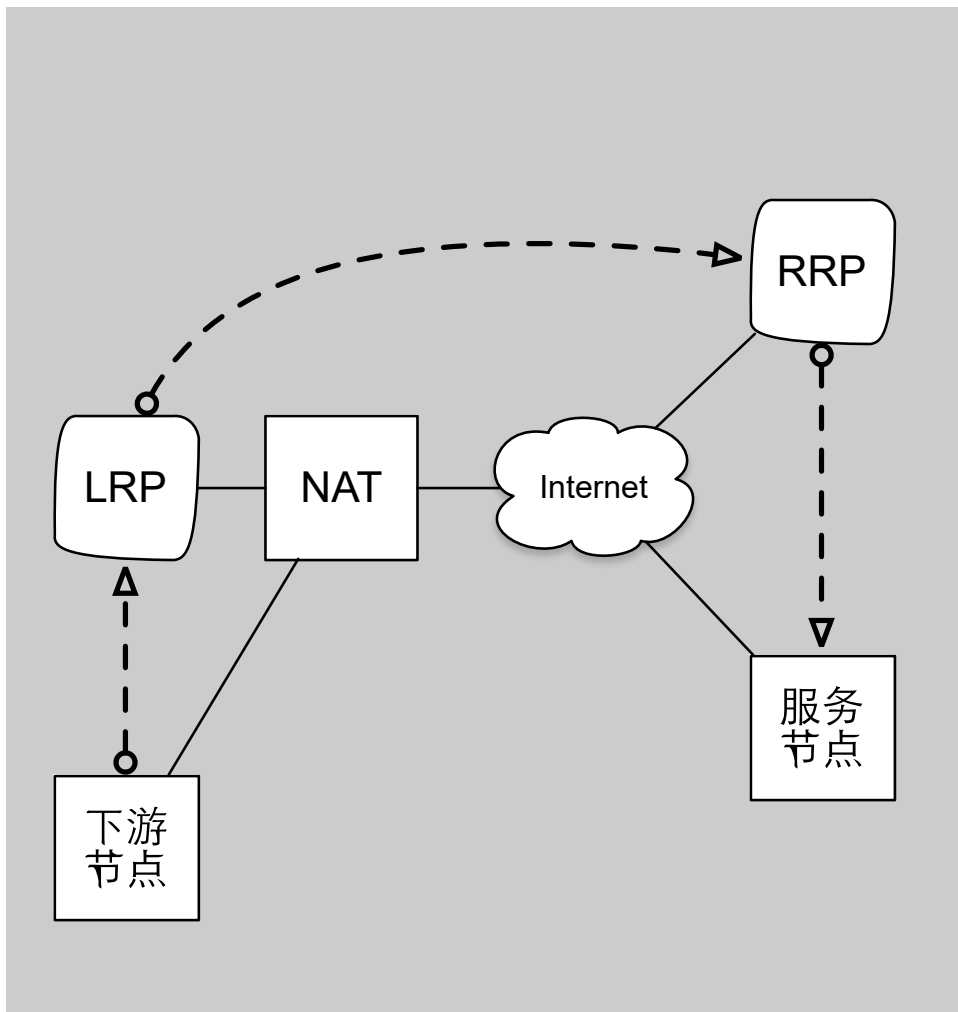
