苏州大学实验报告

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 院、系 | 计算机科学与技术 | | | 年级专业 | 21计科 | | 姓名 | 方浩楠 | 学号 | 2127405048 |
| 课程名称 | | 计算机网络 | | | | | | | 成绩 |  |
| 指导教师 | | 杨哲 | 同组实验者 | | | 彭光 吴佳骏 方浩楠 赵紫楚 张明明 吴小龙 | | 实验日期 | 2023.12.24 | |

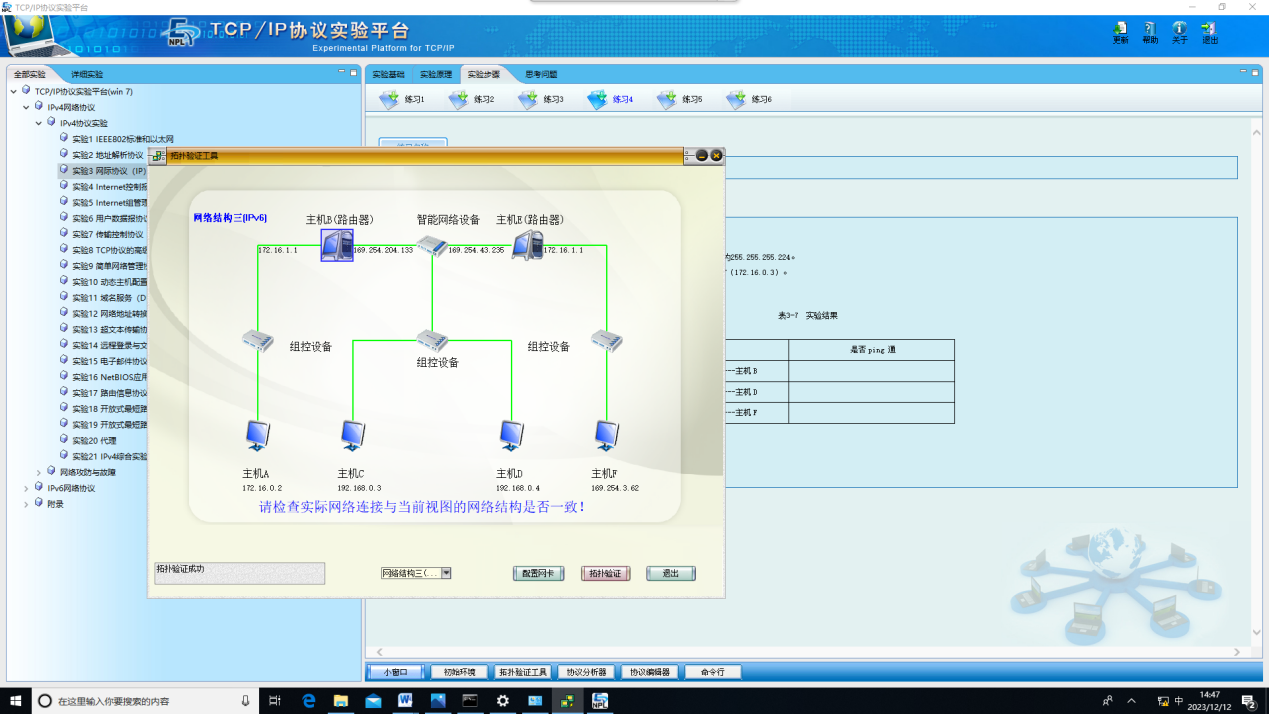
|  |  |
| --- | --- |
| 实 验 名 称 | 实验4：RIP协议 |

