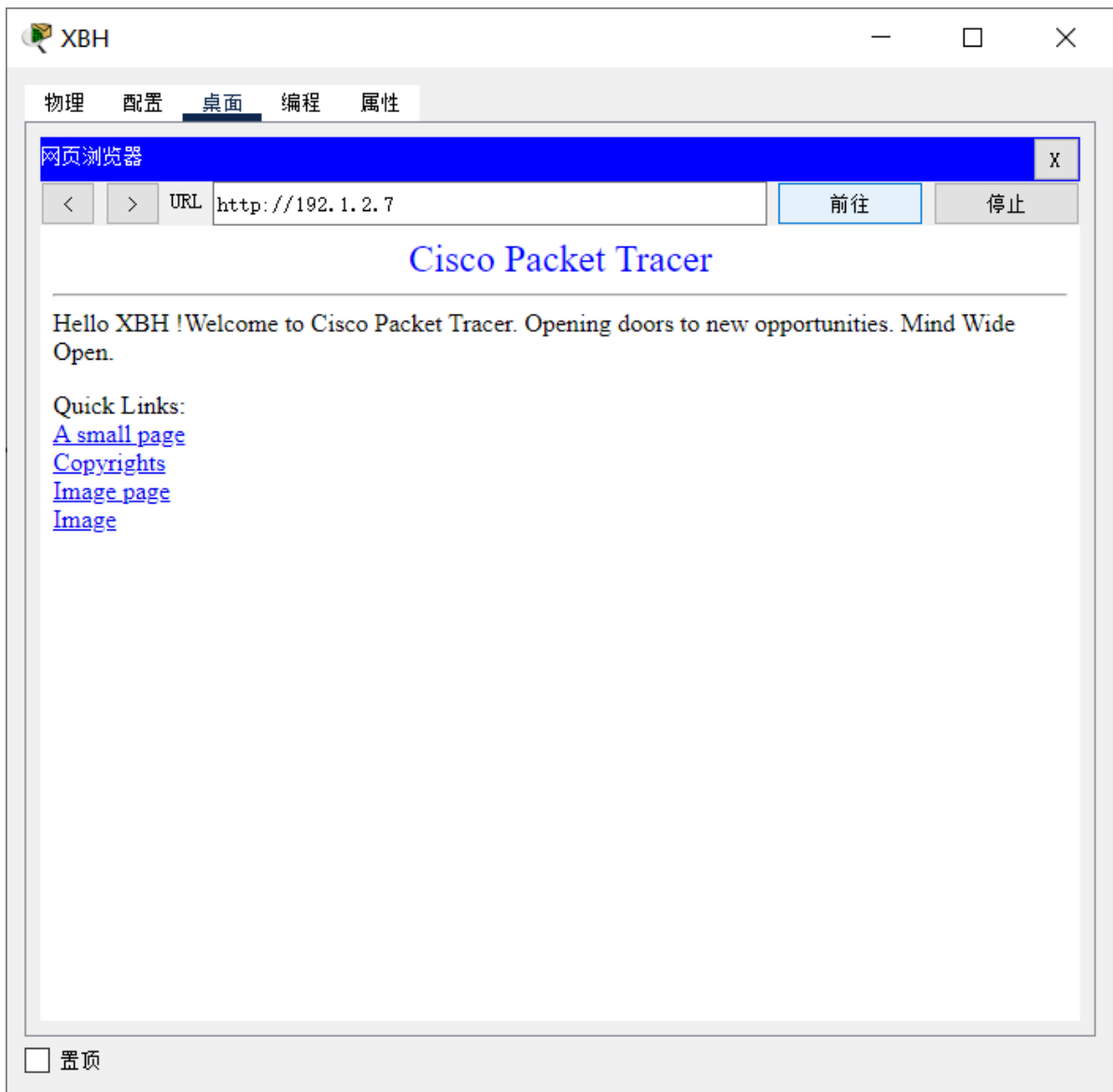
- 1 ip inspect name a1 http timeout 3600
- 2 ip inspect name a1 tcp timeout 3600
- 3 ip inspect name a2 tcp timeout 36
- 4 spanning-tree mode pvst
- 5 interface FastEthernet0/0
- 6 ip access-group 101 in
- 7 ip access-group 102 out
- 8 ip inspect a1 in
- 9 ip inspect a2 out
- 10 duplex auto
- 11 speed auto
- 12 interface FastEthernet0/1
- 13 duplex auto
- 14 speed auto

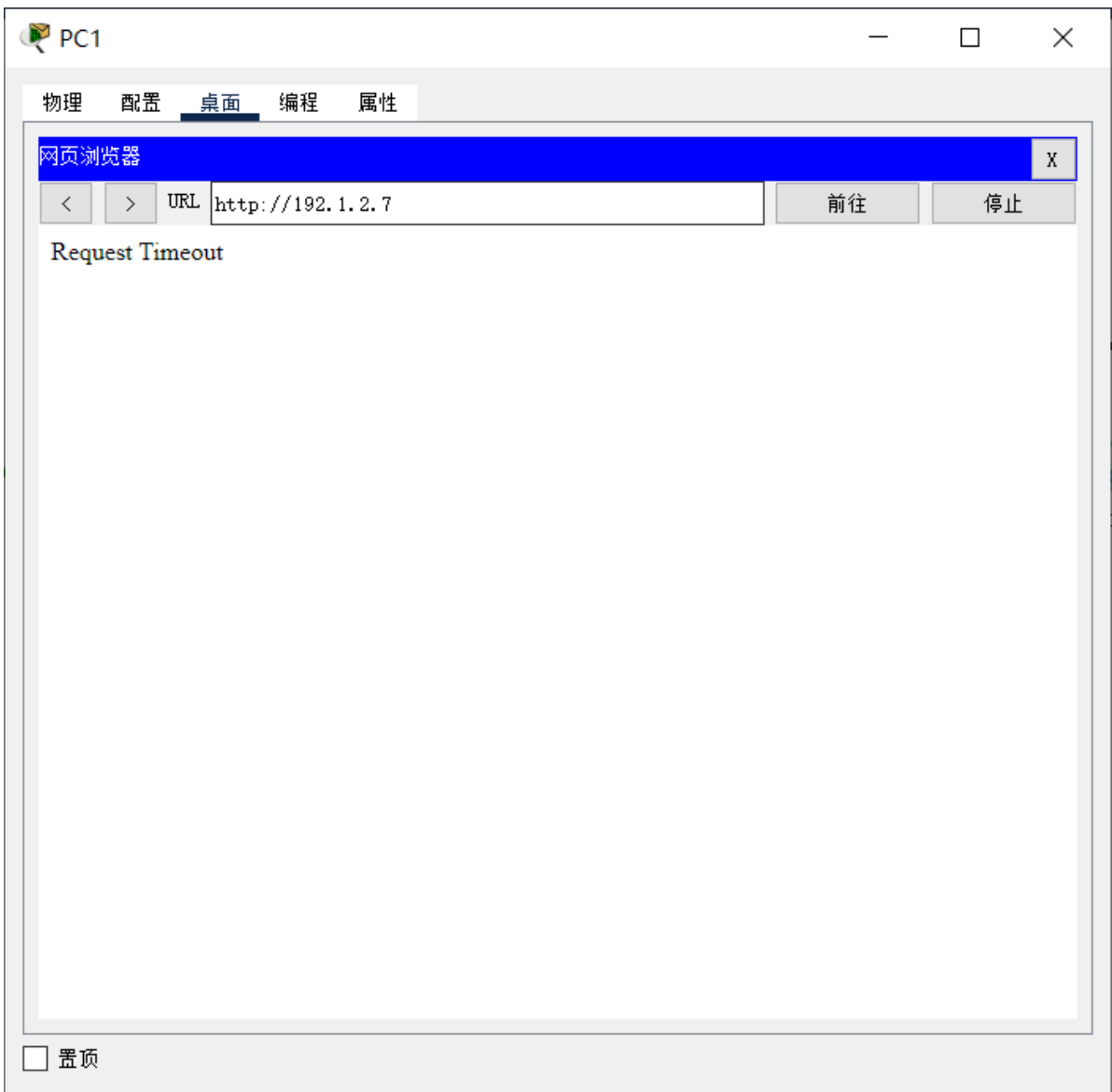
```
15 access-list 101 permit tcp host 192.1.1.1 host 192.1.2.7 eq www
16 access-list 101 deny ip any any
17 access-list 102 permit tcp host 192.1.2.1 host 192.1.1.7 eq ftp
18 access-list 102 permit tcp host 192.1.2.1 host 192.1.1.7 gt 1024
19 access-list 102 deny ip any any
```

