**实验四 路由信息协议（RIP）**

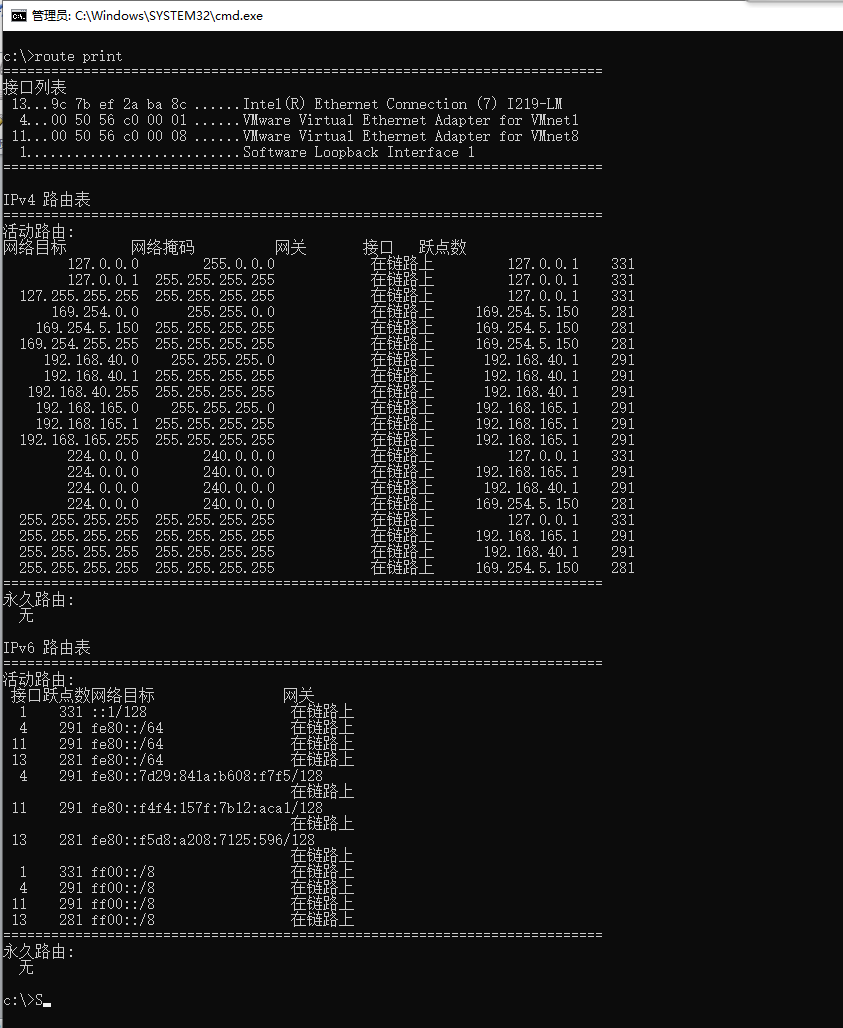
**实验目的**

1. 了解针对RIP协议的攻击方式及原理

2. 理解RIP2的安全属性

3. 增强网络安全意识

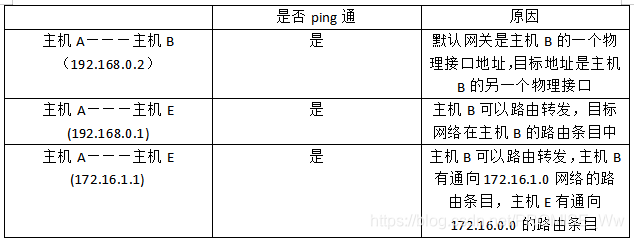
各主机打开工具区的“拓扑验证工具”，选择相应的网络结构，配置网卡后，进行拓扑验证，如果通过拓扑验证，关闭工具继续进行实验，如果没有通过，请检查网络连接。  
    本练习将主机A、B、C、D、E、F作为一组进行实验。  
1.  主机A、B、C、D、E、F在命令行下运行“route print”命令，察看路由表，并回答以下问题：

  
    ●  路由表由哪几项组成？

网络目标；网络掩码；网络地址；接口；跃点数。  
2.  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：  
    ●  主机A的默认网关在本次练习中起到什么作用？