1. 实验目的
2. 了解针对RIP协议的攻击方式及原理
3. 理解RIP2的安全属性
4. 增强网络安全意识

二、实验内容

练习一：静态路由与路由表

各主机打开工具区的“拓扑验证工具”，选择相应的网络结构，配置网卡后，进行拓扑验证，如果通过拓扑验证，关闭工具继续进行实验，如果没有通过，请检查网络连接。

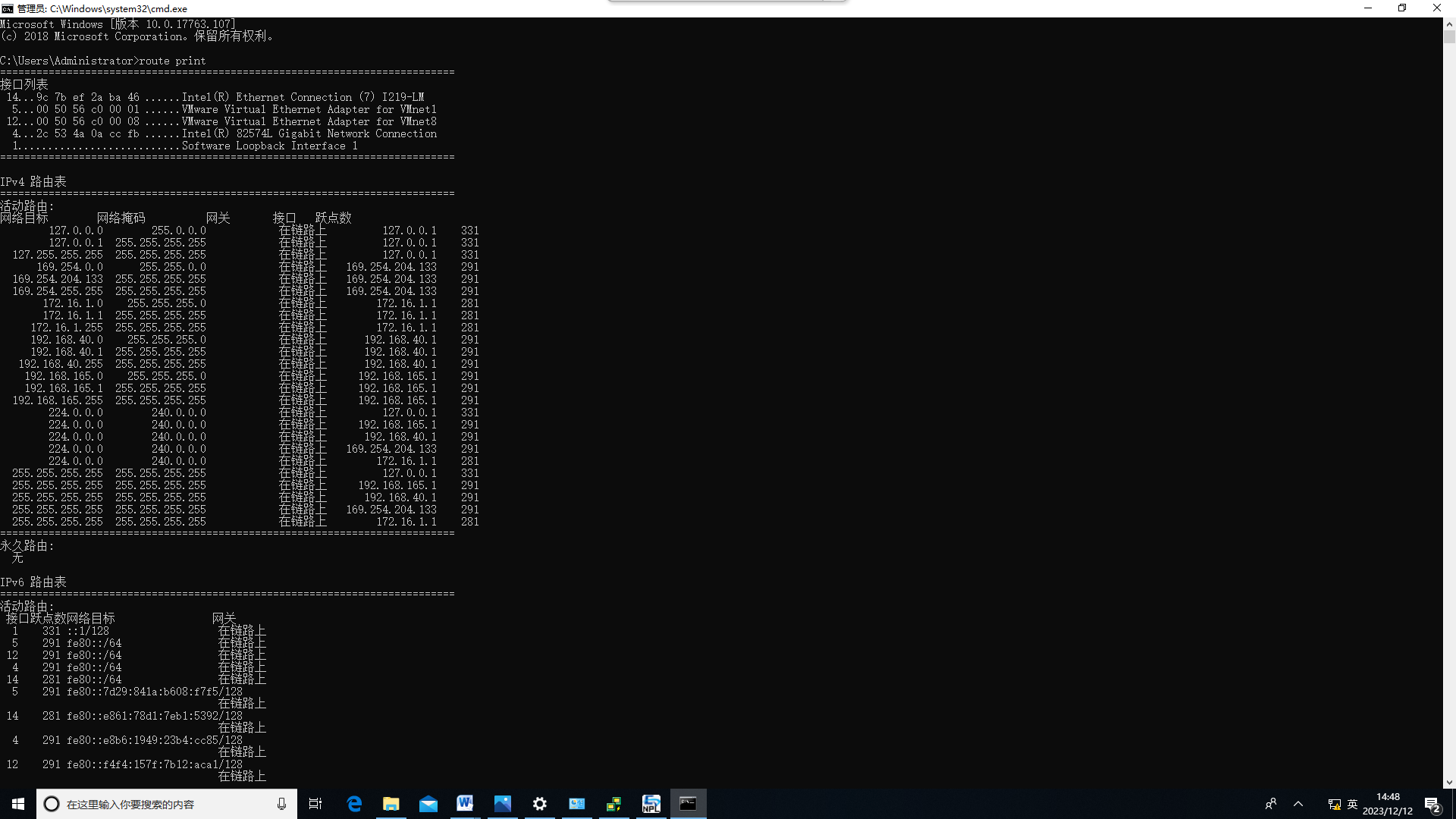


    本练习将主机A、B、C、D、E、F作为一组进行实验。

1.  主机A、B、C、D、E、F在命令行下运行“route print”命令，察看路由表，并回答以下问题：

●  路由表由哪几项组成？

目标网络地址、子网掩码、网关、接口、跃点数

1. 从主机A依次ping 主机B（192.168.0.2）、主机C、主机E（192.168.0.1）、主机E（172.16.1.1），观察现象，记录结果。通过在命令行下运行route print命令，察看主机B和主机E路由表，结合路由信息回答问题：
2. 