R2

```
1 ip inspect name a1 http timeout 3600
2 ip inspect name a1 tcp timeout 3600
3 ip inspect name a2 tcp timeout 3600
4 spanning-tree mode pvst
5 interface FastEthernet0/0
6 duplex auto
7 speed auto
8 interface FastEthernet0/1
9 ip access-group 102 in
10 ip access-group 101 out
11 ip inspect a2 in
12 ip inspect a1 out
13 duplex auto
14 speed auto
15 access-list 101 permit tcp host 192.1.1.1 host 192.1.2.7 eq www
16 access-list 101 deny ip any any
17 access-list 102 permit tcp host 192.1.2.1 host 192.1.1.7 eq ftp
18 access-list 102 permit tcp host 192.1.2.1 host 192.1.1.7 gt 1024
19 access-list 102 deny ip any any
```

6) 测试过滤规则效果





PC2

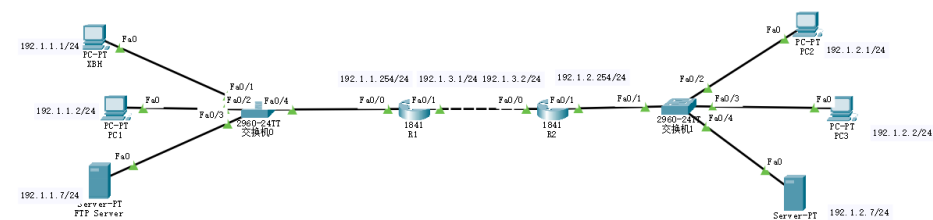
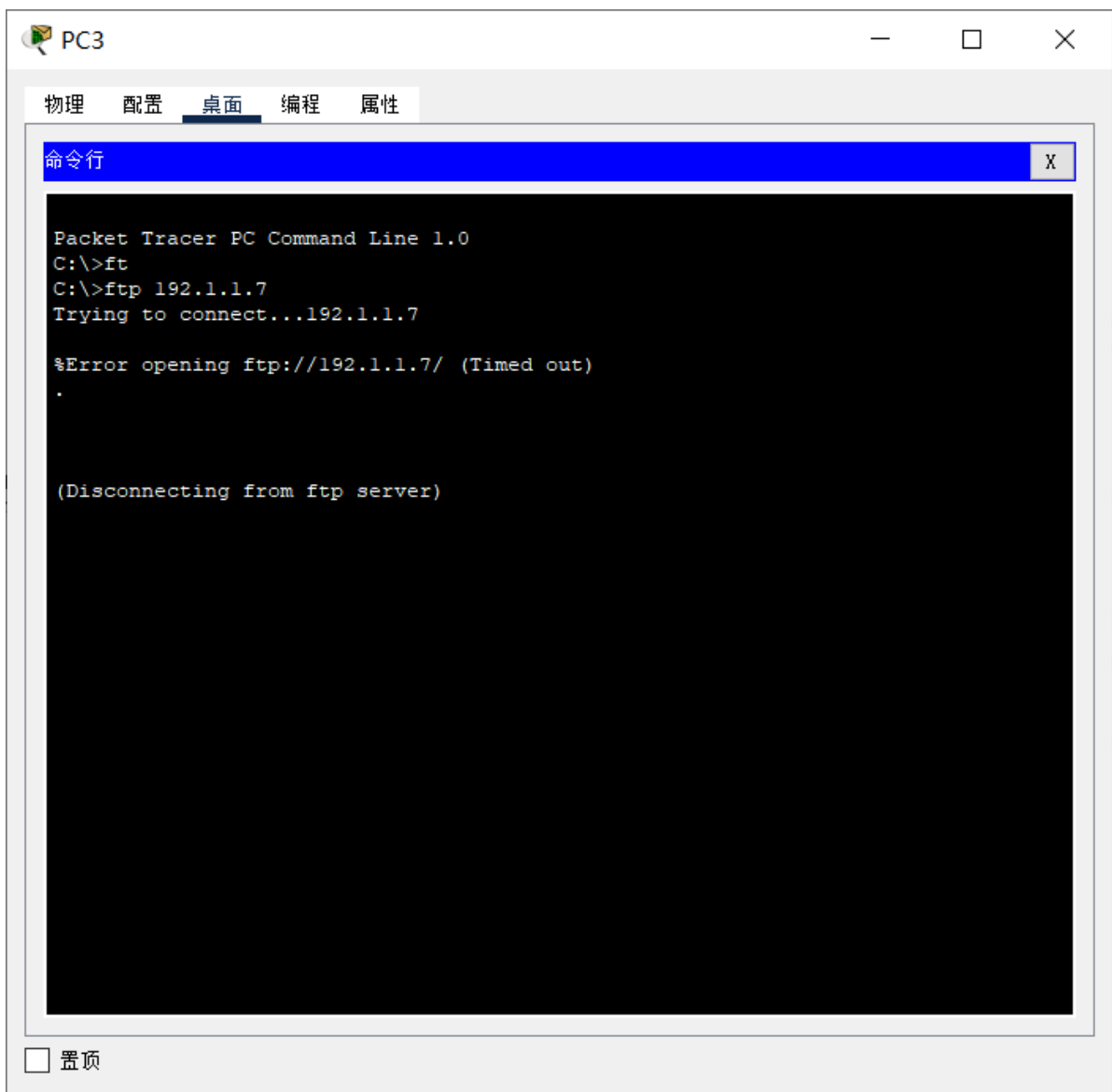
物理配置桌面编程属性