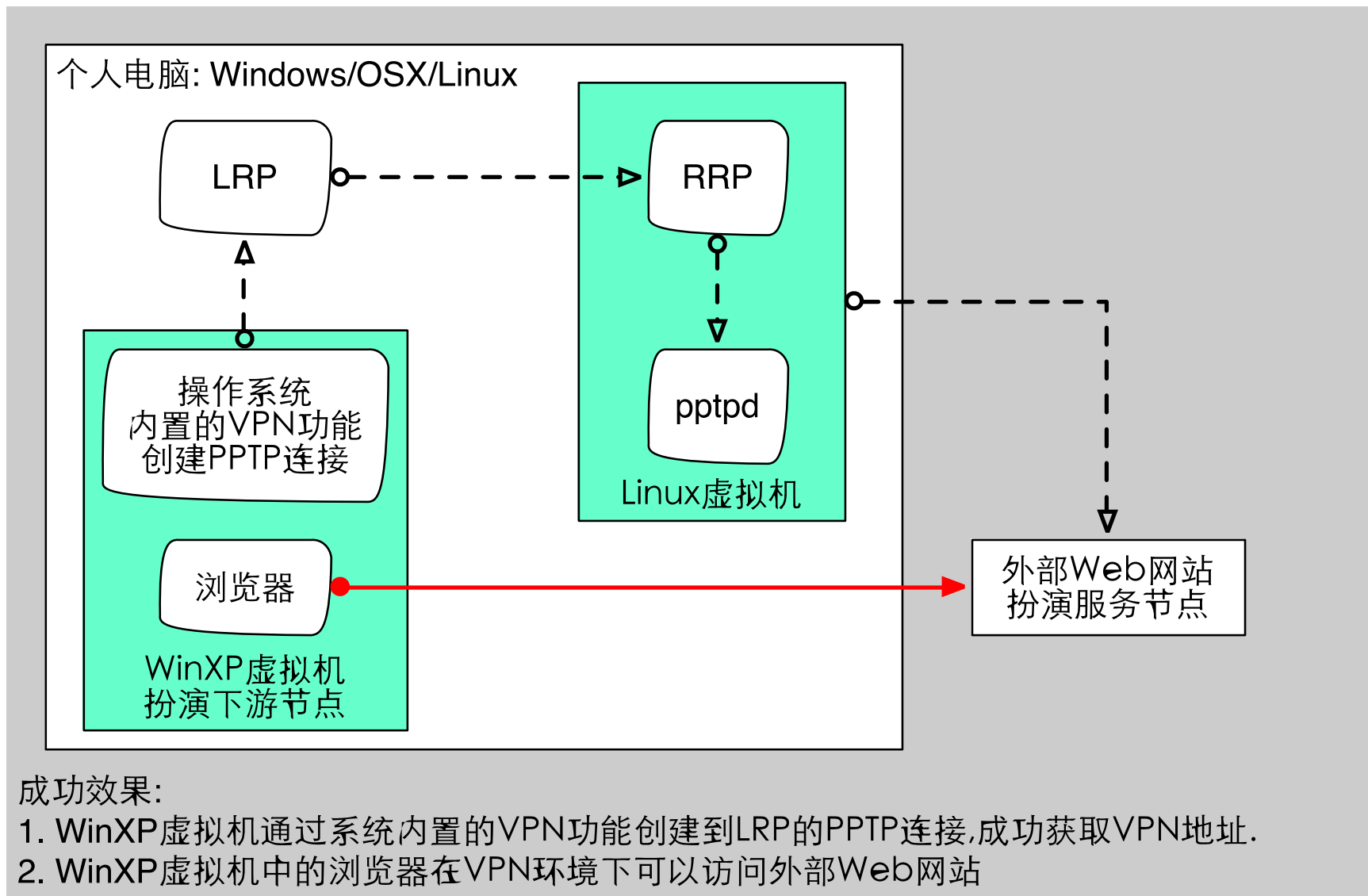


