抓包基本介绍

为了更好地、快速地定位网络问题，降低维护成本，可以通过抓包对报文进行分析。本文档主要介绍ERG2、ERG3、MER、MSR型号产品为例，以谷歌浏览器登录设备的WEB页面为例（不同浏览器，页面显示可能存在差异），分别进行说明。常见的抓包文件是wireshark（可自行网页下载安装）。

**一、WEB页面抓包配置**：

**ERG2产品**：

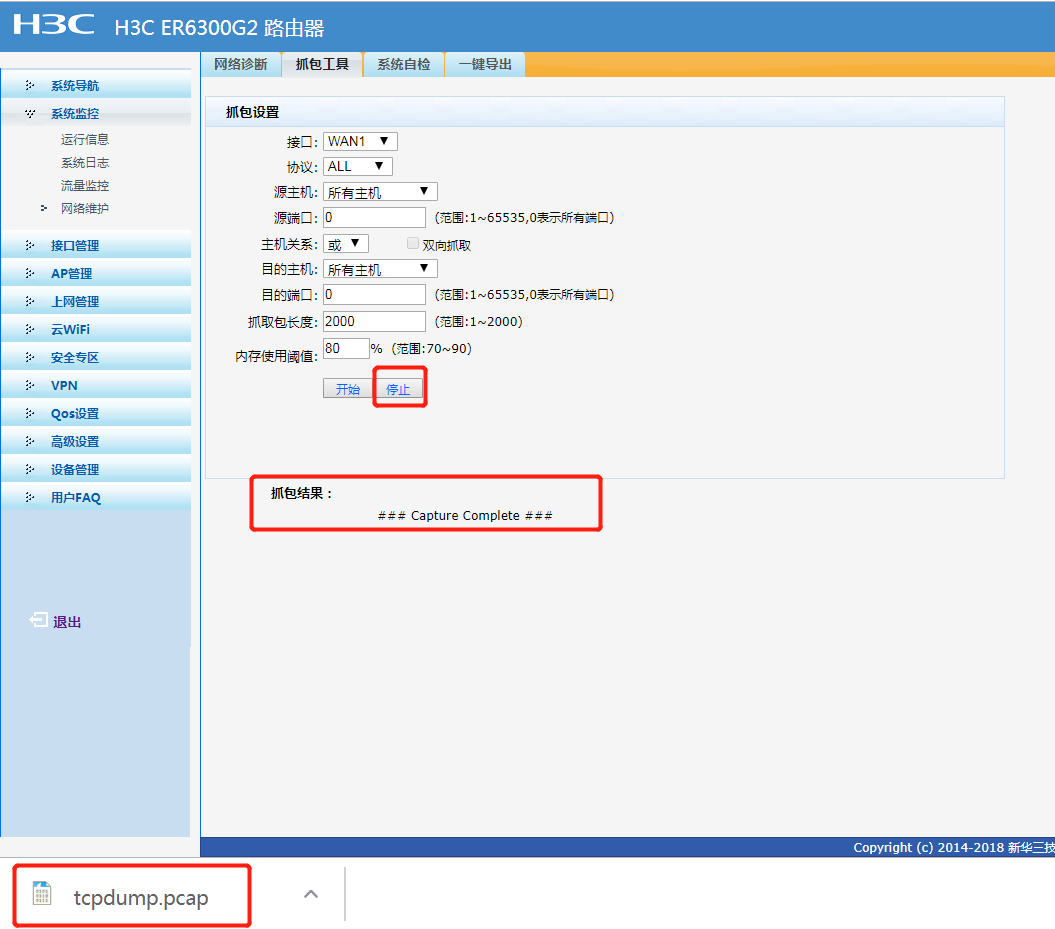
WEB页面：系统监控→网络维护→抓包工具



点击“开始”，系统开始抓包，抓包过程中，当前抓取的分组数会显示在页面上；



点击“停止”，即可停止数据包的抓取，此时系统会自动提示您导出抓包文件“tcpdump.pcap”到本地，该文件可使用wireshark等软件打开。



抓包页面中关键项的含义如下表所示：

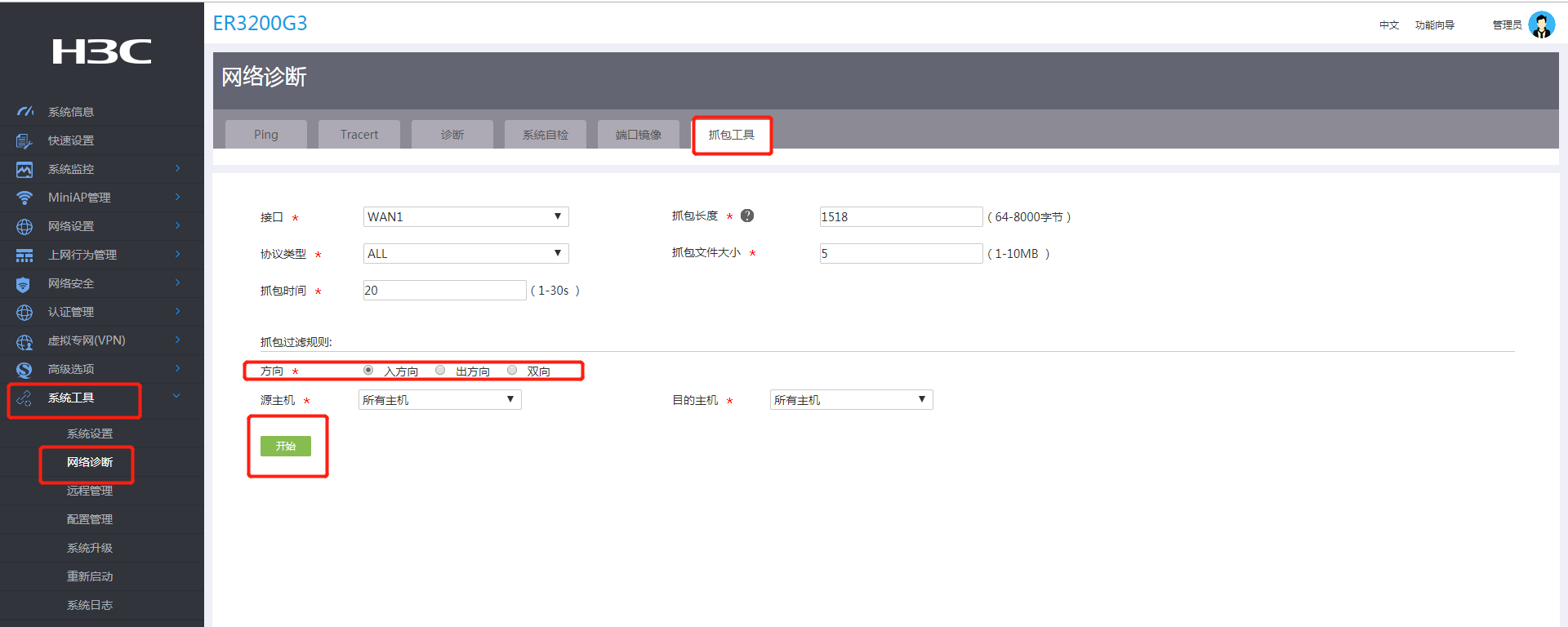
| 页面关键项 | 描述 |
| --- | --- |
| 接口 | 选择抓取报文的来源接口  说明  支持当前路由器的所有WAN、VLAN等接口 |
| 协议 | 选择需要抓取的报文的协议类型  说明  缺省协议为ALL，即抓取所有类型的数据包  如您手动修改协议为ARP、RARP、ICMP时，源端口号和目的端口号将无法设置 |
| 源/目的主机 | 设置抓取报文的源/目的主机过滤条件，以抓取符合条件的数据包：  所有主机：抓取所有源/目的主机的数据包  IP地址过滤：仅允许抓取源/目的主机为所设置IP地址的数据包  MAC地址过滤：仅允许抓取源/目的主机为所设置MAC地址的数据包 |