命令行

C:\>ftp 192.1.1.7
Trying to connect...192.1.1.7
Connected to 192.1.1.7
220- Welcome to FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.1.1.7:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
4 : c1841-ipbasek9-mz.124-12.bin 16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
7 : c2600-i-mz.122-28.bin 5571584
8 : c2600-ipbasek9-mz.124-8.bin 13169700
9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
12 : c2800nm-ipbasek9-mz.124-8.bin 15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin 3058048
15 : c2950-i6q412-mz.121-22.EA8.bin 3117390
16 : c2960-lanbase-mz.122-25.FX.bin 4414921
17 : c2960-lanbase-mz.122-25.SEE1.bin 4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
19 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20 : c3560-advipservicesk9-mz.122-46.SE1.bin 10713276

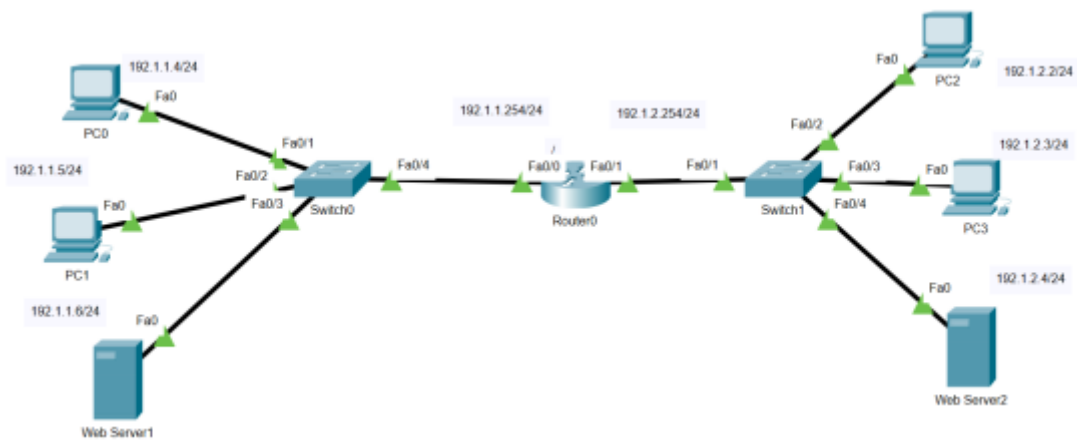
☐ 置顶



激活	最新状态	源	目的地	类型	颜色	时间(秒)	周期的	编号	编译	删除
失败	失败	...	HTTP	ICMP	...	0.000	N	0	(...)	(删除)
失败	失败	...	HTTP	ICMP	...	0.000	N	1	(...)	(删除)
失败	失败	...	FTP	ICMP	...	0.000	N	2	(...)	(删除)
...	(删除)

3. 终端和服务端防火墙配置

网络拓扑如下图所示：



- 1) 配置路由器的各个接口的IP地址，子网掩码
- 2) 配置主机和服务器的IP地址、子网掩码、网关，配置服务器的HTTP服务；
(在两个HTTP服务页面上分别显示自己的名字、自己的兴趣爱好)

R0

```

1 interface FastEthernet0/0
2 ip address 192.1.1.254 255.255.255.0
3 no shutdown
4 interface FastEthernet0/1
5 ip address 192.1.2.254 255.255.255.0
6 no shutdown
7 router rip
8 network 192.1.1.0
9 network 192.1.2.0