网络工程 Route Proxy 项目要求



- 应用场景
 - 下游节点接入LRP的PPTP访问点, 通过RRP访问服务节点
 - LRP与RRP之间是普通的TCP流量
 - 下游节点: 电脑或其他智能终端
 - 服务节点: 即任意网站或其他
- NAT
 - 网络地址转换器, 即常见的路由器
 - NAT无法感知PPTP的存在
- LRP: Local Route Proxy
 - 支持下游节点的PPTP接入
 - PPTP协议要求
 - 监听TCP 1723端口
 - 收发GRE报文
- RRP: Remote Route Proxy
 - 支持下游的LRP接入
 - 监听TCP指定端口
 - 支持上游PPTP服务器
 - 连接TCP 1723端口
 - 收发GRE报文

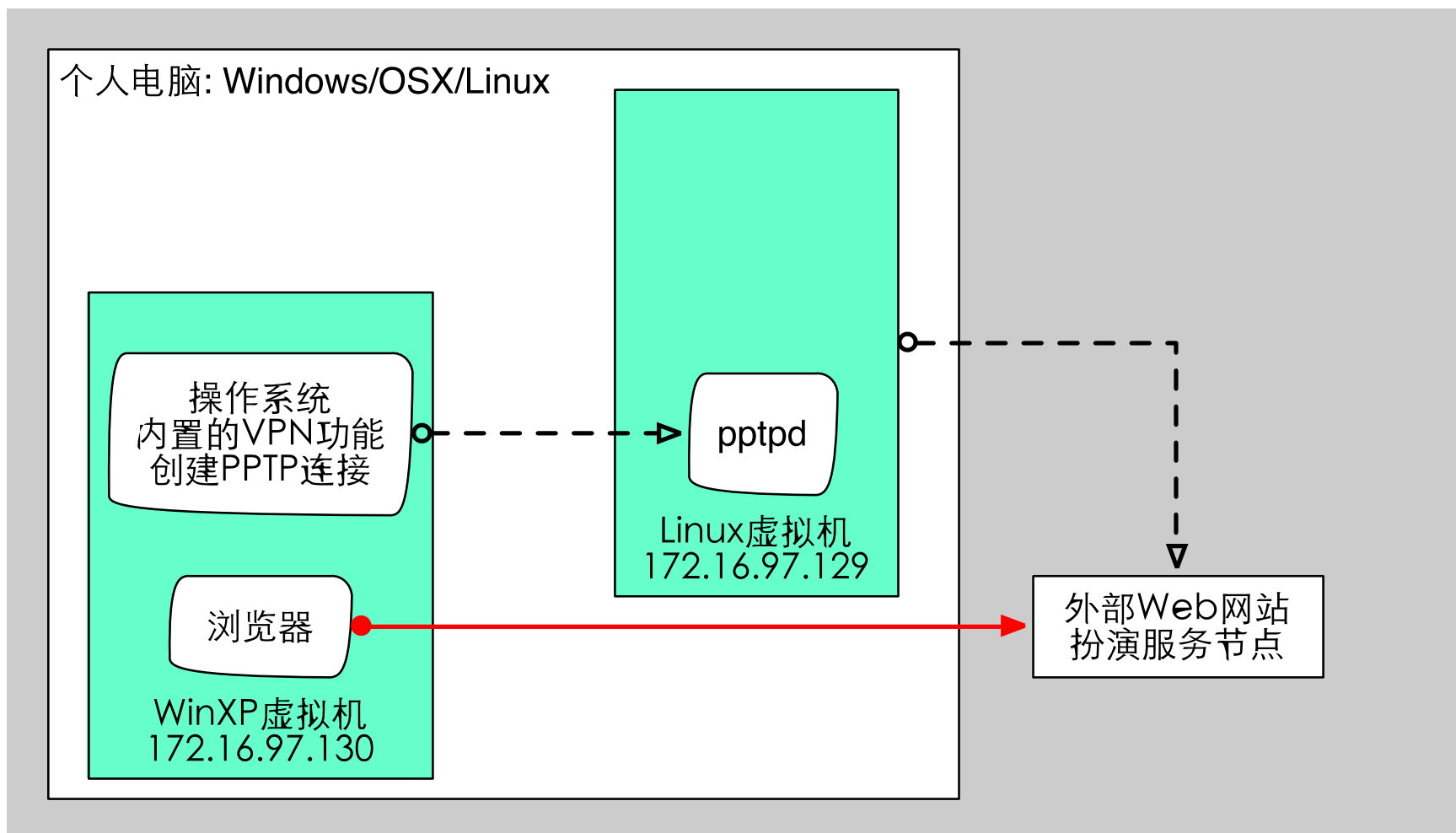
网络工程Route Proxy 参考环境



网络工程Route Proxy 参考思路

- 协议处理
 - TCP需要分析RFC2637的PPTP控制协议获取Call ID等会话标识
 - GRE报文如何绕开NAT,一般操作系统无法调用TCP类型的Raw Socket的收发,所以还是需要采用Pcap作为LRP与RRP之间的GRE转发,即: 下游节点 \longleftrightarrow LRP \longleftrightarrow RRP \longleftrightarrow pptpd
- LRP
 - TCP采用Qt/QTcpSocket
 - 服务器QTcpServer面向下游节点
 - 客户端QTcpSocket面向RRP
 - GRE报文收发采用Pcap
 - Linux/OSX: <http://www.tcpdump.org/pcap.html>
 - Windows: <http://www.winpcap.org>
 - Win10采用Win10Pcap: <http://www.win10pcap.org>
- RRP
 - 方案1
 - RRP作为独立程序采用PPTP方式连接普通的pptpd
 - 同样要完成TCP服务器+GRE报文转发
 - 潜在问题: 在同一主机上是否会影响pptpd对GRE在127.0.0.1地址上的收发
 - 方案2
 - RRP融入到pptpd程序直接支持LRP接入
 - 需要修改Poptop源码
- 开发语言
 - 没有限制可以采用C/C++/Python或其他任何语言