| IP地址 | 设置抓取报文的源/目的IP地址，点分十进制类型，取值范围：0.0.0.0～255.255.255.255 |
| MAC地址 | 设置抓取报文的MAC地址，输入格式为xx:xx:xx:xx:xx:xx（或xx-xx-xx-xx-xx-xx、或xxxx-xxxx-xxxx），且不区分大小写 |
| 源/目的端口 | 输入抓取报文的源/目的端口号，需要配置正确的端口号才能抓到相应端口的报文。  取值范围：1～65535，最多可设置10个单一端口，端口间用英文逗号“,”隔开，比如：100,200,300  说明  如果要抓取所有端口的报文，您可以将其设置为0 |
| 主机关系 | 设置源主机与目的主机之间的逻辑关系：  或：设置抓取报文为源主机与目的主机之间所有报文的并集  与：设置抓取报文为源主机与目的主机之间所有报文的交集 |
| 双向抓取 | 选中该项，则系统会抓取源主机与目的主机之间的双向报文  说明  只有在主机关系设置为“与”时，该选项方可勾选 |
| 抓取包长度 | 设置抓包的最大报文长度，当tcpdump的数据包长度超过所设数值时，数据包将会被截断。取值范围：1～2000  说明  如果您设置的抓取包长度过大，会增加包的处理时间，并减少可缓存数据包的数量，从而可能导致部分数据包的丢失。故而，在保证数据包长度足够的前提下，建议您设置尽可能小的抓包长度 |
| 内存使用阈值 | 设置抓包过程中所允许的系统内存最大使用率，当内存使用率达到所设阈值时，系统会主动停止抓包，并提示用户导出抓包文件。取值范围为70～90，缺省值为80 |