```

Web Server1

物理

配置

服务

桌面

编程

属性

服务

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

物联网

虚拟机管理

Radius EAP

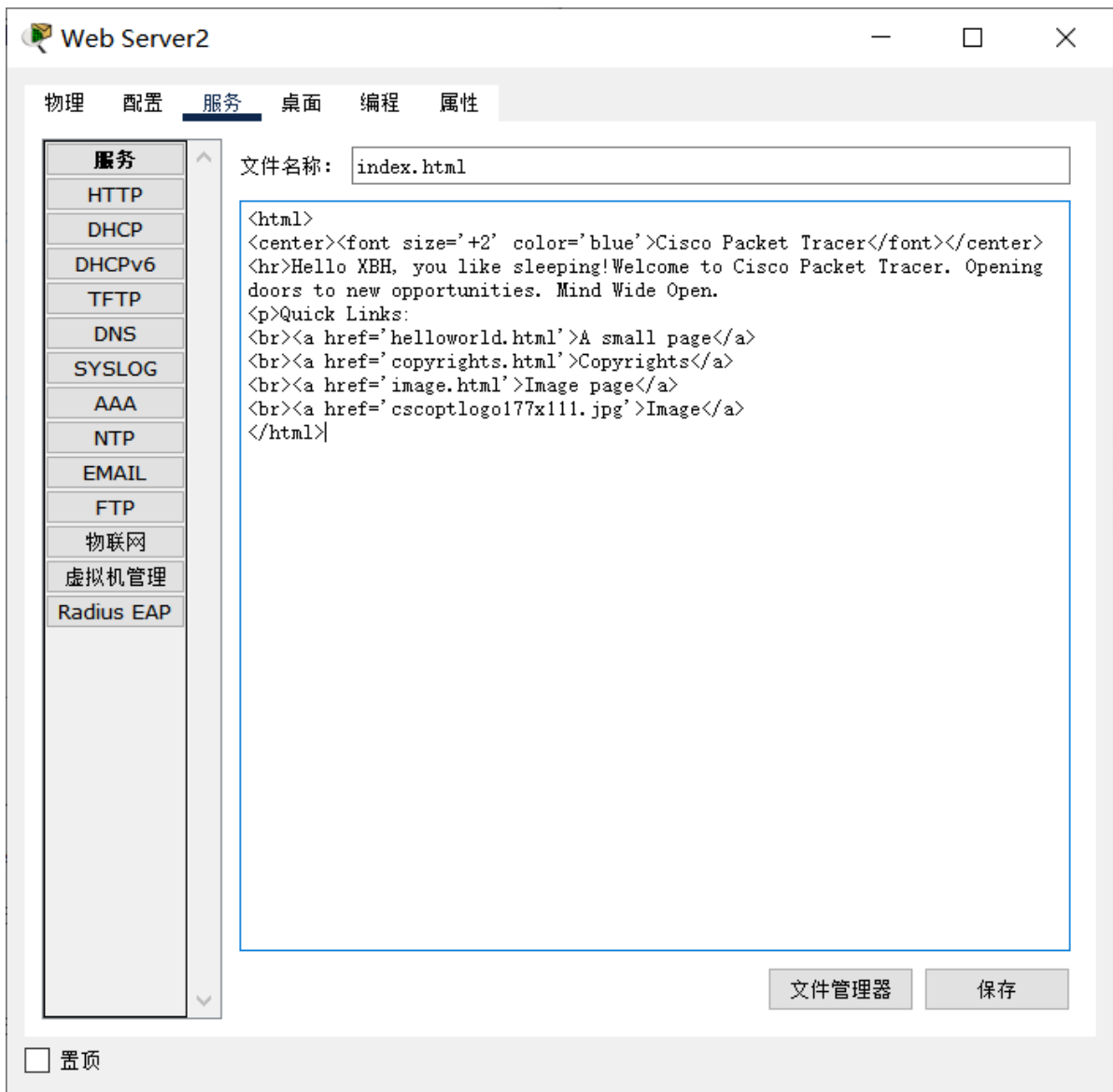
文件名称: index.html

```
<html>
<center><font size='+2' color='blue'>Cisco Packet Tracer</font></center>
<hr>Hello XBH, you like eating!Welcome to Cisco Packet Tracer. Opening
doors to new opportunities. Mind Wide Open.
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

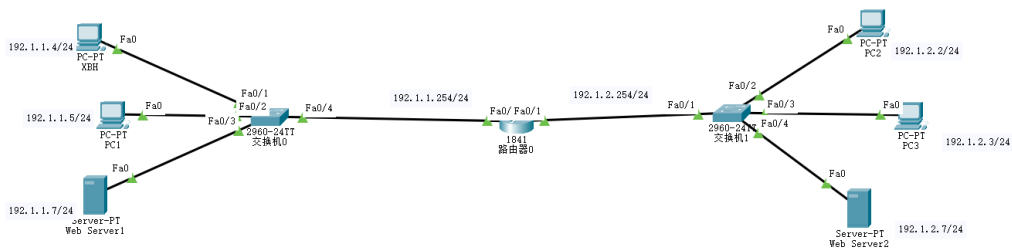
文件管理器

保存

☐ 置顶



3) 测试全网连通性



Scenario 0

新建 删除