●  主机A的默认网关在本次练习中起到什么作用？

本地主机用于向其他IP网络转发IP数据报的IP地址

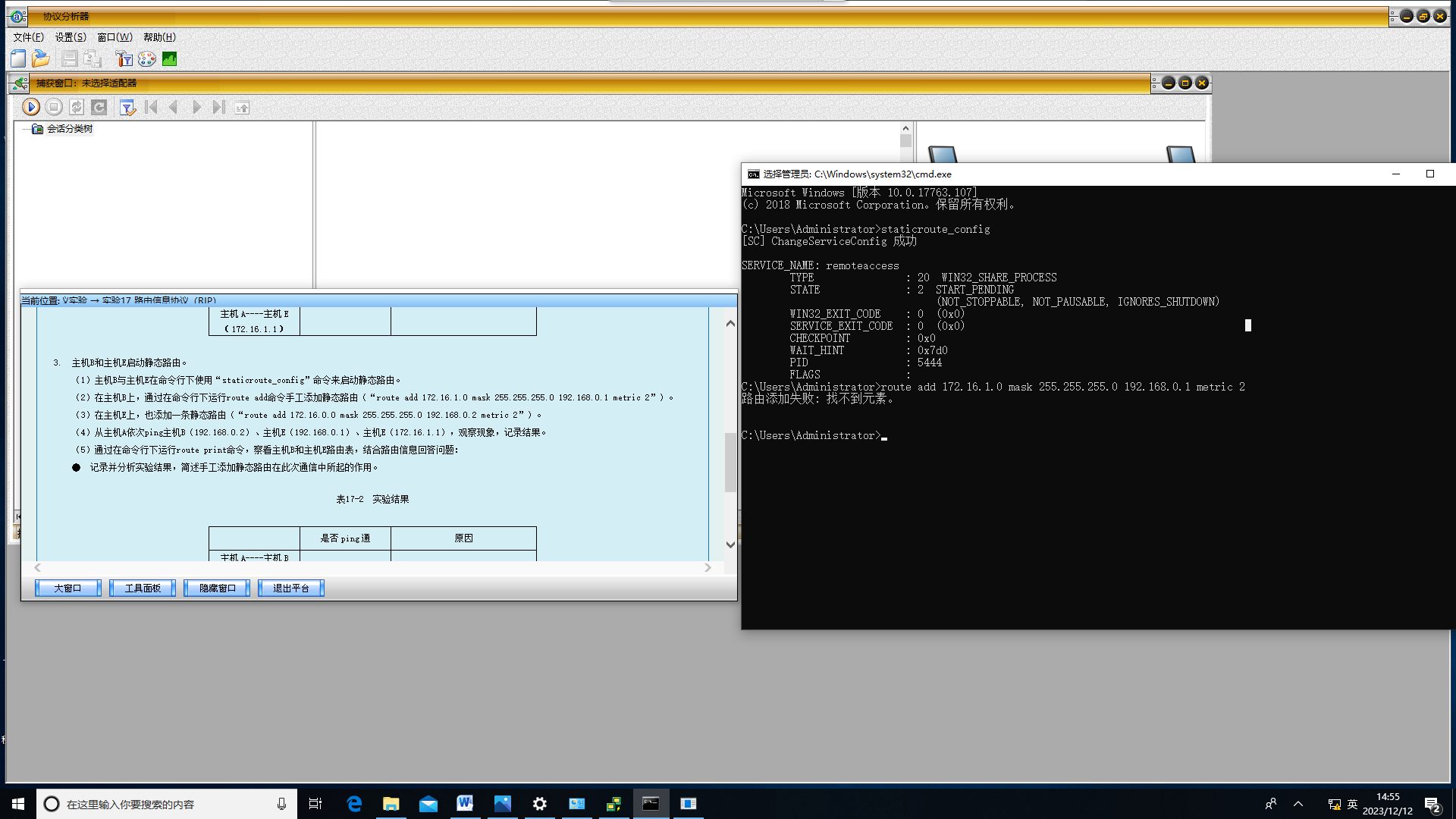
●  记录并分析实验结果，简述为什么会产生这样的结果？

表17-1  实验结果

|  |  |  |
| --- | --- | --- |
|  | 是否ping通 | 原因 |
| 主机A---主机B  （192.168.0.2） | 是 | 默认网关是主机B的一个物理接口地址，而目标地址是主机B的另一个物理接口地址 |
| 主机A---主机C | 否 | 主机B没有路由转发的功能 |
| 主机A---主机E  （192.168.0.1） | 否 | 主机B没有路由转发的功能 |
| 主机A---主机E  （172.16.1.1） | 否 | 主机B没有路由转发的功能 |