验证标准的PPTP环境



实验pptpVerify: PPTP协议验证

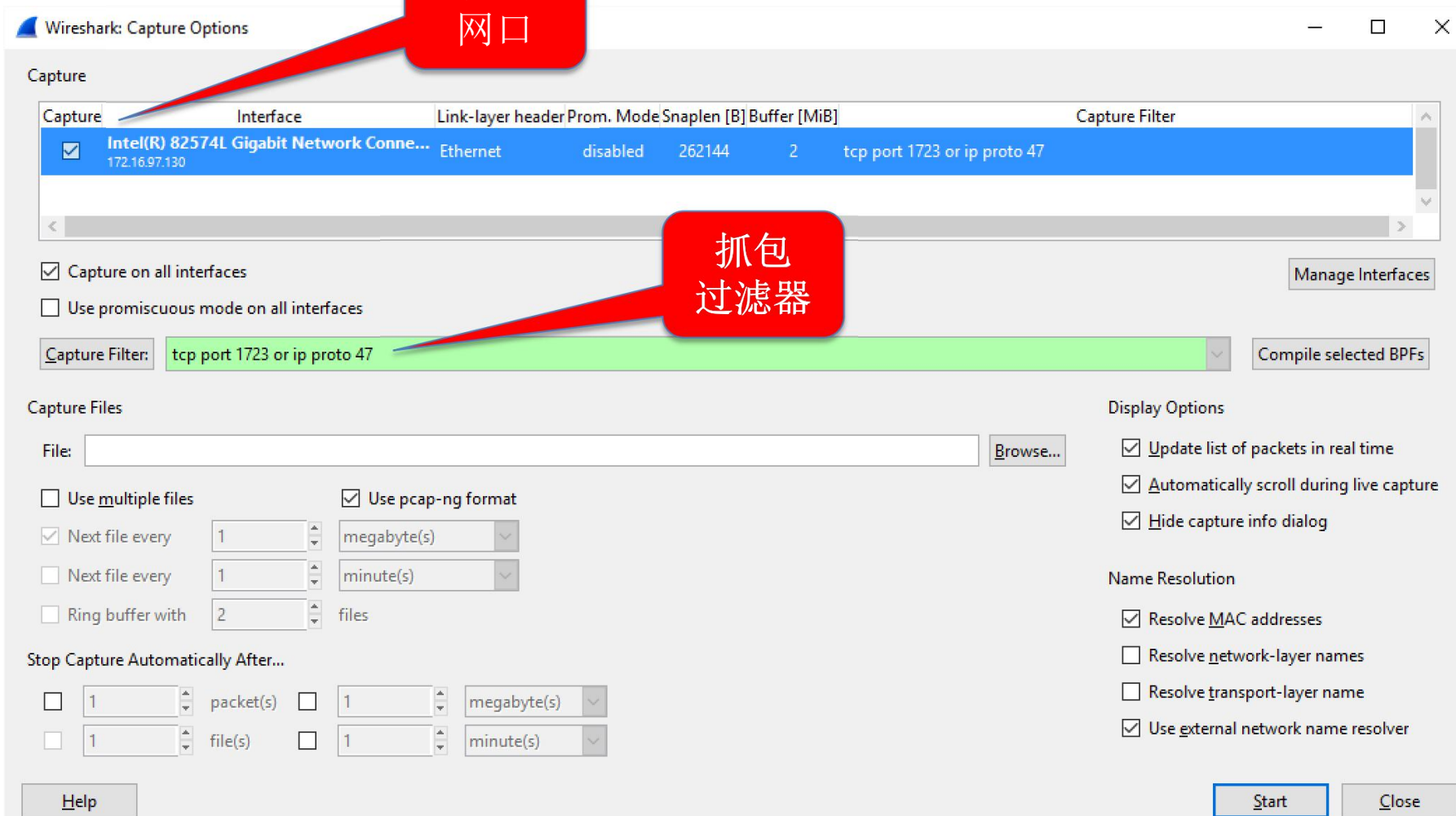
- 提交邮箱: buptne@gmail.com
- 邮件标题: pptpVerify-班级-学号-姓名
- 邮件正文: 报告粘贴到正文（**不要使用附件**）
- 提交时间: 2017年3月16日
- 报告内容: 描述PPTP协议验证的过程