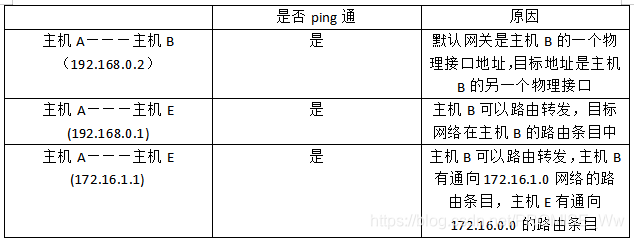
**向其他IP网络转发IP数据报的IP地址。**  
    ●  记录并分析实验结果，简述为什么会产生这样的结果？

是否PING通原因  
主机A—主机B （192.168.0.2） 通 默认网关是主机B的一个物理接口地址，而目标地址作为主机B的另一个物理接口地址。  
主机A—主机C 不通 主机B没有路由转发功能。

表17-1  实验结果

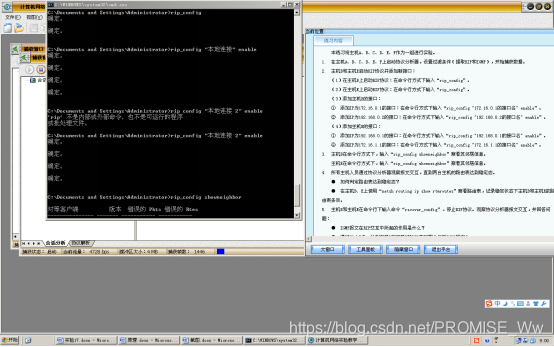
3.  主机B和主机E启动静态路由。  
    （1）主机B与主机E在命令行下使用“staticroute\_config”命令来启动静态路由。  
    （2）在主机B上，通过在命令行下运行route add命令手工添加静态路由（“route add 172.16.1.0 mask 255.255.255.0 192.168.0.1 metric 2”）。  
    （3）在主机E上，也添加一条静态路由（“route add 172.16.0.0 mask 255.255.255.0 192.168.0.2 metric 2”）。  
    （4）从主机A依次ping主机B（192.168.0.2）、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。

增加路由信息。

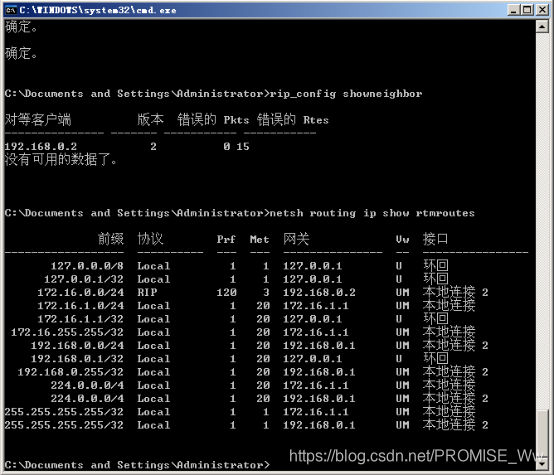
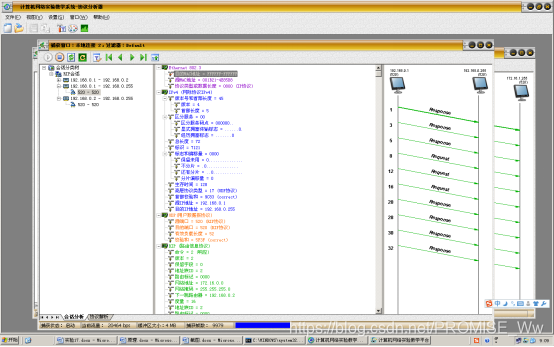
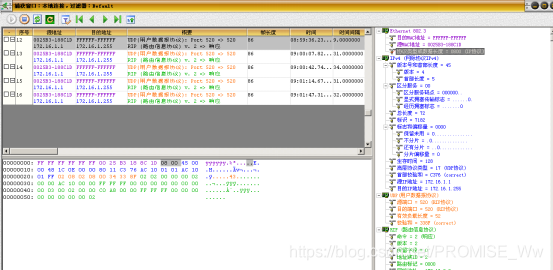
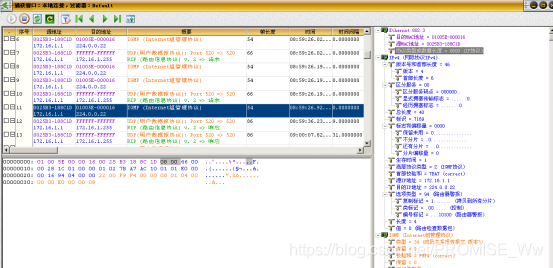
表17-2  实验结果