3.  主机B和主机E启动静态路由。

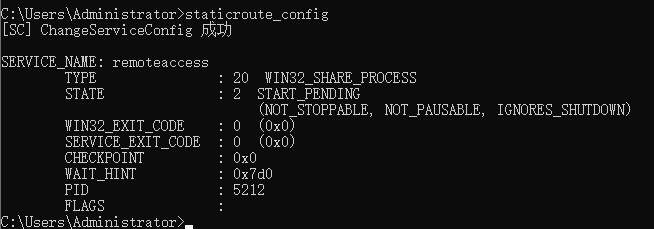
（1）主机B与主机E在命令行下使用“staticroute\_config”命令来启动静态路由。

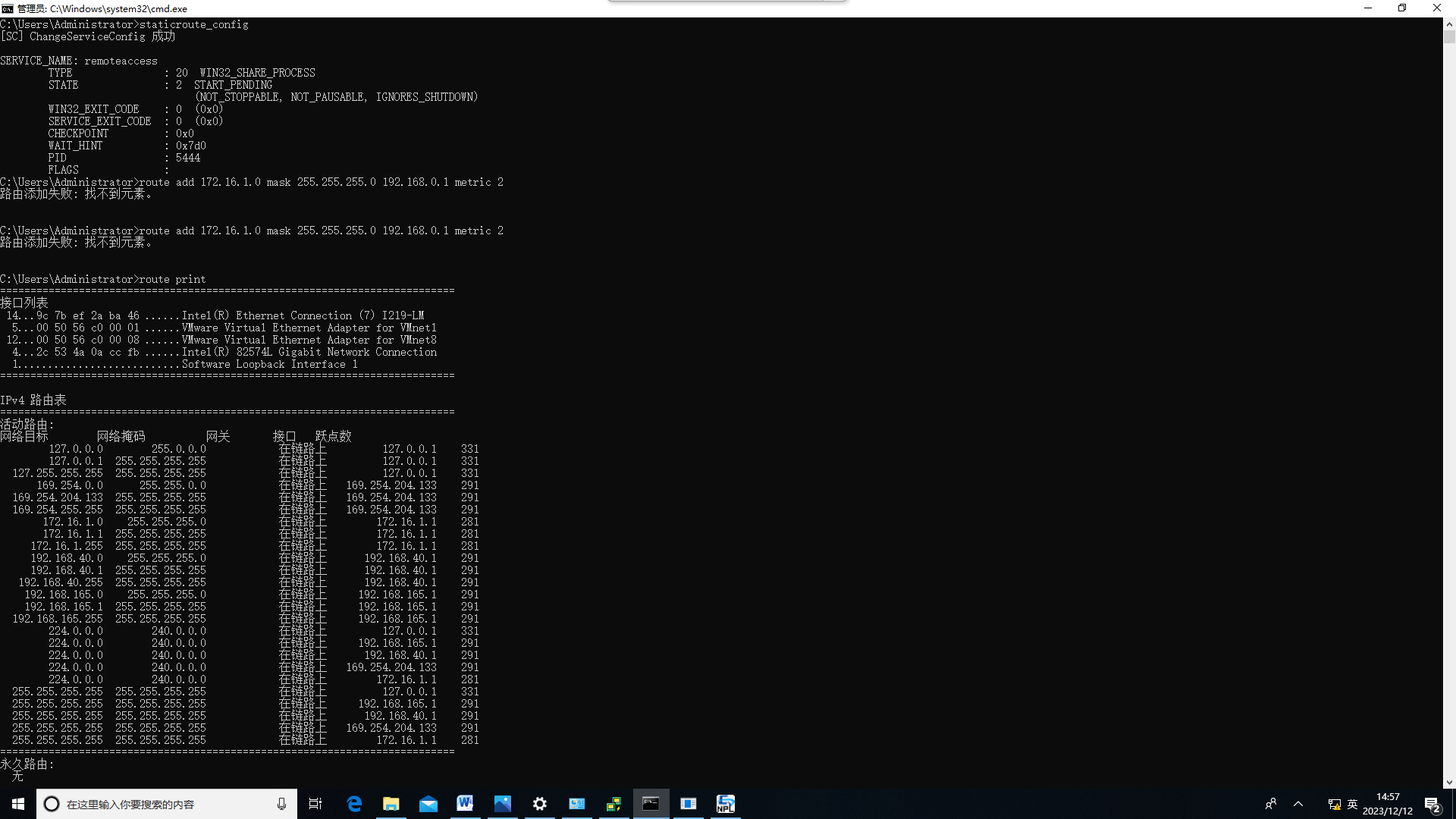


    （2）在主机B上，通过在命令行下运行route add命令手工添加静态路由（“route add 172.16.1.0 mask 255.255.255.0 192.168.0.1 metric 2”）。

