

实验六 入侵检测系统实验

1. 入侵检测系统实验一

1.1 实验内容

互连网结构如图 1 所示，完成路由器 R 的接口和终端的网络信息配置过程后，各个终端之间是可以相互 ping 通的。

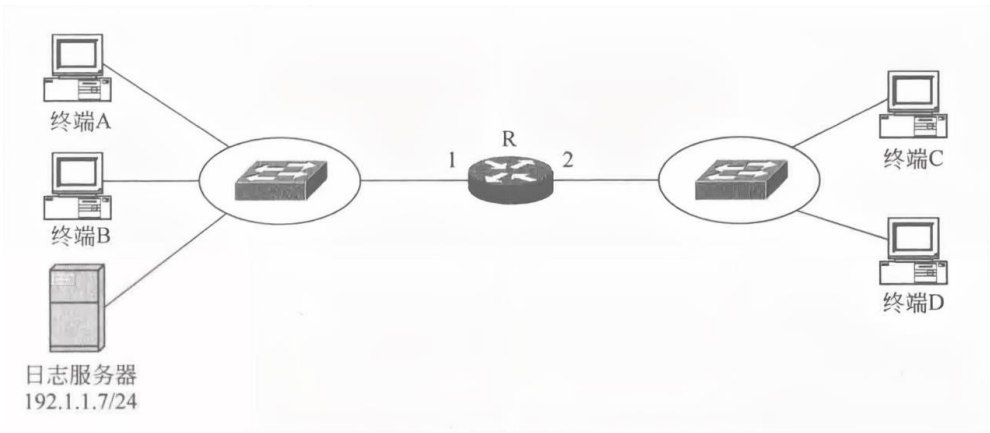


图 1 互连网结构

在路由器 R 接口 1 输出方向设置入侵检测规则，该规则要求，一旦检测到 ICMP ECHO 请求报文，则丢弃该 ICMP ECHO 请求报文，并向日志服务器发送警告信息。启动该入侵检测规则后，如果终端 C 和 D 发起 ping 终端 A 和 B 的操作，则 ping 操作不仅无法完成，而且会在日志服务器中记录警告信息。如果终端 A 和终端 B 发起 ping 终端 C 和 D 的操作，则 ping 操作依然能够完成。

1.2 实验目的

- 1) 验证入侵检测系统配置过程。
- 2) 验证入侵检测系统控制信息流传输过程的机制。
- 3) 验证基于特征库的入侵检测机制的工作过程。
- 4) 验证特征定义过程。

1.3 实验原理

Cisco 集成在路由器中的入侵检测系统(Intrusion Detection System, IDS)采用基于特征的入侵检测机制。首先需要加载特征库，特征库中包含用于标识各种入侵行为的信息流特征，一旦在某个路由器接口的输入或输出方向设置入侵监测机制，则需要采集通过该接口输入或输出的信息流，然后与加载的特征库中的特征进行比较，如果该信息流与标识某种入侵行为相关的信息流特征匹配，则对该信息流采取相关的动作。因此，特征库中与每一种入侵行为相关的信息流特征有两部分：一是标识入侵行为的信息流特征；二是对具有入侵行为特征的信息流所采取的动作。

1.4 实验步骤

- 1) 根据如图 1 所示互连网结构放置和连接设备，完成设备放置和连接后的逻辑工作区界面如图 2 所示。完成路由器接口 IP 地址和子网掩码配置过程，根据路由器接口配置的信息完成各个终端、Syslog Server（日志服务器）的网络信息配置过程（图示 ip 配置仅供参考，合理即可），验证终端之间的连通性，如图 3 所示。