**ERG3产品：**

抓包时，将会把抓取到的临时文件保存到系统中。随着临时文件占用空间持续增加到某个阀值时，系统会主动停止抓包并导出抓取的文件。

WEB页面：

1. 系统工具→网络诊断→抓包工具：



在“接口”配置项处，选择需要抓取数据的接口，支持当前路由器的所有的WAN、VLAN等接口。

在“抓包长度”配置项处，输入tcpdump数据包的抓取长度。如果数据包长度大于此数值，数据包将会被截断。需要注意的是，采用长的抓取长度，会增加包的处理时间，并且会减少tcpdump可缓存的数据包的数量，从而会导致数据包的丢失。所以，在能抓取我们想要的包的前提下，抓取长度越小越好。

在“协议类型”配置项处，选择需要过滤的协议类型。如果选择ALL，将抓取当前接口下所有报文。

在“抓包文件大小”配置项处，输入抓取报文的大小。

在“抓包时间”配置项处，输入抓包的持续时长。

在“方向”配置项处，选择抓取报文的方向。

在“源主机”、“目的主机”配置项处，选择抓取报文时过滤发出或者接收报文的主机。

所有主机：对源或者目的主机进行过滤，即抓取所有的源/目的主机的报文。

IP地址过滤：选择此项时，需设置主机的IP地址。

MAC地址过滤：选择此项时，需设置主机的MAC地址。

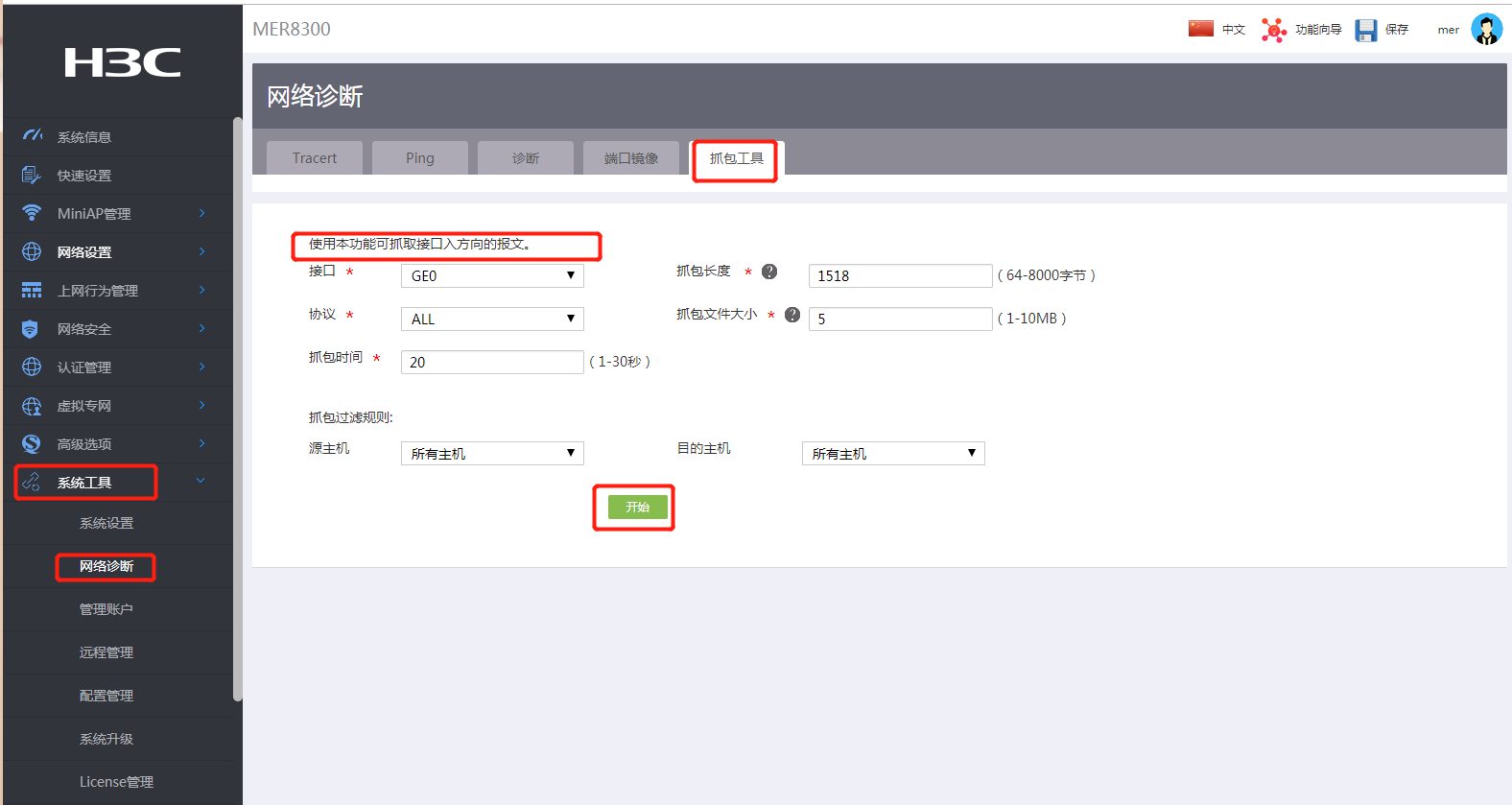
1. 点击 开始 按钮，系统开始进行抓包。抓包的过程和当前抓取的分组数显示在当前页面，在抓包的过程中，您可以点击<取消>按钮，终止当前的操作，并导出抓取的文件“capture.pacp”。