    （3）在主机E上，也添加一条静态路由（“route add 172.16.0.0 mask 255.255.255.0 192.168.0.2 metric 2”）。

（4）从主机A依次ping主机B（192.168.0.2）、主机E（192.168.0.1）、主机E（172.16.1.1），观察现象，记录结果。





    （5）通过在命令行下运行route print命令，察看主机B和主机E路由表，结合路由信息回答问题：

    ●  记录并分析实验结果，简述手工添加静态路由在此次通信中所起的作用。

表17-2  实验结果

|  |  |  |
| --- | --- | --- |
|  | 是否ping通 | 原因 |
| 主机A---主机B  （192.168.0.2） | 是 | 默认网关是主机B的一个物理接口地址，而目的地址是主机B的另一个物理接口地址 |
| 主机A---主机E  （192.168.0.1） | 否 | 主机B具有路由转发的功能，并且目标网络在主机B的路由条目中 |
| 主机A---主机E  （172.16.1.1） | 否 | 主机B具有路由转发的功能，并且主机B存在通向172.16.1.0网络的路由条目，主机E存在通向172.16.0.0的路由条目 |

4.  在主机B上，通过在命令行下运行route delete命令（“route delete 172.16.1.0”）；在主机E上，运行route delete命令（“route delete 172.16.0.0”）删除手工添加的静态路由条目。

    ●  简述静态路由的特点以及路由表在路由期间所起到的作用。

静态路由是一种特殊的路由，由网络管理员采用手工方法在路由器中配置而成。这种方法适合在规模较小、路由表也相对简单的网络中使用。他比较简单，容易实现；可以精确控制路由选择，改进网络性能；减小路由器的开销，为重要的应用保证带宽。但杜宇大规模的网络而言，如果网络拓扑结构发生改变或网络链路发生故障，用手工的方法配置及修改路由表，对管理员会形成很大的压力。

练习二：领略动态路由协议RIPv2

各主机打开工具区的“拓扑验证工具”，选择相应的网络结构，配置网卡后，进行拓扑验证，如果通过拓扑验证，关闭工具继续进行实验，如果没有通过，请检查网络连接。

    本练习将主机A、B、C、D、E、F作为一组进行实验。

    注：如果想使用地址本扫描到各个虚拟路由器，那么首先要进入到虚拟路由系统中，执行“zebra -d”和“addrscan”命令。然后使用地址本扫描就可以扫描到虚拟路由器了。

1.在主机A、B、C、D、E、F上启动协议分析器，设置过滤条件（提取RIP和IGMP），开始捕获数据。

2.主机B和主机E启动RIP协议:

(1)主机B和主机E分别开启Ipv4虚拟路由器。

(2)主机B和主机E在Ipv4虚拟路由器内使用“zebra -d”和“ripd -d”命令开启RIP协议。

3.所有主机人员通过协议分析器观察报文交互，直到两台主机的路由表达到稳定态。

●如何判定路由表达到稳定态？

在路由协议的环境中，路由表达到稳定态通常表示网络中的路由信息已经收敛，即各路由器的路由表不再发生变化。在RIPv2协议中，可以通过以下几个条件来判定路由表是否达到稳定态：

定时器不再变化： 在RIPv2中，路由器通过周期性地发送路由更新信息来通知其他路由器。当路由器之间的更新信息不再发生变化，特别是定时器不再计时，可以认为路由表已经达到稳定态。

收敛时间过后： 在RIPv2中，网络中的路由器需要一定时间来学习并更新路由信息，这个时间称为收敛时间。当收敛时间过后，路由表应该已经收敛到一个稳定的状态，不再发生变化。

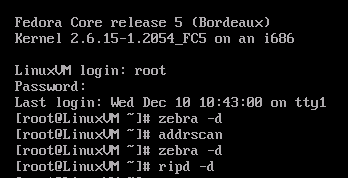
由表不再增加或减少： 当路由表中的路由条目不再增加或减少时，可以认为路由表已经达到稳定态。这意味着路由器已经学习到了网络中所有可达的路由信息，并且不再有新的路由信息进入或离开路由表。