在Linux虚拟机上安装PPTP服务器

- 安装虚拟机软件
 - Windows/Linux: VMware workstation
 - OSX: VMware Fusion
- 安装PPTP服务器
 - 在虚拟机上安装Ubuntu 14.04
 - 登录Ubuntu后
 - 执行命令`apt-get install pptpd` 安装PPTP服务器软件
 - 编辑文件`/etc/pptpd.conf` 定义PPTP动态分配的地址池从192.168.77.10到254
 - `localip 192.168.77.1`
 - `remoteip 192.168.77.10-254`
 - 编辑文件`/etc/ppp/chap-secrets` 定义PPTP认证所用的账号和密码,如:账号u1的密码为passwd1
 - `u1 pptpd passwd1 *`
 - `u2 pptpd passwd2 *`
 - 编辑文件`/etc/ppp/pptpd-options` 定义给Windows客户端使用的DNS服务器地址
 - `ms-dns 10.3.9.4`
 - `ms-dns 10.3.9.5`
 - 执行命令`service pptpd restart` 启动PPTP服务器
 - 编辑文件`/etc/sysctl.conf` 启用IPv4报文转发
 - `net.ipv4.ip_forward=1`
 - 执行命令`sysctl -p`
 - 执行命令`iptables -t nat -A POSTROUTING -s 192.168.77.0/24 -o eth0 -j MASQUERADE` 启用NAT
 - 执行命令`iptables-save`