**MER产品：**

WEB页面：

1. 系统工具→网络诊断→抓包工具：

MER WEB页面抓包，只可抓取接口入方向的报文。



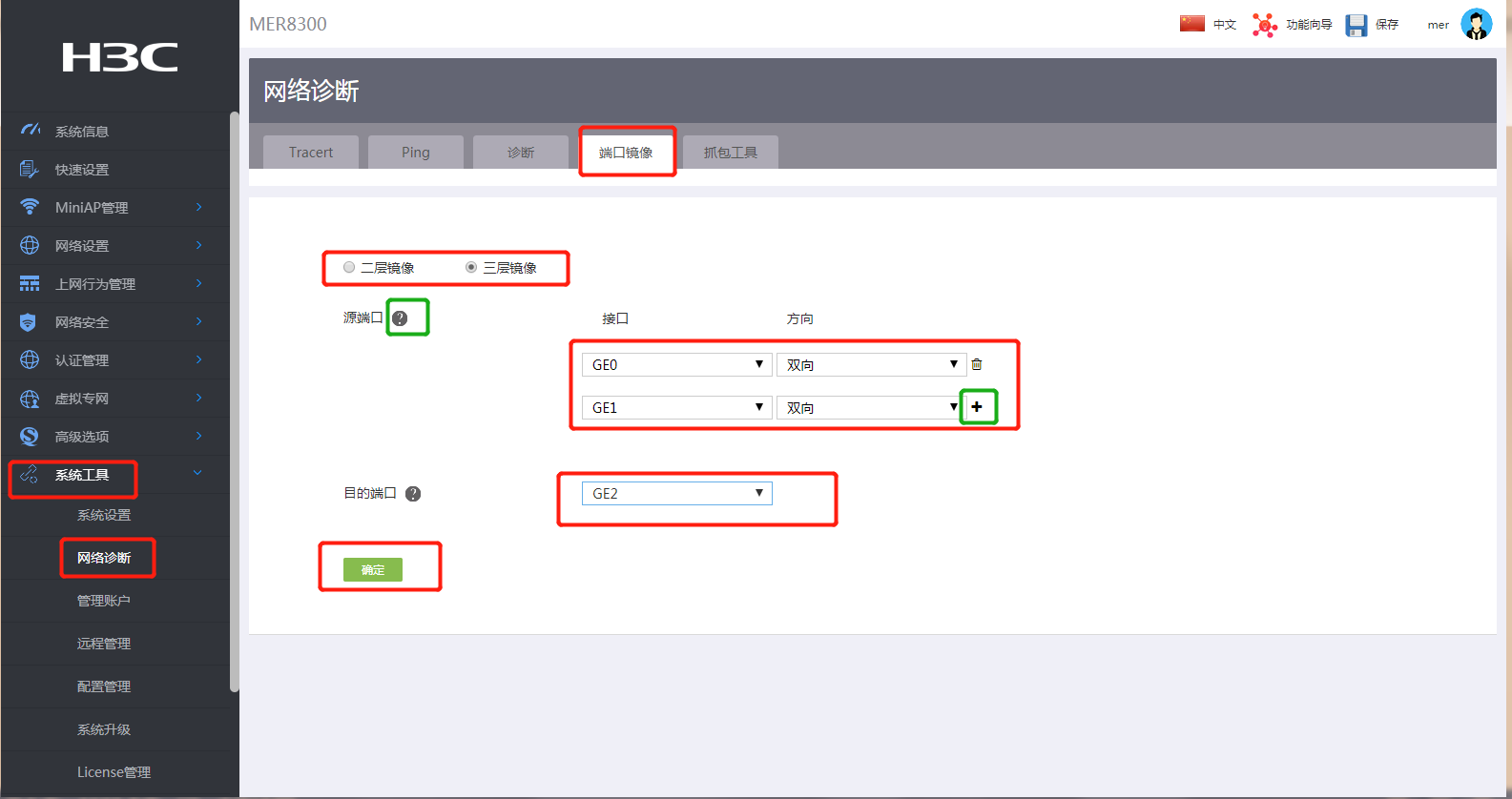
页面中关键项的解释，与上面ER产品的基本一致，不再赘述。

镜像抓包：

1. 系统工具→网络诊断→端口镜像
2. 设置源端口（可以设置多个），目的端口（不能与源端口重复）

建议目的端口为空闲端口（没有部署业务的端口）

1. 点击 确定，配置完成。

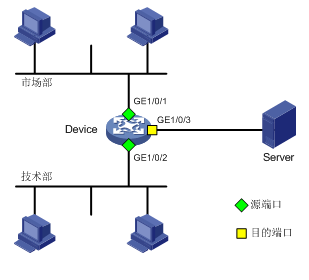


**MSR产品：**

本地端口镜像抓包（举例说明）：

1. 组网需求：

Device通过端口GigabitEthernet1/0/1和GigabitEthernet1/0/2分别连接市场部和技术部，并通过端口GigabitEthernet1/0/3连接Server。通过配置源端口方式的本地端口镜像，使Server可以监控所有进、出市场部和技术部的报文。



1. 配置步骤：

#创建本地镜像组1：

<Device> system-view

[Device] mirroring-group 1 local

# 配置本地镜像组1的源端口为GigabitEthernet1/0/1和GigabitEthernet1/0/2，对源端口收发(单收：inbound方向；单发：outbound方向)的报文都进行镜像，目的端口为GigabitEthernet1/0/3。

全局视图下配置：

[Device] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 gigabitethernet 1/0/2 both

[Device] mirroring-group 1 monitor-port gigabitethernet 1/0/3

或者 在接口视图下配置：

[Device] interface gigabitethernet 1/0/1

[Device-GigabitEthernet1/0/1] mirroring-group 1 mirroring-port both

[Device] interface gigabitethernet 1/0/2

[Device-GigabitEthernet1/0/2] mirroring-group 1 mirroring-port both

[Device] interface gigabitethernet 1/0/3

[Device-GigabitEthernet1/0/3] mirroring-group 1 monitor-port

# 在目的端口GigabitEthernet1/0/3上关闭生成树协议。

[Device] interface gigabitethernet 1/0/3

[Device-GigabitEthernet1/0/3] undo stp enable

[Device-GigabitEthernet1/0/3] quit

1. 验证配置：

# 显示所有镜像组的配置信息。

[Device] display mirroring-group all

Mirroring group 1:

Type: Local

Status: Active

Mirroring port:

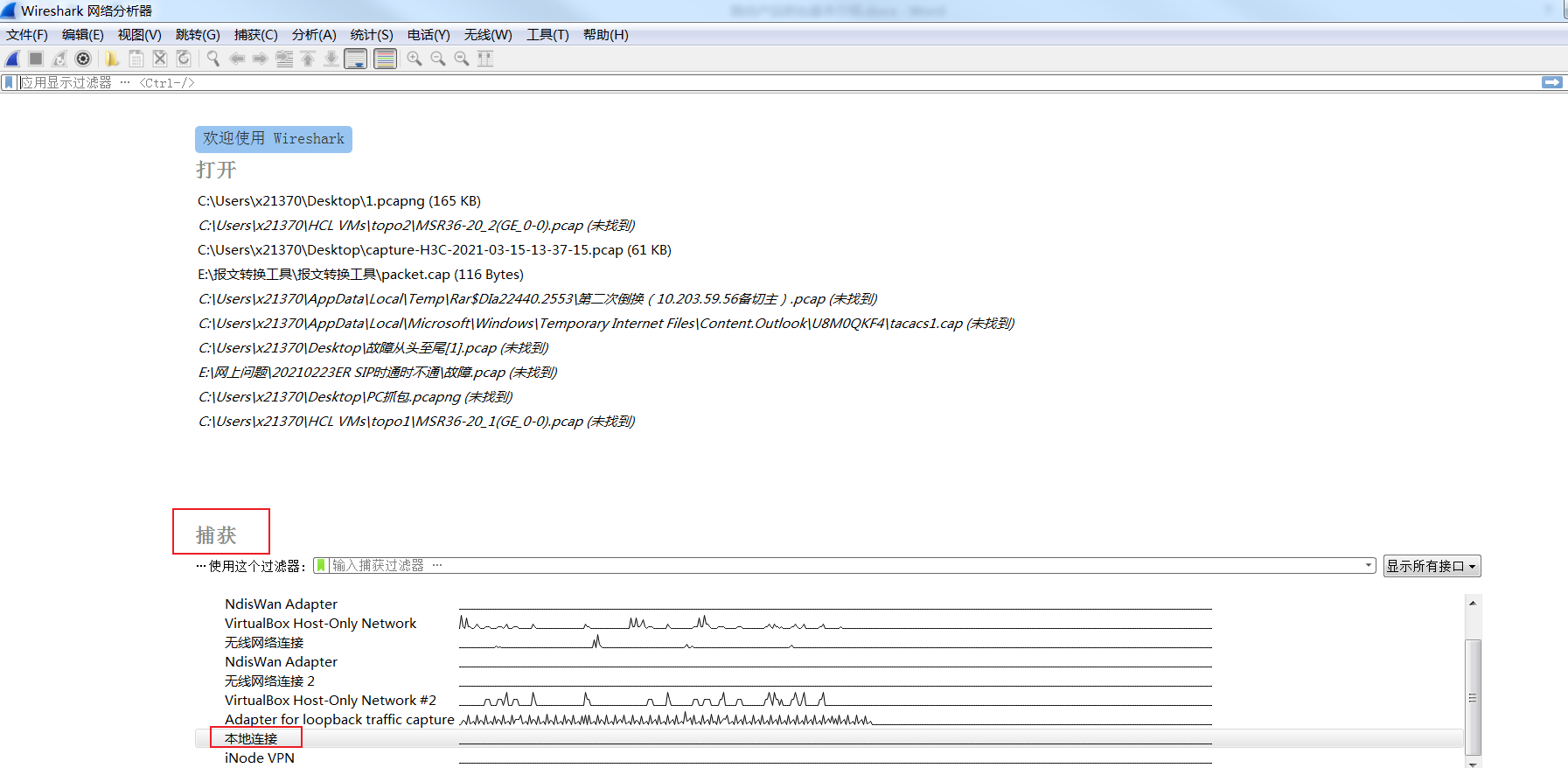
GigabitEthernet1/0/1 Both

GigabitEthernet1/0/2 Both

Monitor port: GigabitEthernet1/0/3

配置完成后，用户可以通过Server监控所有进、出市场部和技术部的报文。

1. 将PC与目的端口GigabitEthernet1/0/3网线连接，打开wireshark抓包软件，选择[捕获/本地连接]，开始捕获报文。



1. 抓取到自己需要的报文后，点击红色按钮停止捕获。点击[文件/另存为]保存到本地。