●在主机B、E察看路由表，记录稳定状态下主机B和主机E的路由表条目。

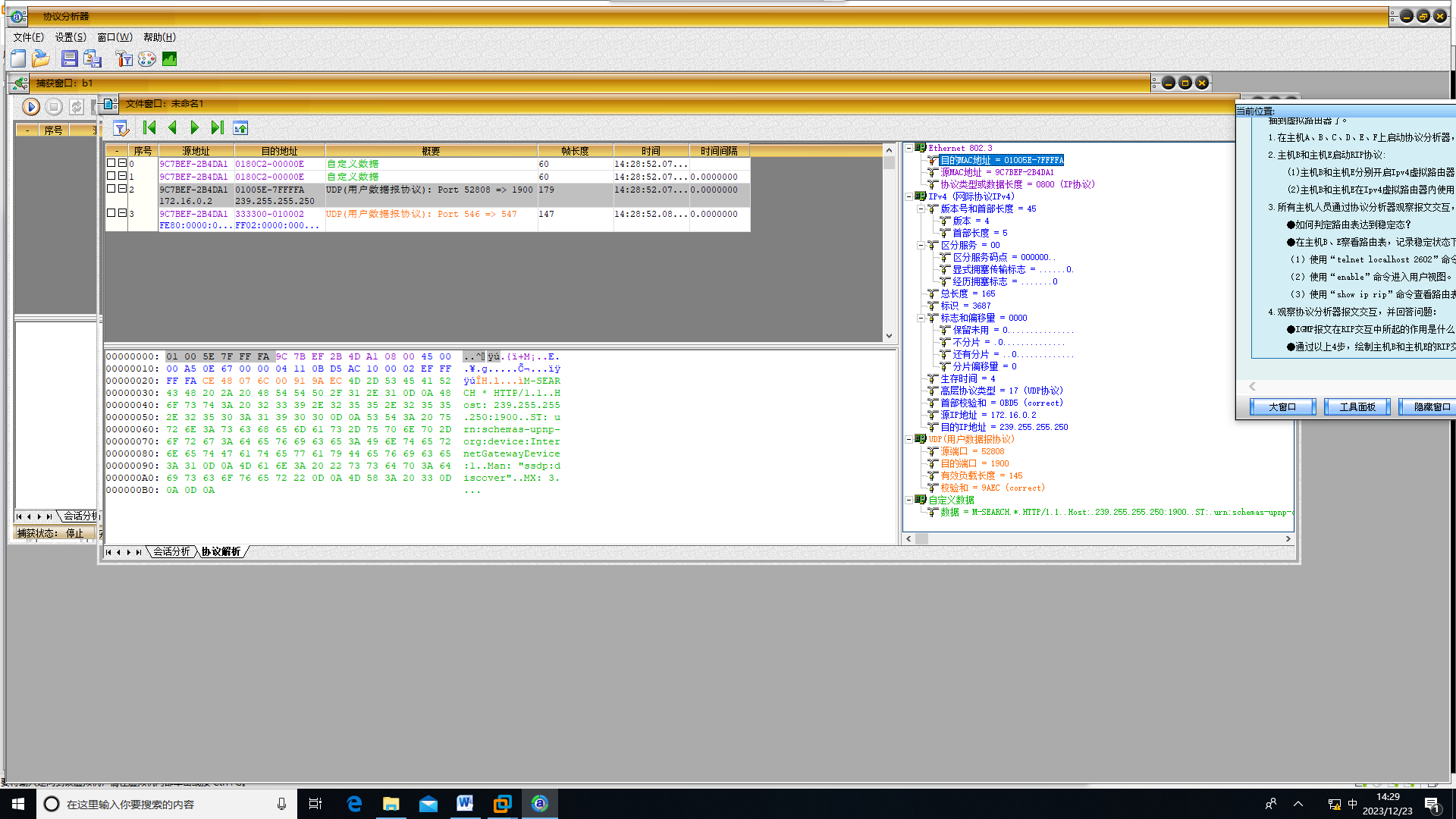
（1）使用“telnet localhost 2602”命令登陆虚拟路由器终端，密码123456。