切换PDU列表窗口

源	目的地	类型	颜色	时间(秒)	周期	编号	编辑	删除
成功 XBH	Web Server2	ICMP	0.000	N	0	(...)		(删除)
成功 PC1	Web Server2	ICMP	0.000	N	1	(...)		(删除)
成功 PC2	Web Server1	ICMP	0.000	N	2	(...)		(删除)

4) 配置每台终端的防火墙



XBH



物理

配置

桌面

编程

属性

防火牆

X

服务

● 开 ○ 关

接口 FastEthernet0

入站规则

动作



协议



远程IP

远程通配符掩码

远程端口

本地端口

保存

移除

添加

	动作	协议	远程IP	远程通配符	远程端口	本地端口
1	Deny	ICMP	192.1.2.2	0.0.0.1	-	-
2	Allow	IP	0.0.0.0	255.255.255...	-	-

☐ 置顶

PC1

物理配置桌面编程属性

防火墙

X

服务

开关

接口

FastEthernet0

入站规则

动作

协议

远程IP

远程通配符掩码

远程端口

本地端口

保存

移除

添加

	动作	协议	远程IP	远程通配符	远程端口	本地端口
1	Deny	ICMP	192.1.2.2	0.0.0.1	-	-
2	Allow	IP	0.0.0.0	255.255.255...	-	-

置顶

Web Server1

物理

配置

服务

桌面

编程

属性

防火墙

X

服务

开

关

接口

FastEthernet0

入站规则

动作

协议

远程IP

远程通配符掩码

远程端口

本地端口

保存

移除

添加

	动作	协议	远程IP	远程通配符	远程端口	本地端口
1	Allow	TCP	192.1.2.2	0.0.0.1	any	80
2	Allow	IP	192.1.1.4	0.0.0.1	-	-
3	Deny	IP	0.0.0.0	255.255.255...	-	-

置顶



PC2



物理

配置

桌面

编程

属性

X

● 开 ○ 关

接口

FastEthernet0

入站规则

协议

协议

远程通配符掩码

远程通配符掩码

本地端口

本地端口

移除

添加

	动作	协议	远程IP	远程通配符	远程端口	本地端口
1	Deny	ICMP	192.1.1.4	0.0.0.1	-	-