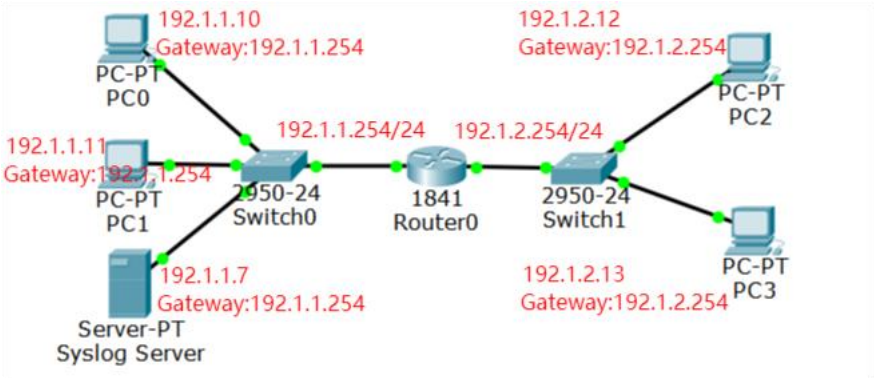


图 2 完成设备放置和连接后的逻辑工作区界面

Fire	Last Statu	Sourc	Destinatio	Type	Colo	Time(s	Period	Num	Edit	Delete
●	Successful	PC0	PC2	ICMP		0.000	N	0	(ed...	(delete)
●	Successful	PC1	PC3	ICMP		0.000	N	1	(ed...	(delete)
●	Successful	PC2	PC1	ICMP		0.000	N	2	(ed...	(delete)

图 3 验证终端之间的连通性

- 2) 在 CLI（命令行接口）配置方式下，完成路由器 Router0 入侵检测系统配置过程。配置的入侵检测规则使路由器 Router0 接口 FastEthernet0/0 输出方向丢弃与编号为 2004、子编号为 0 的特征匹配的 ICMP ECHO 请求报文。
- ① 确定特征库存储位置并指定入侵检测规则

```
Router0
Physical Config CLI
IOS Command Line Interface
Router>en
Router#mkdir ipsdr
Create directory filename [ipsdr]?
Created dir flash:ipsdr

Router#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#ip ips config location flash:ipsdr
Router(config)#ip ips name al
```

图 4 入侵检测系统配置过程一

mkdir directory-name 是特权模式下使用的命令，该命令的作用是在闪存中创建一个用于存储特征库的目录。该命令执行后，需要按 Enter 键确定目录名。

ip ips config location url 是全局模式下使用的命令，该命令的作用是指定用于存储特征库的目录。

ip ips name ips-name [list acl] 是全局模式下使用的命令,该命令的作用是指定名字为 **al** 的入侵检测规则。在该入侵检测规则作用到某个路由器接口的输入或输出方向前,路由器并不加载特征库。也可以指定一个分组过滤器,则只对分组过滤器允许通过的信息流进行入侵检测。参数 **acl** 是分组过滤器编号。

② 开启日志功能

以下命令序列完成四个功能:一是将事件记录在日志服务器中作为指定的事件通知方法,检测到与特征匹配的信息流称为事件;二是指定日志服务器的 IP 地址。由于指定的事件通知方法是将是事件记录在日志服务器中,因此,需要指定日志服务器的 IP 地址;三是指定在日志信息中标记日期和时间,且将时间精确到毫秒;四是为了产生正确的日期时间,调整路由器的时钟。

```
Router(config)#ip ips notify log
Router(config)#logging host 192.1.1.7
Router(config)#service timestamps log datetime msec
Router(config)#exit
Router#
*3? 01, 01:46:26.4646: *3? 01, 01:46:26.4646: %SYS-5-CONFID
*3? 01, 01:46:26.4646: *3? 01, 01:46:26.4646: %SYS-6-LOGGII
Router#clock set 14:06:00 2 May 2022
```

图 5 入侵检测配置过程二

ip ips notify log 是全局模式下使用的命令,该命令的作用是将事件记录在日志服务器中作为指定的事件通知方法, **log** 表明将事件记录在日志服务器中。

logging host ip-address 是全局模式下使用的命令,该命令的作用是指定 192.1.1.7 为日志服务器的 IP 地址。

service timestamps log datetime msec 是全局模式下使用的命令,该命令的作用是要求在发送的日志信息中标记日期时间,并要求时间精确到毫秒。

clock set 14:06:00 2 May 2022 是特权模式下使用的命令,该命令的作用是将路由器时钟设置为 2022-5-2 14:06。

③ 配置每一类特征

以下命令序列完成两个功能:一是释放所有类别的特征库;二是指定需要加载特征库类别。

```
Router(config)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this
```