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。

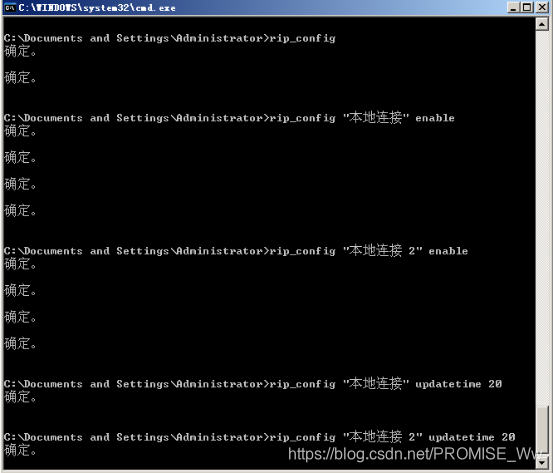
静态路由：一种特殊的路由，由网络管理员手工在路由器中配置的，此方法仅适用于规模小、路由表相对简单的网络中使用。  
 作用：较简单，易实现；可精确控制路由选择，改进网络性能；减少路由器的开销，为重要应用保证带宽。

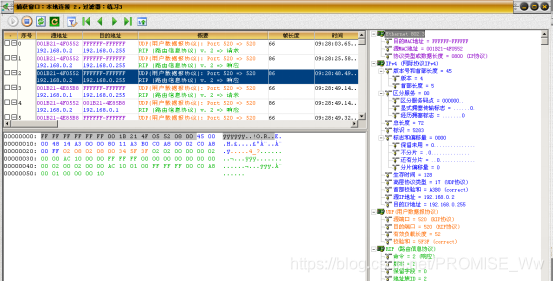
1. 练习2：  
   本练习将主机A、B、C、D、E、F作为一组进行实验。
2. 在主机A、B、C、D、E、F上启动协议分析器，设置过滤条件（提取RIP和IGMP），开始捕获数据。
3. 主机B和主机E启动[RIP协议](https://so.csdn.net/so/search?q=RIP%E5%8D%8F%E8%AE%AE&spm=1001.2101.3001.7020" \t "_blank)并添加新接口：  
   （1）在主机B上启动RIP协议：在命令行方式下输入“rip\_config”。  
   （2）在主机E上启动RIP协议：在命令行方式下输入“rip\_config”。  
   （3）添加主机B的接口：  
   ① 添加IP为172.16.0.1的接口：在命令行方式下输入“rip\_config “172.16.0.1的接口名” enable”。  
   ② 添加IP为192.168.0.2的接口：在命令行方式下输入“rip\_config “192.168.0.2的接口名” enable”。  
   

（4）添加主机E的接口：  
① 添加IP为192.168.0.1的接口：在命令行方式下输入“rip\_config “192.168.0.1的接口名” enable”。  
② 添加IP为172.16.1.1的接口：在命令行方式下输入“rip\_config “172.16.1.1的接口名” enable”。

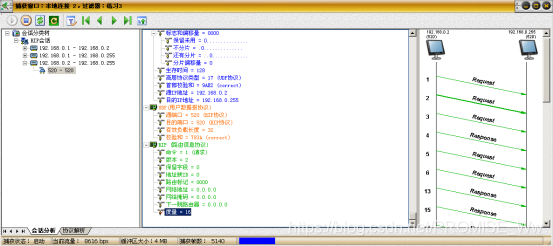
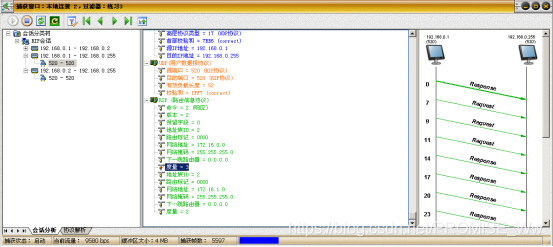
1. 主机B在命令行方式下，输入“rip\_config showneighbor”察看其邻居信息。  
   主机E在命令行方式下，输入“rip\_config showneighbor”察看其邻居信息。  
   
2. 所有主机人员通过协议分析器观察报文交互，直到两台主机的路由表达到稳定态。  
   ● 如何判定路由表达到稳定态？  
   **当主机B的路由条目中出现172.16.1.0网络信息，同时主机E的路由条目中出现172.16.0.0网络信息，则稳定。**  
   ● 在主机B、E上使用“netsh routing ip show rtmroutes”察看路由表，记录稳定状态下主机B和主机E的路由表条目。
3. 主机B和主机E在命令行下输入命令“recover\_config”，停止RIP协议。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？  
   **启动RIP协议的路由器受限使用IGMP组成成员报告报文加入多播组，从而减轻以后RIP交互报文对网络的负载。**  
   ● 通过以上5步，绘制主机B和主机E的RIP交互图（包括IGMP报文）。  
   **1.加入多播组——路由信息请求——路由信息应答；**  
   **2.发送IGMP组成成员报告报文——发送RIP请求报文——发送RIP应答报文。**  
     