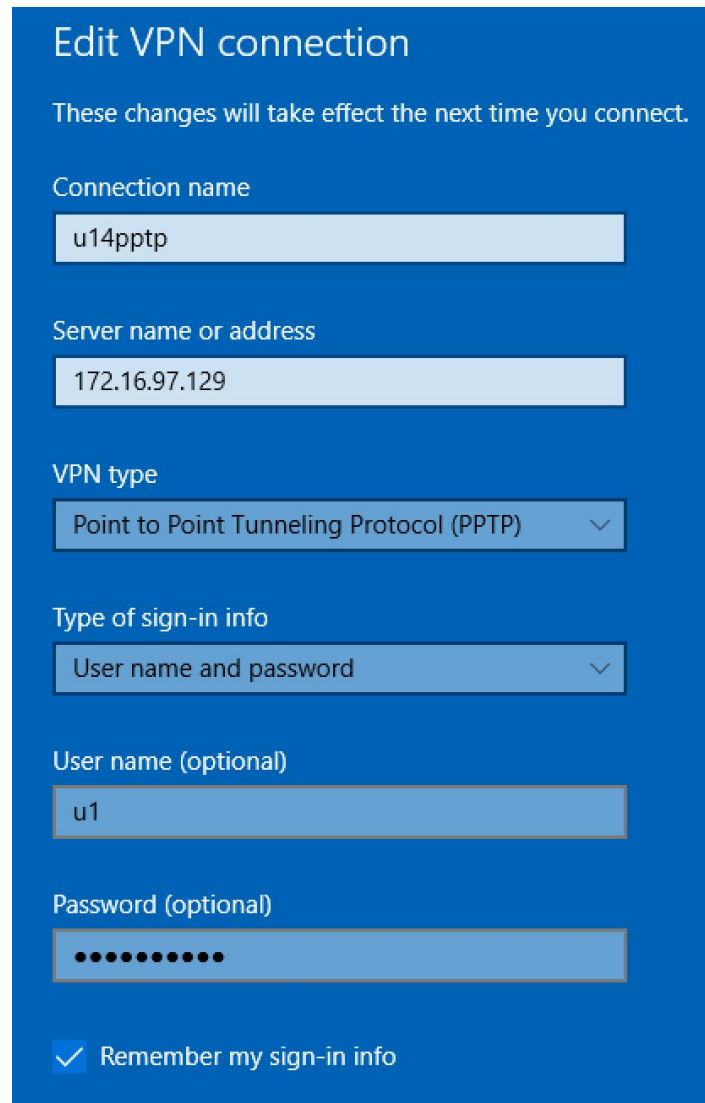
WinXP虚拟机上安装WinPcap和Wireshar

抓包
网口



在WinXP虚拟机上测试PPTP拨号

- 右侧是Win10举例
- Connection Name 随意取
- Server name:172.16.97.129 Linux虚拟机地址
- VPN type: PPTP
- User name: u1
对应Linux虚拟机中/etc/ppp/chap-secrets
- Password: passwd1
对应Linux虚拟机中/etc/ppp/chap-secrets



The image shows a Windows 'Edit VPN connection' dialog box with a blue background. It contains several input fields and dropdown menus for configuring a VPN connection. The fields are filled with the following values: Connection name: u14pptp, Server name or address: 172.16.97.129, VPN type: Point to Point Tunneling Protocol (PPTP), Type of sign-in info: User name and password, User name (optional): u1, Password (optional): passwd1 (masked with dots). At the bottom, there is a checked checkbox labeled 'Remember my sign-in info'.

Edit VPN connection

These changes will take effect the next time you connect.

Connection name

u14pptp

Server name or address

172.16.97.129

VPN type

Point to Point Tunneling Protocol (PPTP)

Type of sign-in info

User name and password

User name (optional)

u1

Password (optional)

.....

☒ Remember my sign-in info

显示
过滤器

验证PPTP与GRE对应关系

PPTP消息中的Call ID和Peer Call ID

Filter: pptp

Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
4	0.001474	172.16.97.130	172.16.97.129	PPTP	210	Start-Control-Connection-Request
6	0.002717	172.16.97.129	172.16.97.130	PPTP	210	Start-Control-Connection-Reply
7	0.002769	172.16.97.130	172.16.97.129	PPTP	222	Outgoing-Call-Request
8	0.005564	172.16.97.129	172.16.97.130	PPTP	86	Outgoing-Call-Reply
9	0.013695	172.16.97.130	172.16.97.129	PPTP	78	Set-Link-Info
37	0.052713	172.16.97.130	172.16.97.129	PPTP	78	Set-Link-Info
159	9.787766	172.16.97.130	172.16.97.129	PPTP	78	Set-Link-Info
163	9.829871	172.16.97.130	172.16.97.129	PPTP	70	Call-Clear-Request

⊕ Frame 8: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0

⊕ Ethernet II, Src: Vmware_69:da:4d (00:0c:29:69:da:4d), Dst: Vmware_24:4a:84 (00:0c:29:24:4a:84)

⊕ Internet Protocol Version 4, Src: 172.16.97.129, Dst: 172.16.97.130

⊕ Transmission Control Protocol, Src Port: 1723 (1723), Dst Port: 50039 (50039), Seq: 157, Ack: 325, Len: 32

⊖ Point-to-Point Tunneling Protocol

Length: 32

Message type: Control Message (1)

Magic cookie: 0x1a2b3c4d (correct)

Control Message Type: Outgoing-Call-Reply (8)

Reserved: 0000

Call ID: 256

Peer Call ID: 57982

Result code: Connected (1)

Error Code: None (0)