图 6 入侵检测系统配置过程三

ip ips signature-category 是全局模式下使用的命令,该命令的作用是进入特征库分类配置模式。

category all 是特征库分类配置模式下使用的命令。该命令的作用有两个:一是指定所有类别特征库, **all** 表示所有类别特征库;二是进入指定类别特征库的动作配置模式。

retired true 是动作配置模式下使用的命令。该命令的作用是释放指定类别的特征

库，这里的指定类别是所有类别。各种类别的特征库都比较庞大，如果加载所有类别的特征库，则会引发内存紧张，因此，一般情况下之加载部分类别特征库。

category ios_ips basic 是特征库分类配置模式下使用的命令，该命令的作用有两个：一是指定特征库类别，ios_ips 是类别名，basic 是类别子名，即 ios_ips 类别中的 basic 子类别；二是进入指定类别特征库的动作配置模式。

retired false 是动作配置模式下使用的命令，该命令的作用是加载指定类别的特征库，这里的指定类别是 ios_ips 类别中的 basic 子类别。

退出特征库分类配置模式时，会出现提示信息，按 Enter 键确认。

④ 将规则作用到路由器接口

```
Router(config-if)#exit
Router(config)#int f0/0
Router(config-if)#ip ips al out
Router(config-if)#
*5? 02, 15:24:01.2424:  %IPS-6-ENGINE_BUILDS_STARTED:  15:24:01 UTC 5? 02 2022
*5? 02, 15:24:01.2424:  %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of
*5? 02, 15:24:01.2424:  %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - pack
*5? 02, 15:24:01.2424:  %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
```

图 7 入侵检测系统配置过程四

ip ips al out 是接口配置模式下使用的命令，该命令的作用是将名为 al 的入侵检测规则作用到路由器接口 FastEthernet0/0 的输出方向，out 表示输出方向。

⑤ 重新定义特征

以下命令序列完成两个功能：一是重新配置编号为 2004、子编号为 0 的特征状态；二是重新配置发生事件时的动作。发生事件是指检测到与编号为 2004、子编号为 0 的特征匹配的信息流。

```
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this eng
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms
```

图 8 入侵检测系统配置过程五

ip ips signature-definition 是全局模式下使用的命令，该命令的作用是进入特征定义模式。

signature 2004 0 是特征定义模式下使用的命令，该命令的作用有两个：一是指定编号为 2004、子编号为 0 的特征；二是进入该特征的定义模式，即指定特征定义模式。与编号为 2004、子编号为 0 的特征所匹配的报文是 ICMP ECHO 请求报文。

status 是指定特征定义模式下使用的命令，该命令的作用是进入指定特征状态配置模式。

retired false 是指定特征状态配置模式下使用的命令，该命令的作用是加载指定特征。

enabled true 是指定特征状态配置模式下使用的命令，该命令的作用是启动指定特

征，启动指定特征是指用该特征匹配需要检测入侵行为的信息流。

engine 是指定特征定义模式下使用的命令，该命令的作用是进入指定特征引擎配置模式。

event-action deny-packet-inline 是指定特征引擎配置模式下使用的命令，该命令的作用是将在线丢弃作为对与指定特征匹配的信息流所采取的动作。

event-action produce-alert 是指定特征引擎配置模式下使用的命令，该命令的作用是将发送警告信息作为对与指定特征匹配的信息流所采取的动作。

退出特征定义模式时，会出现提示信息，按 Enter 键确认。

- 3) 验证 PC2 不能 ping 通 PC0，但 PC0 可以 ping 通 PC2。如图 9、10 所示。进行 PC2 ping PC0 的操作后，日志服务器将记录该事件，日志服务器记录的事件如图 11 所示。