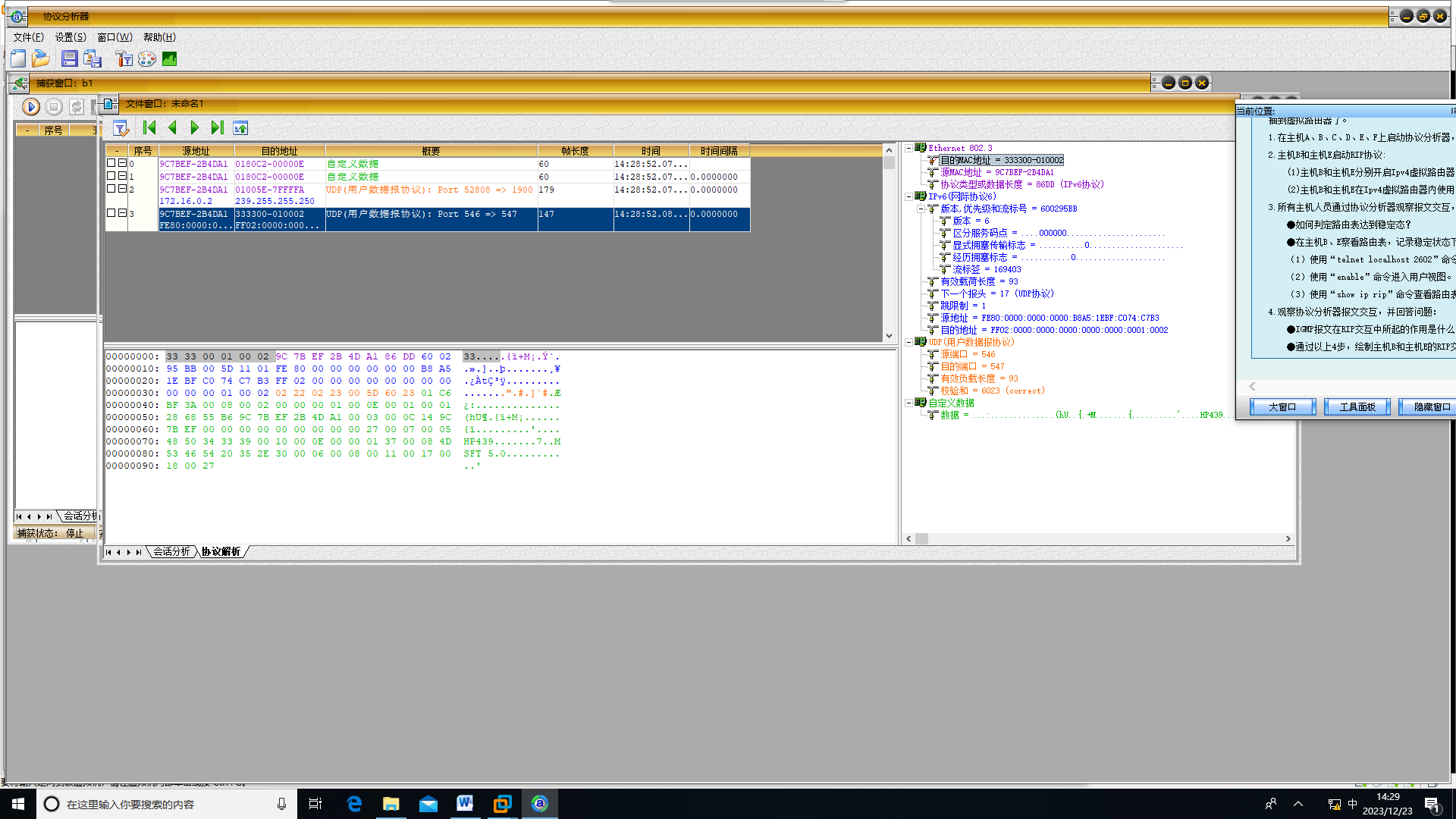
（2）使用“enable”命令进入用户视图。

（3）使用“show ip rip”命令查看路由表。



4.观察协议分析器报文交互，并回答问题：





●IGMP报文在RIP交互中所起的作用是什么？

在RIP（Routing Information Protocol）交互中，IGMP（Internet Group Management Protocol）报文的作用与RIP本身并无直接关联。IGMP主要用于管理和维护IP多播组的成员关系，而RIP则是一种用于路由选择的协议。它们在网络协议栈中处于不同的层次和功能领域。