     
   

练习3：  
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。
2. 主机B和主机E重启RIP协议并添加新接口（同练习二的步骤2），同时设置“周期公告间隔”为20秒。  
   （1）在主机B命令行方式下，输入“rip\_config “172.16.0.1的接口名” updatetime 20”、“rip\_config “192.168.0.2的接口名” updatetime 20”。  
   （2）在主机E命令行方式下，输入“rip\_config “192.168.0.1的接口名” updatetime 20”、“rip\_config “172.16.1.1的接口名” updatetime 20”。  
   

（3）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？  
**不行。**  
**对“周期公告间隔”有时间限制是对发送更新报文时机的一种权衡。**  
**上限是限制更新报文发送过于频繁，增加网络负载；下限是确保路由信息得到及时更新。**  
● 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？  
**不完全是。**  
**虽指定时间20秒，但工作模式是使用在15—25之间的一个随机数，这是为了避免出现任何可能的同步，从而可以防止在互联网上由于路由器都同时更新而引起的过载。**

1. 将“路由过期前的时间”设置为30秒。  
   （1）在主机B命令行方式下，输入“rip\_config “172.16.0.1的接口名” expiretime 30”、“rip\_config “192.168.0.2的接口名” expiretime 30”。  
   （2）在主机E命令行方式下，输入“rip\_config “192.168.0.1的接口名” expiretime 30”、“rip\_config “172.16.1.1的接口名” expiretime 30”。  
   （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？  
   **管理路由的有效性。若网络出现问题，在分配的时间内没有收到更新报文，则该路由器被认为是过期的，而路由的跳数便为16，表示目的端不可达。**
2. 恢复主机E的192.168.0.1的网络连接。
3. 主机B和主机E在命令行下输入命令“recover\_config”，停止RIP协议。  
   练习4：  
   本练习将主机A、B、C、D、E、F作为一组进行实验。
4. 在主机A、B、C、D、E、F上重新启动协议分析器捕获数据，并设置过滤条件（提取RIP）。
5. 主机B和主机E重启RIP协议并添加新接口（同练习二的步骤2），同时去掉“启用水平分割处理”和“启用毒性反转”选项。  
   （1）主机B在命令行方式下输入“rip\_config “172.16.0.1的接口名” splithorizon disable”、“rip\_config “192.168.0.2的接口名” splithorizon disable”。  
   （2）主机E在命令行方式下输入“rip\_config “192.168.0.1的接口名” splithorizon disable”、“rip\_config “172.16.1.1的接口名” splithorizon disable”。  
   （3）等待一段时间，直到主机B和主机E的路由表达到稳定态。  
   
6. 主机B和主机E在命令行下使用“netsh routing ip show rtmroutes”查看路由表，结合协议分析器上捕获的RIP报文内容，回答问题：  
     
   

● 记录此时主机B和主机E的路由表条目。  
● 同练习二中记录的路由表条目作比较，简述发生变化的原因。  
**增加协议为RIP的172.16.1.路由。**

1. 查看未启用毒性反转的效果。  
   （1）拔掉主机E与主机F相连的网线  
   （2）主机A，主机C查看协议分析器捕获的数据  
   ● 主机A收到度量为16的RIP报文了吗？  
   **无**  
   ● 主机C收到度量为16的RIP报文了吗？  
   **无**
2. 主机B和主机E在命令行下输入“recover\_config”停止RIP协议。  
   思考问题：
3. RIP使用UDP，这样做有何优点？  
   提高速度，节约资源。UDP为较简单协议，开销小；RIP不关心可靠性，因而将其用为下层协议。
4. 跳数限制如何缓解RIP的问题？  
   限制为15，防止分组在网络中兜圈子，用RIP自治系统的直径被限制为15；数值16被认为是无穷大，表示为不可达网络。
5. 试列举RIP的缺点及其相应的补救办法。  
   RIP协议具有不稳定性，通过触发更新，毒性逆转等机制得以缓解；RIP协议使用广播通信，增大了网络压力，RIPv2通过组播通信机制得以缓解。