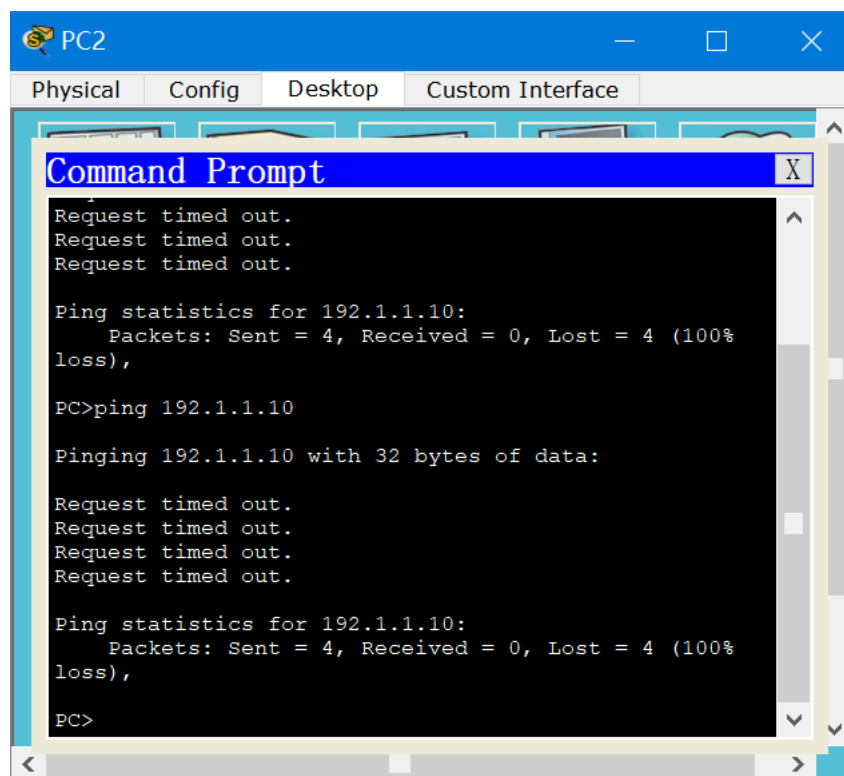


图 9 PC2 不能 ping 通 PC0

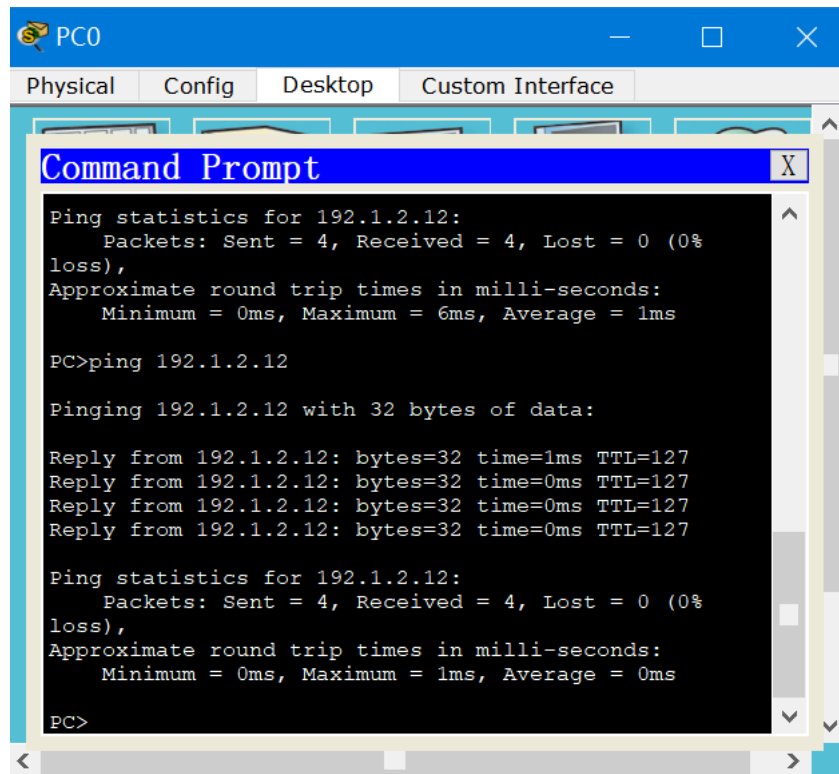


图 10 PC0 可以 ping 通 PC2

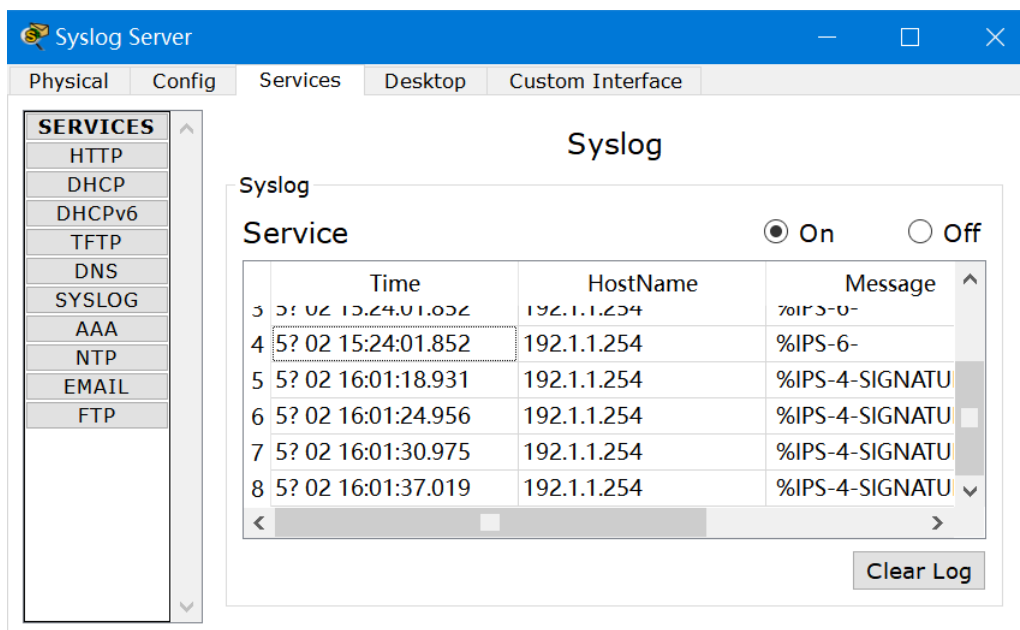


图 11 日志服务器记录的事件

2.入侵检测系统实验二

2.1 实验内容

在图 1 中的路由器 R 接口 1 输出方向设置入侵检测规则，该规则要求，一旦检测到终端 C 发送给终端 A 的 ICMP ECHO 请求报文，则丢弃该 ICMP ECHO 请求报文，并向日志服务器发送警告信息。启动该入侵检测规则后，如果终端 C 发起 ping 终端 A 的操作，则 ping 操作不仅无法完成，而且在日志服务其中记录警告信息，其他终端之间的 ping 操作依然能够正常完成。

2.2 实验目的

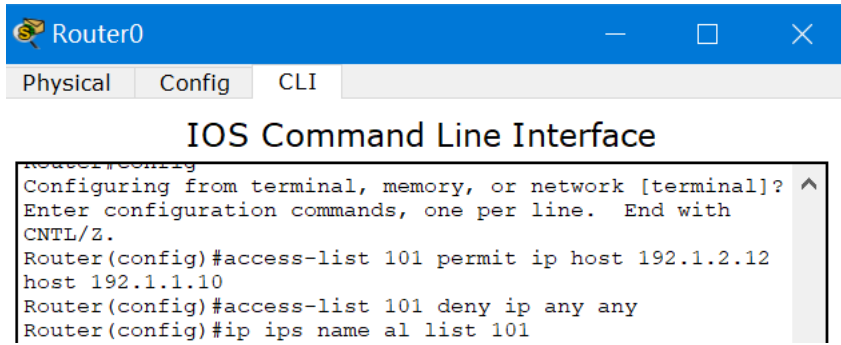
- 1) 验证对特定信息流实施入侵检测的过程。
- 2) 验证指定信息流的入侵检测配置过程。

2.3 实验原理

用扩展分组过滤器指定信息流类别，将用于指定信息流类别的扩展分组过滤器与入侵检测规则绑定在一起。

2.4 实验步骤

在前一个实验的基础上，相关的命令行接口配置过程如图 12。



```
Router0
Physical Config CLI
IOS Command Line Interface
Router(config)#
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#access-list 101 permit ip host 192.1.2.12
host 192.1.1.10
Router(config)#access-list 101 deny ip any any
Router(config)#ip ips name a1 list 101
```

图 12 命令行接口配置过程

编号为 101 的扩展分组过滤器允许继续传输的 IP 分组是源 IP 地址是 PC2 的 IP 地址 192.1.2.12，目的 IP 地址是 PC0 的 IP 地址 192.1.1.10 的 IP 分组。指定名字为 a1 的入侵检测规则时，绑定编号为 101 的扩展分组过滤器，这表示只对编号为 101 的扩展分组过滤器允许继续传输的 IP 分组实施名为 a1 的入侵检测规则，则只对 PC2 发送给 PC0 的 IP 分组实施名为 a1 的入侵检测规则。

验证 PC2 不能 ping 通 PC0，但 PC3 可以 ping 通 PC0。如图 13、14 所示。进行 PC2 ping PC0 的操作后，日志服务器将记录该事件。