Cause Code: 0

Connect Speed: 100000000

Packet Receive Window Size: 64

Packet Processing Delay: 0

Physical Channel ID: 0

Call ID
Peer Call ID

验证PPTP与GRE对应关系

GRE消息中的Call ID: WinXP → Linux

Filter:	gre	▼	Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info
10	0.015287	172.16.97.130	172.16.97.129	PPP LCP	71	Configuration Request
11	0.016571	172.16.97.129	172.16.97.130	PPP LCP	75	Configuration Request
12	0.016695	172.16.97.130	172.16.97.129	PPP LCP	79	Configuration Ack
13	0.018556	172.16.97.129	172.16.97.130	PPP LCP	61	Configuration Reject
14	0.018693	172.16.97.130	172.16.97.129	PPP LCP	72	Configuration Request
15	0.019655	172.16.97.129	172.16.97.130	PPP LCP	72	Configuration Ack
16	0.019656	172.16.97.129	172.16.97.130	PPP LCP	60	Echo Request
17	0.019864	172.16.97.129	172.16.97.130	PPP CHAP	74	Challenge (NAME='pptpd',
18	0.020232	172.16.97.130	172.16.97.129	PPP LCP	70	Identification
19	0.020481	172.16.97.130	172.16.97.129	PPP LCP	79	Identification
20	0.020780	172.16.97.130	172.16.97.129	PPP LCP	72	Identification
21	0.022957	172.16.97.130	172.16.97.129	PPP LCP	56	Echo Reply
22	0.028219	172.16.97.130	172.16.97.129	PPP CHAP	104	Response (NAME='u1', VAL
23	0.029618	172.16.97.129	172.16.97.130	PPP CHAP	115	Success (MESSAGE='S=FR14
+ Frame 12: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0						
+ Ethernet II, Src: Vmware_24:4a:84 (00:0c:29:24:4a:84), Dst: Vmware_69:da:4d (00:0c:29:69:da:4d)						
+ Internet Protocol Version 4, Src: 172.16.97.130, Dst: 172.16.97.129						
- Generic Routing Encapsulation (PPP)						
+ Flags and Version: 0x3081						
Protocol Type: PPP (0x880b)						
Payload Length: 29						
Call ID: 256						
Sequence Number: 1						
Acknowledgment Number: 0						
+ Point-to-Point Protocol						
+ PPP Link Control Protocol						

Call ID

验证PPTP与GRE对应关系

GRE消息中的Call ID: Linux → WinXP

Filter:	gre	▼	Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info
10	0.015287	172.16.97.130	172.16.97.129	PPP LCP	71	Configuration Request
11	0.016571	172.16.97.129	172.16.97.130	PPP LCP	75	Configuration Request
12	0.016695	172.16.97.130	172.16.97.129	PPP LCP	79	Configuration Ack
13	0.018556	172.16.97.129	172.16.97.130	PPP LCP	61	Configuration Reject
14	0.018693	172.16.97.130	172.16.97.129	PPP LCP	72	Configuration Request
15	0.019655	172.16.97.129	172.16.97.130	PPP LCP	72	Configuration Ack
16	0.019656	172.16.97.129	172.16.97.130	PPP LCP	60	Echo Request
17	0.019864	172.16.97.129	172.16.97.130	PPP CHAP	74	Challenge (NAME='pptpd')
18	0.020232	172.16.97.130	172.16.97.129	PPP LCP	70	Identification
19	0.020481	172.16.97.130	172.16.97.129	PPP LCP	79	Identification
20	0.020780	172.16.97.130	172.16.97.129	PPP LCP	72	Identification
21	0.022957	172.16.97.130	172.16.97.129	PPP LCP	56	Echo Reply
22	0.028219	172.16.97.130	172.16.97.129	PPP CHAP	104	Response (NAME='u1', VA
23	0.029618	172.16.97.129	172.16.97.130	PPP CHAP	115	Success (MESSAGE='S=F31
+ Frame 13: 61 bytes on wire (488 bits), 61 bytes captured (488 bits) on interface 0						
+ Ethernet II, Src: Vmware_69:da:4d (00:0c:29:69:da:4d), Dst: Vmware_24:4a:84 (00:0c:29:24:4a:84)						
+ Internet Protocol Version 4, Src: 172.16.97.129, Dst: 172.16.97.130						
+ Generic Routing Encapsulation (PPP)						
+ Flags and Version: 0x3081						
Protocol Type: PPP (0x880b)						
Payload Length: 11						
Call ID: 57982						
Sequence Number: 1						
Acknowledgment Number: 0						
+ Point-to-Point Protocol						
+ PPP Link Control Protocol						

Call ID

PPTP协议验证结论

- PPTP控制消息(即TCP 1723收发)
 - Call ID
 - Peer Call ID
 - 两个方向上分别代表各自对Call ID的分配
- PPTP数据报文(即GRE报文)
 - GRE的Call ID字段
- LRP程序只需要处理以上3个字段的转换
- 理论上Route Proxy是可行的