IGMP主要用于在主机和路由器之间通信，以确定哪些主机对于特定的多播组是成员，以便正确地将多播流量传递给这些成员。它并不直接参与路由表的更新或路由选择的过程。

在RIP中，路由器之间通过RIP协议来交换路由信息，以实现动态路由的更新。RIP报文用于在网络中广播路由信息，以便邻居路由器能够了解到整个网络的路由情况。RIP报文中包含了路由表的信息，例如目的网络的地址、下一跳的路由器地址和跳数等。

综上所述，IGMP和RIP在网络中扮演不同的角色，分别用于处理多播组成员关系和路由信息的传递。在一个网络环境中，可能同时存在IGMP和RIP，但它们之间并不直接互动。

练习三：RIP的计时器

 各主机打开工具区的“拓扑验证工具”，选择相应的网络结构，配置网卡后，进行拓扑验证，如果通过拓扑验证，关闭工具继续进行实验，如果没有通过，请检查网络连接。

    本练习将主机A、B、C、D、E、F作为一组进行实验。

1.在主机A、B、C、D、E、F上重新启动协议分析器，设置过滤条件（提取RIP），开始捕获数据。

注：如果想使用地址本扫描到各个虚拟路由器，那么首先要进入到虚拟路由系统中，执行“zebra -d”和“addrscan”命令。然后使用地址本扫描就可以扫描到虚拟路由器了。

2.主机B和主机E重启RIP协议（同练习二的步骤2、步骤3），使用“configure terminal”命令进入配置视图，同时设置“周期公告间隔”为20秒。

（1）在进入用户视图的基础上，使用“configure terminal”命令进入配置视图。

（2）使用“router rip”命令进入rip协议配置视图。

（3）使用“timer basic 20 180 120”命令设置“周期公告间隔”为20秒。

（4）所有主机人员用协议分析器察看报文序列，并回答问题：

●将“周期公告间隔”设置为0秒可以吗？为什么操作系统对“周期公告间隔”有时间上限和时间下限？上限和下限的作用是什么？

不能。将“周期公告间隔”设置为0秒可能会引发一些问题，因为这意味着路由器将会非常频繁地发送路由更新信息，可能导致网络流量激增和资源消耗。操作系统对“周期公告间隔”设置时间上限和下限的原因是为了平衡路由信息的实时性和网络资源的有效利用。

上限的作用： 避免网络拥塞和资源浪费。如果周期公告间隔设置得太短，路由器将频繁地发送更新信息，导致网络中的路由器和主机处理过多的路由更新，增加了网络流量和处理负担。上限的存在限制了更新信息的发送频率，防止了潜在的网络拥塞。

下限的作用： 确保及时性和故障快速发现。如果周期公告间隔设置得太长，路由器之间更新信息的传递将变得缓慢，导致网络中的路由信息不够实时。较短的间隔可以更迅速地反映网络拓扑的变化，确保路由表及时更新，提高网络的故障快速发现和恢复能力。

●通过协议分析器，比较两个相邻通告报文之间的时间差，是20秒吗？如果不全是，为什么？

不全是

路由器处理时间： 路由器处理RIP信息的时间也会影响通告报文之间的时间差。路由器可能会在接收到更新信息后进行一些处理，这会耗费一些时间。

时钟同步： 如果路由器的时钟没有进行同步，也可能导致时间差的不一致性。

3.将“路由过期前的时间”设置为30秒。

(1) 主机B 在rip协议配置下，输入“timer basic 20 30 120”。

(2) 主机E 在rip协议配置下，输入“timer basic 20 30 120”。

(3)禁用主机E的192.168.0.1的网络连接。在30秒内观察主机B的路由条目变化，并回答问题：

●简述“路由过期计时器”的作用是什么？

过期检测： 路由过期计时器用于监测路由表中的每个路由信息的新鲜度。每当路由器收到关于某个路由的更新信息时，它会重新启动相应路由的过期计时器。如果一段时间内没有收到更新信息，路由过期计时器将会超过设定的阈值。

标记过期路由： 当路由过期计时器超过设定的阈值时，路由器会认为与该路由相关的信息已经过期。此时，该路由信息将被标记为过期，不再被认为是有效的路由信息。

路由信息的删除： 一旦路由信息被标记为过期，路由器可能会采取删除该路由信息的操作。这样做的目的是确保路由表中的信息保持最新，避免使用过期的路由信息导致数据包被错误地发送。

防止使用陈旧路由： 过期计时器的存在可以确保路由表中的信息不会无限期地保持不变，防止网络中的拓扑结构变化后路由表仍然使用过时的路由信息。

4.恢复主机e2的的网络连接。