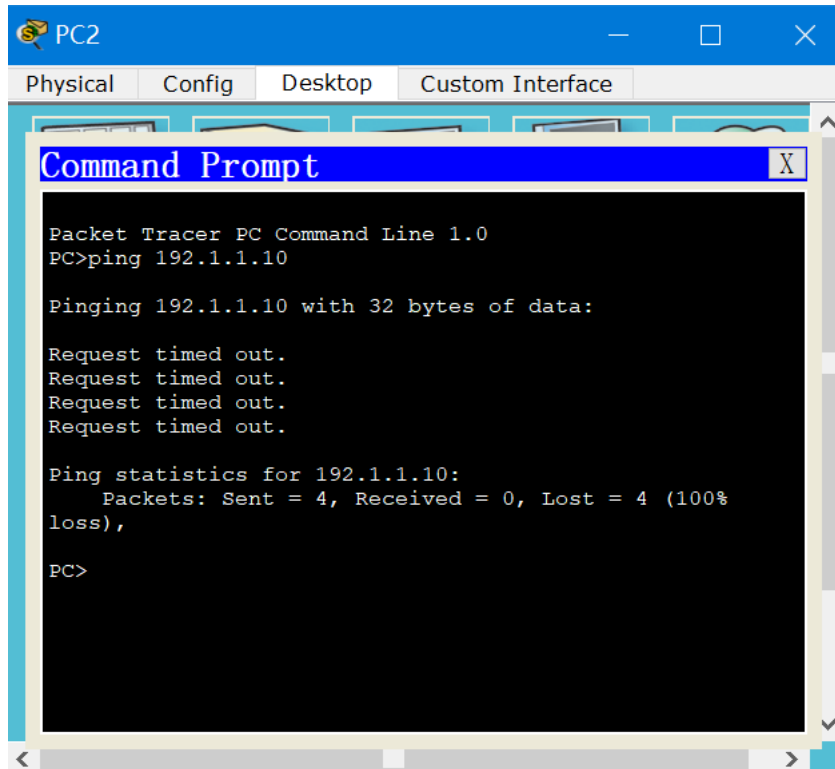


图 13 PC2 不能 ping 通 PC0

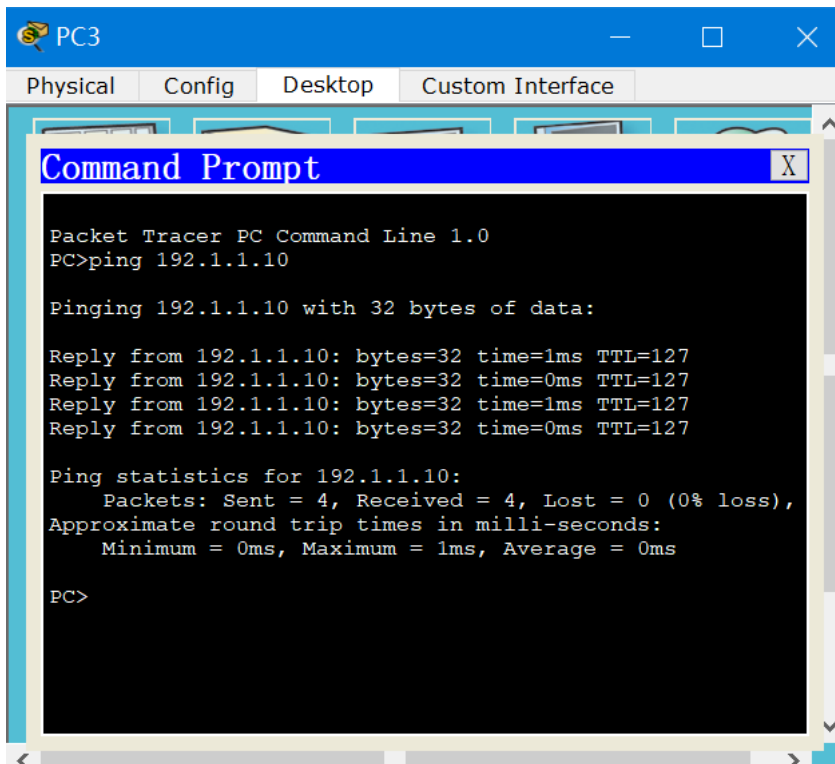


图 14 PC3 可以 ping 通 PC0