2	Allow	IP	0.0.0.0	255.255.255...	-	-



PC3



物理

配置

桌面

编程

属性

X

● 开 ○ 关

接口

FastEthernet0

入站规则

动作

协议

远程IP

远程通配符掩码

远程端口

本地端口

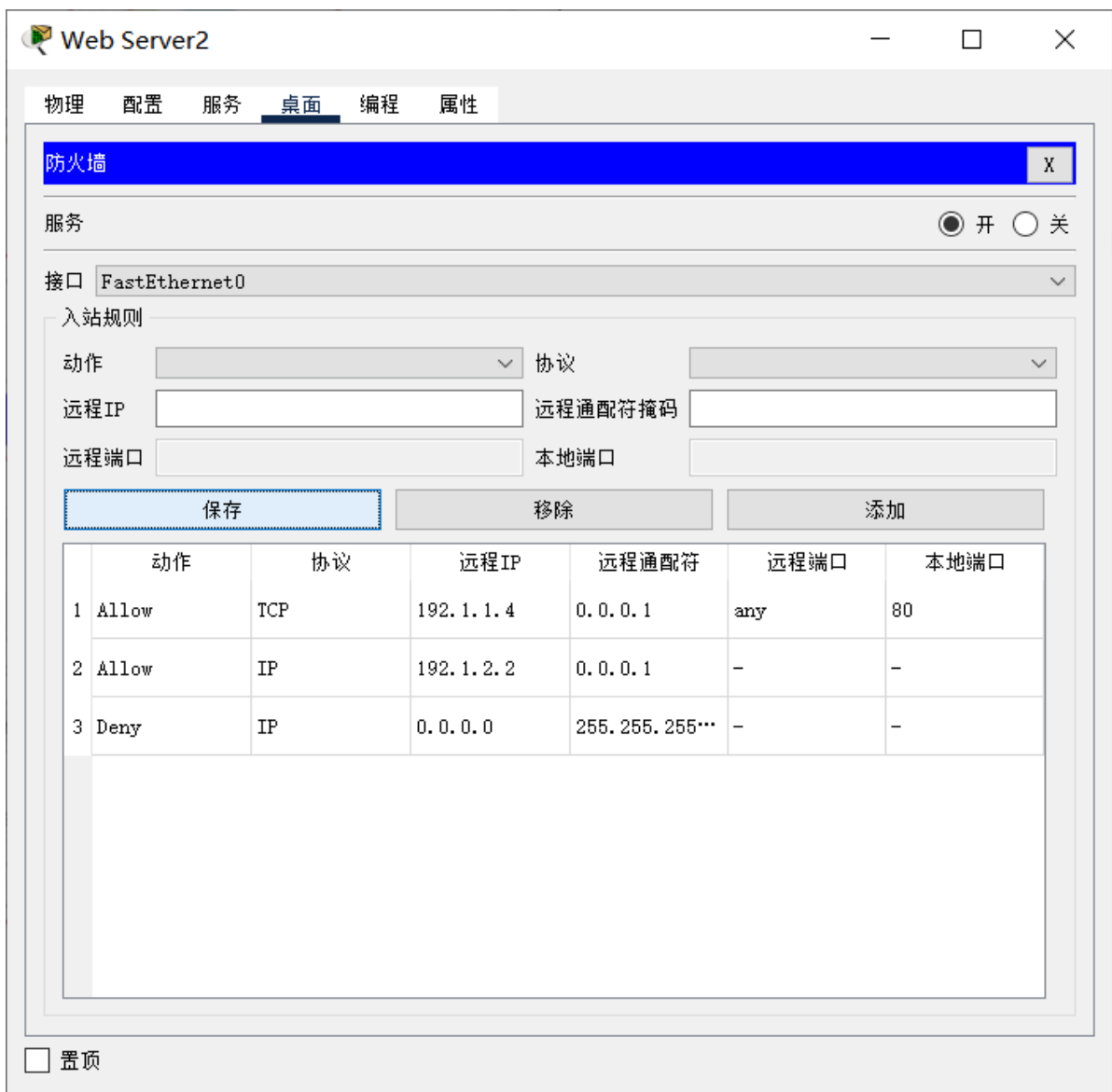
移除

添加

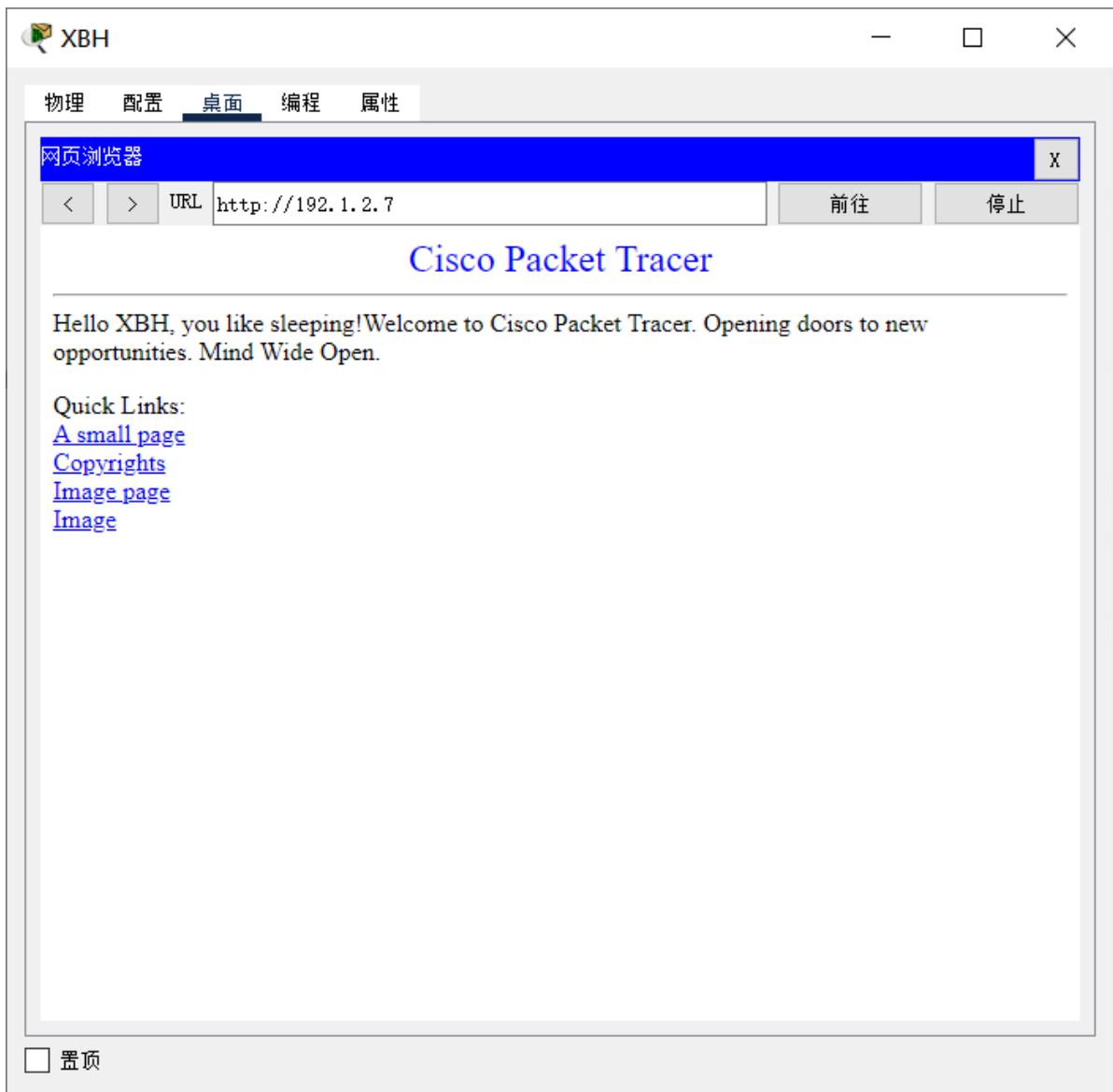
	动作	协议	远程IP	远程通配符	远程端口	本地端口
1	Deny	ICMP	192.1.1.4	0.0.0.1	-	-
2	Allow	IP	0.0.0.0	255.255.255...	-	-

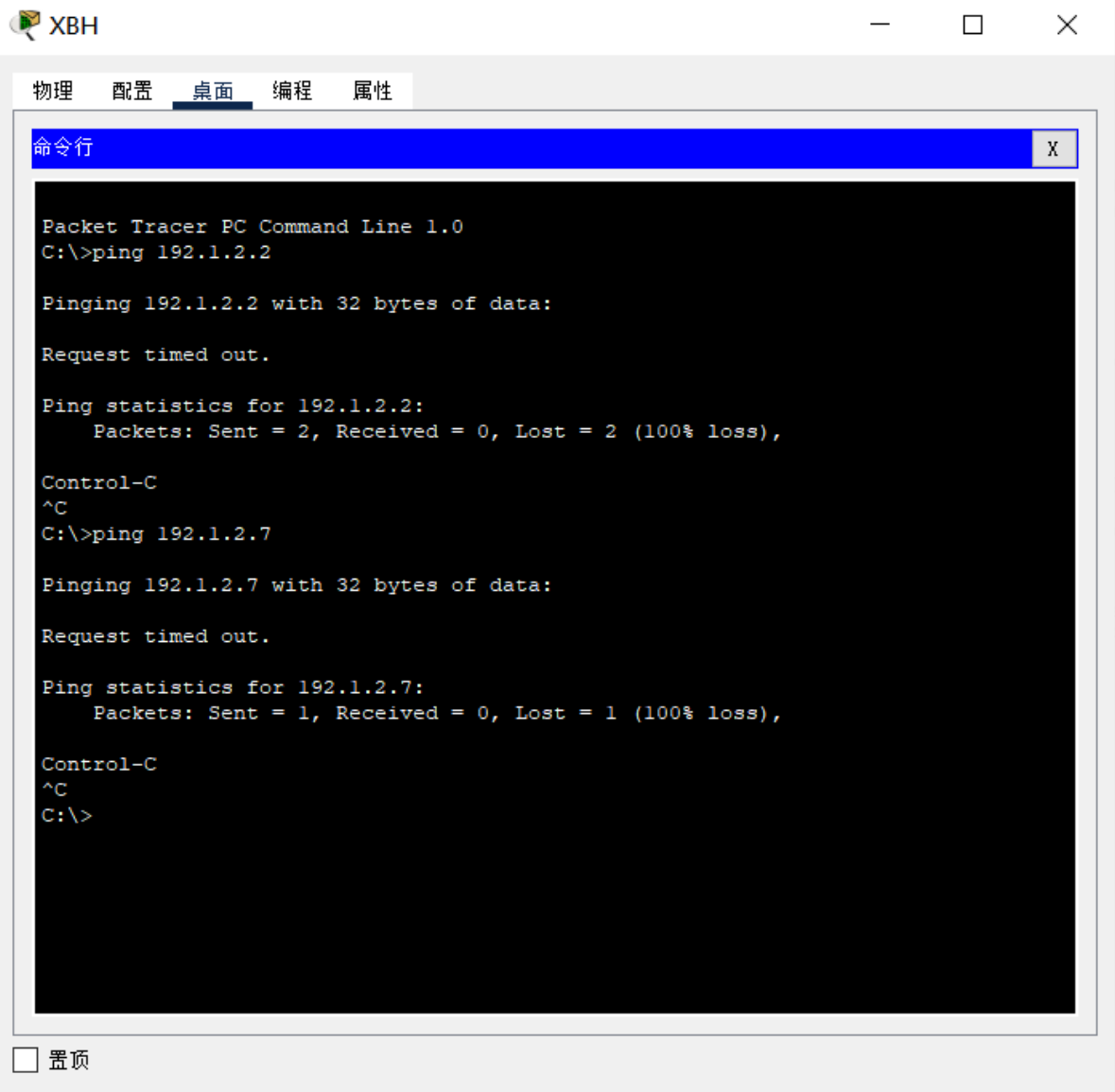
☐ 置顶

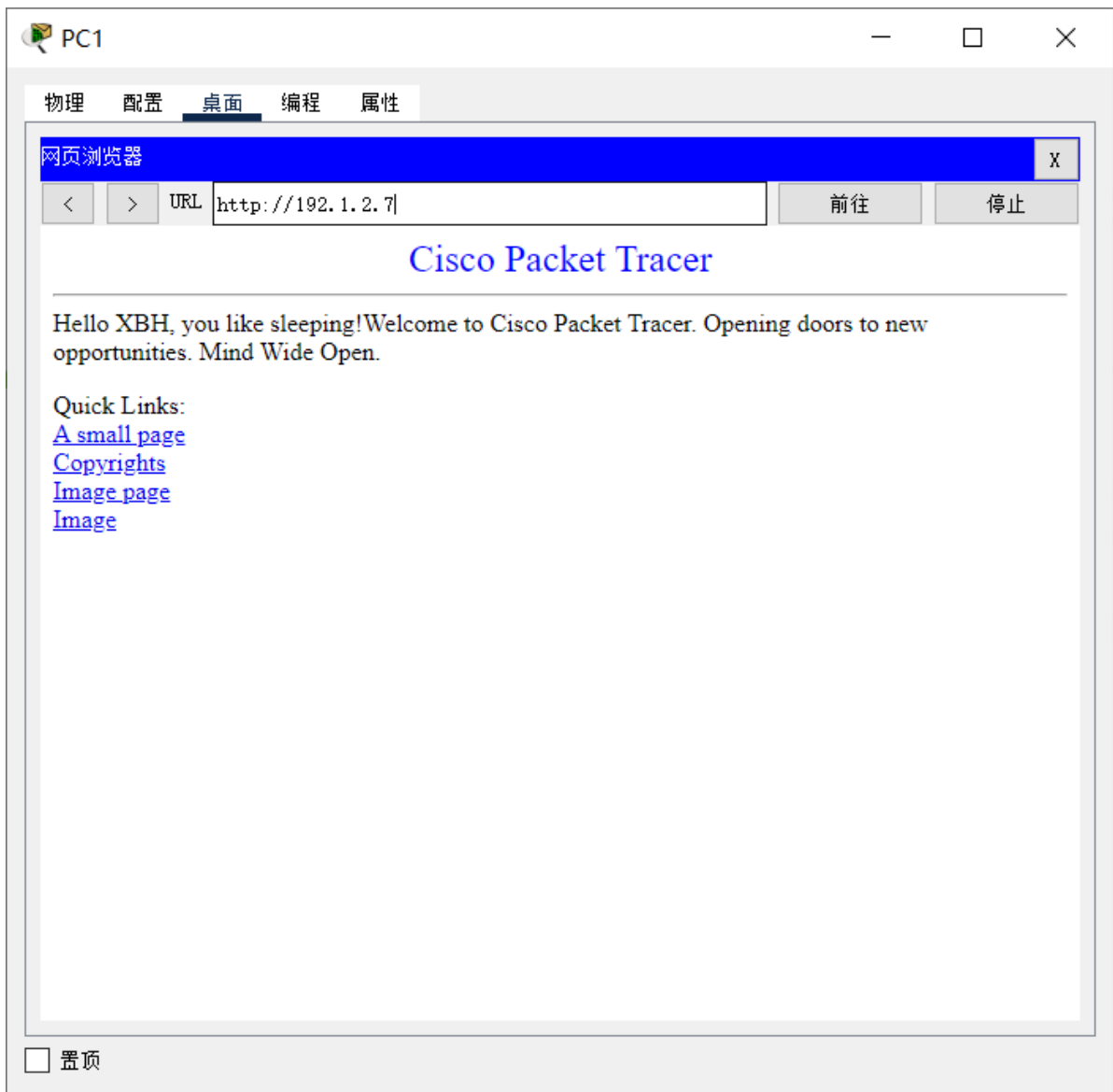
置顶

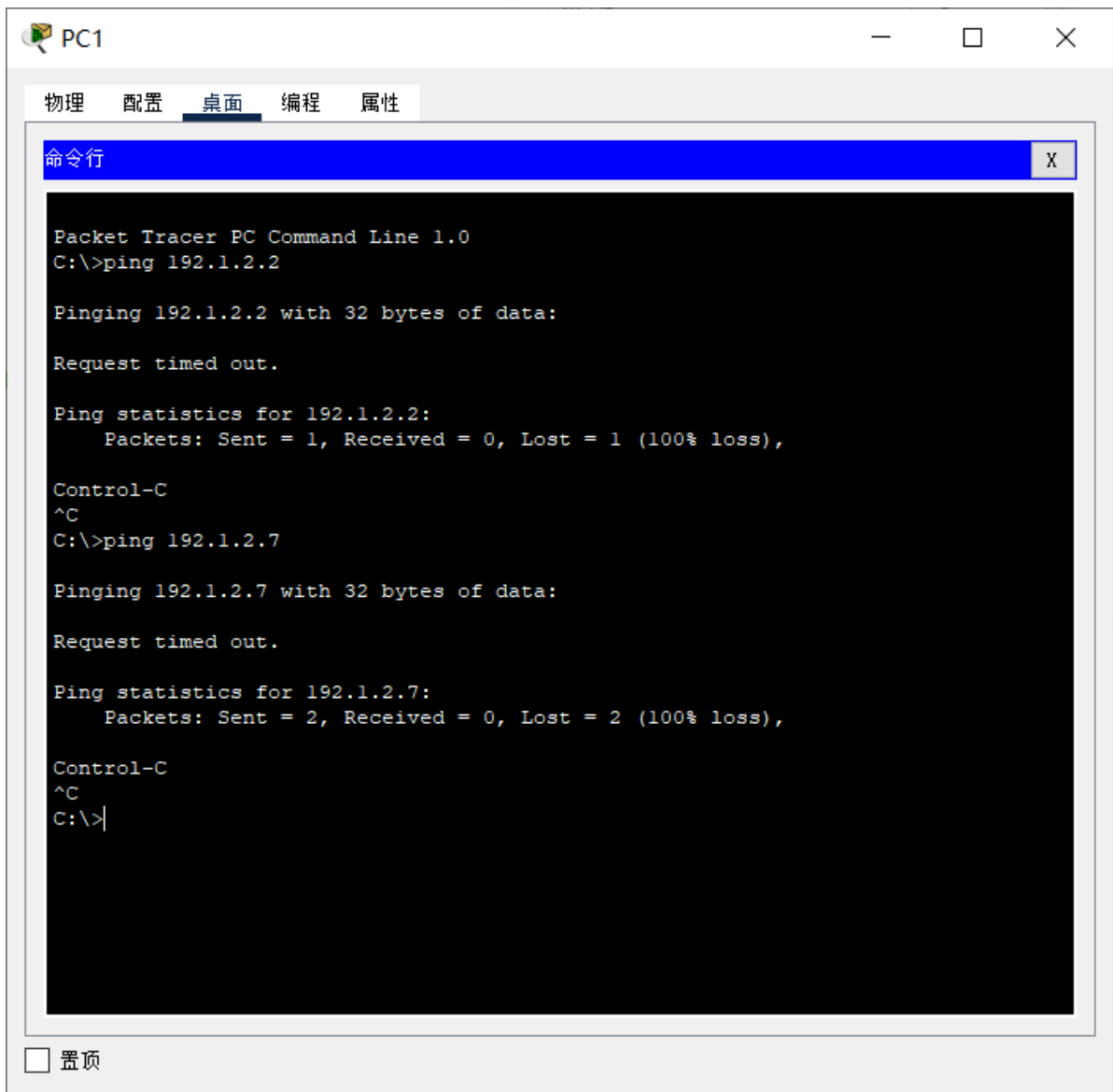


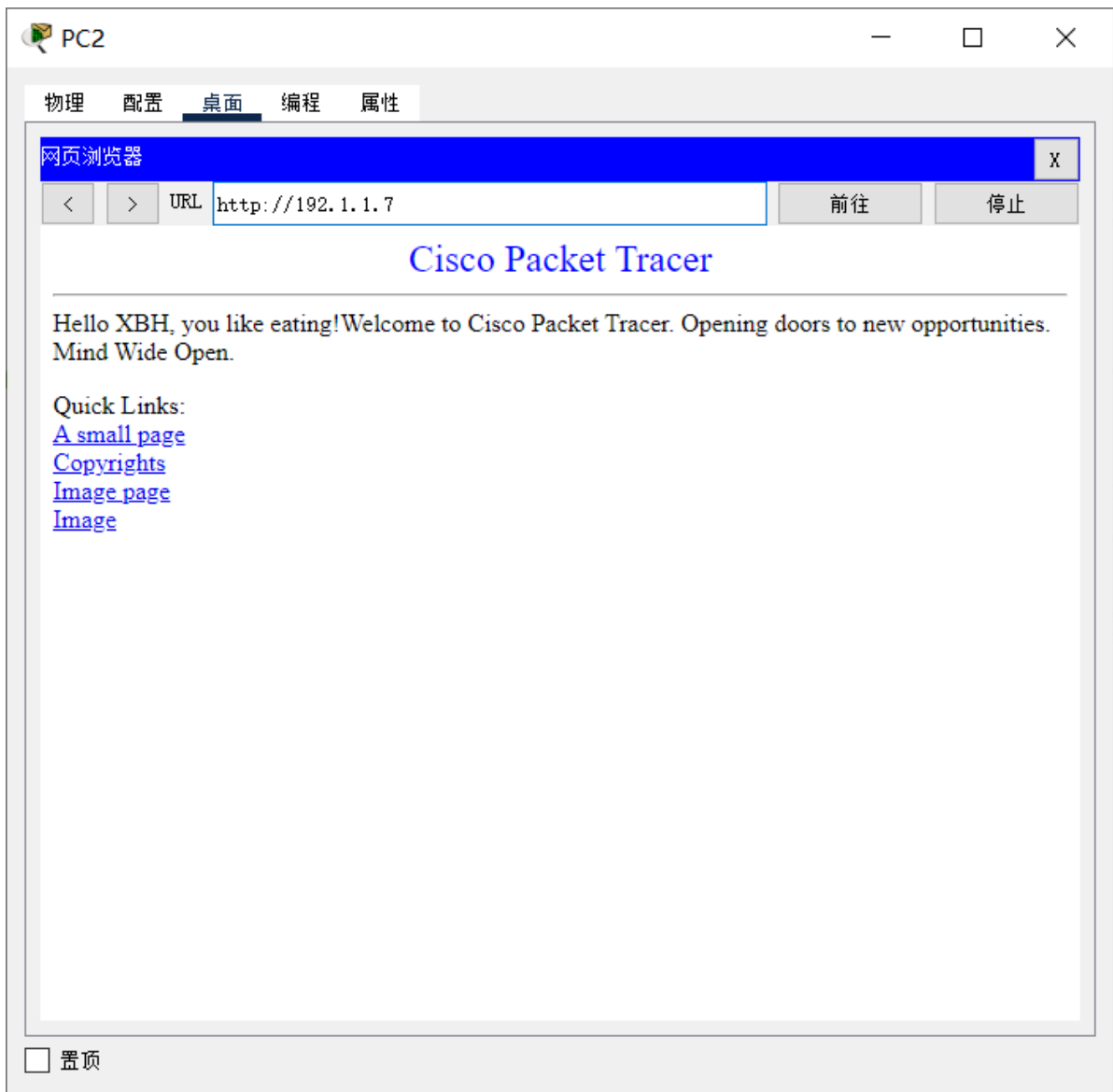
5) 测试防火墙过滤规则效果











```
Packet Tracer PC Command Line 1.0
C:\>ping 192.1.1.4

Pinging 192.1.1.4 with 32 bytes of data:

Request timed out.

Ping statistics for 192.1.1.4:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

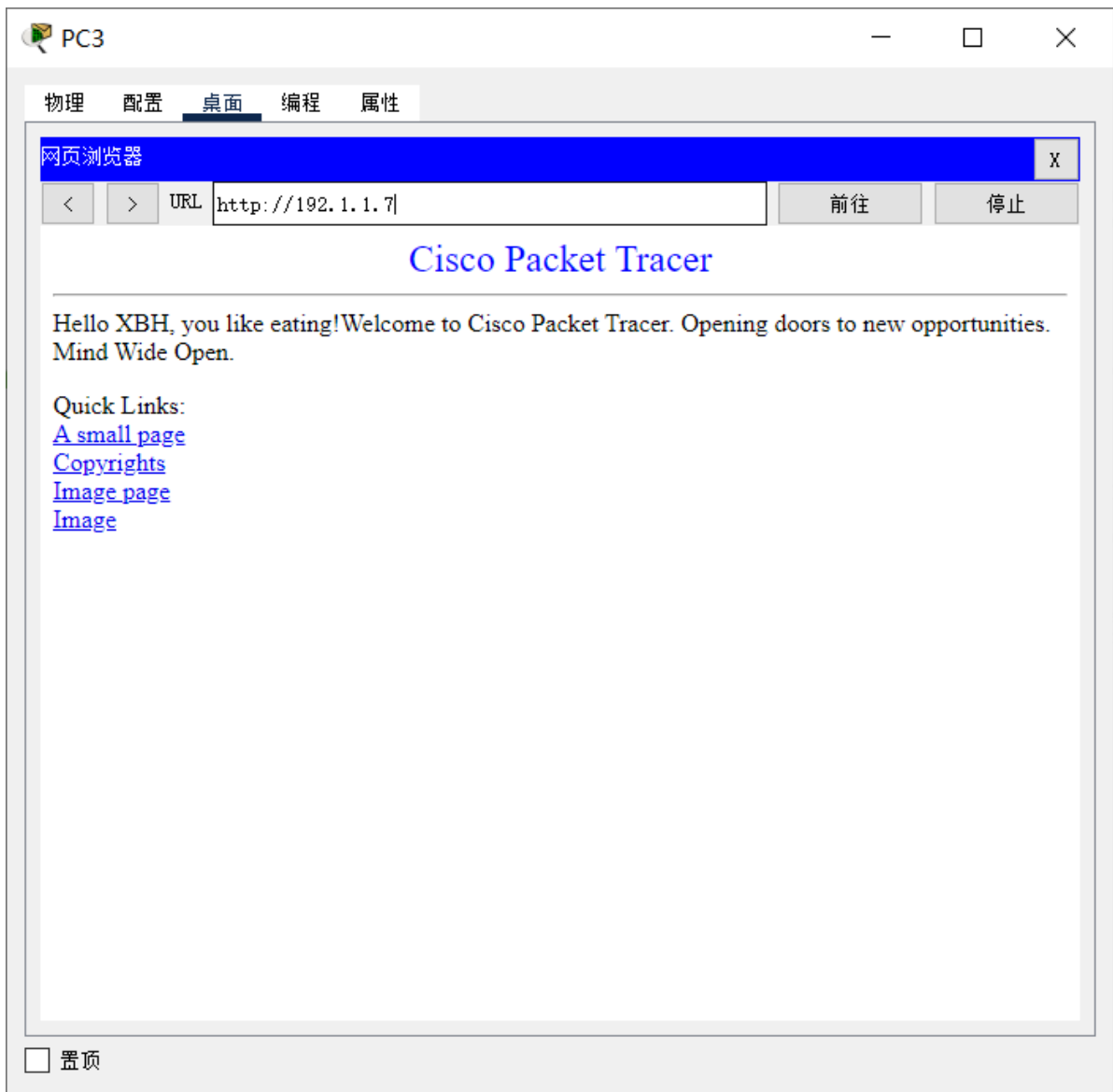
Control-C
^C
C:\>ping 192.1.1.7

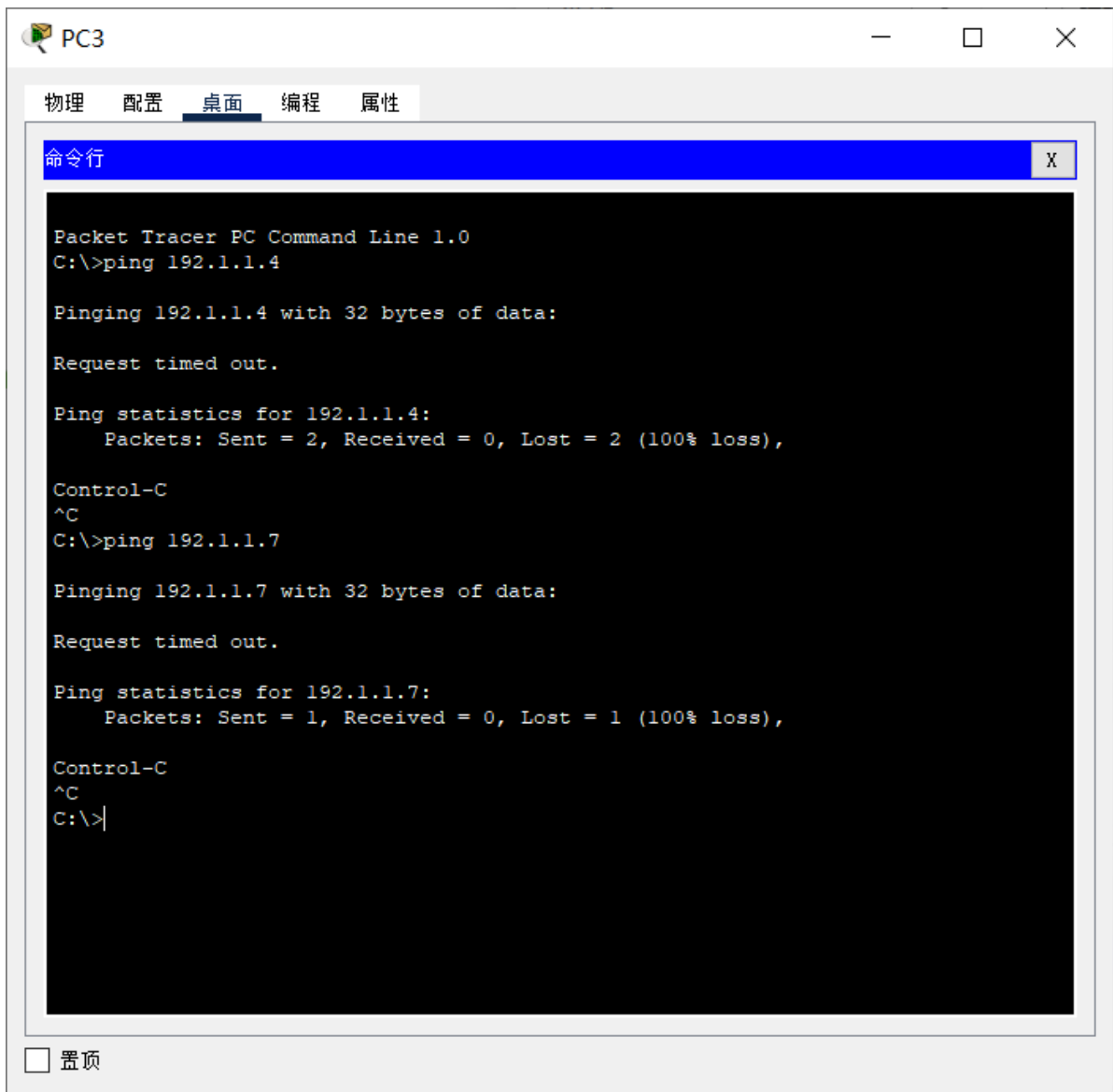
Pinging 192.1.1.7 with 32 bytes of data:

Request timed out.

Ping statistics for 192.1.1.7:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
C:\>
```





四、收获感想：

记录实验感受、操作过程中遇到的困难及解决办法、遗留的问题、意见和建议等。

学习了防火墙的设置