远程报文捕获案例（packet-capture remote）

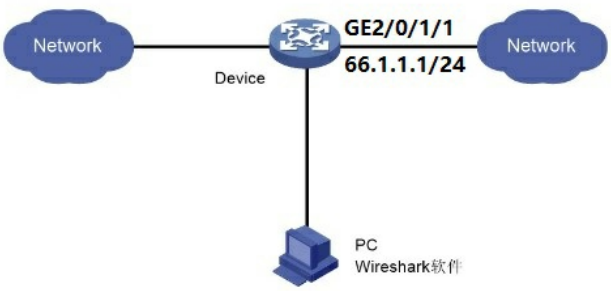
软件相关 王科 2022-09-17 发表

组网及说明

1. 组网需求

在Device的三层接口GigabitEthernet2/0/1/1上开启远程入方向报文捕获功能，将捕获的报文上送到Wireshark软件上解析。

2. 组网图



配置步骤

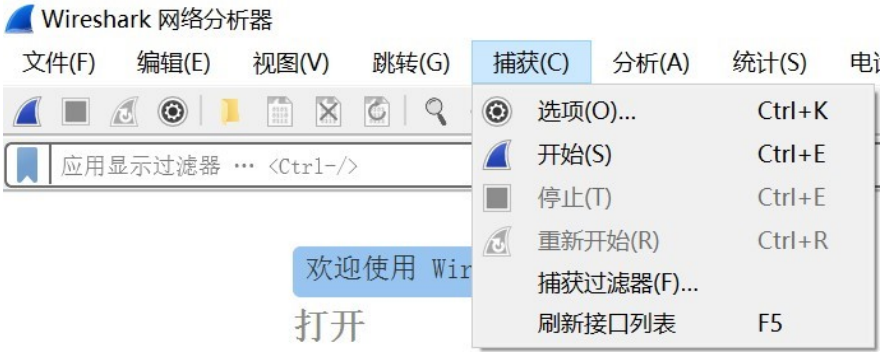
1. 配置Device

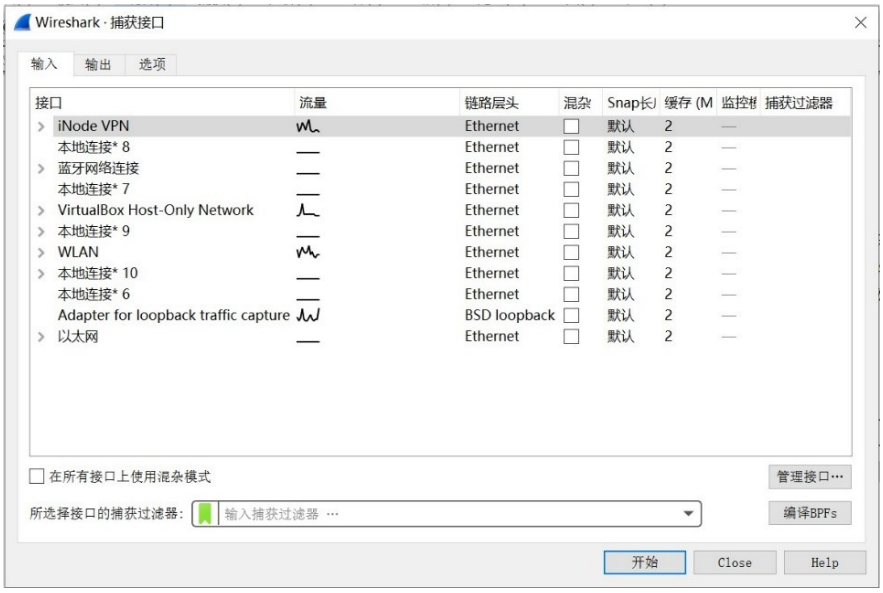
在GigabitEthernet2/0/1/1上开启远程入方向报文捕获功能，指定RPCAP服务端口号为4000。

<CR19K-L>packet-capture remote interface g2/0/1/1 bidirection port 4000

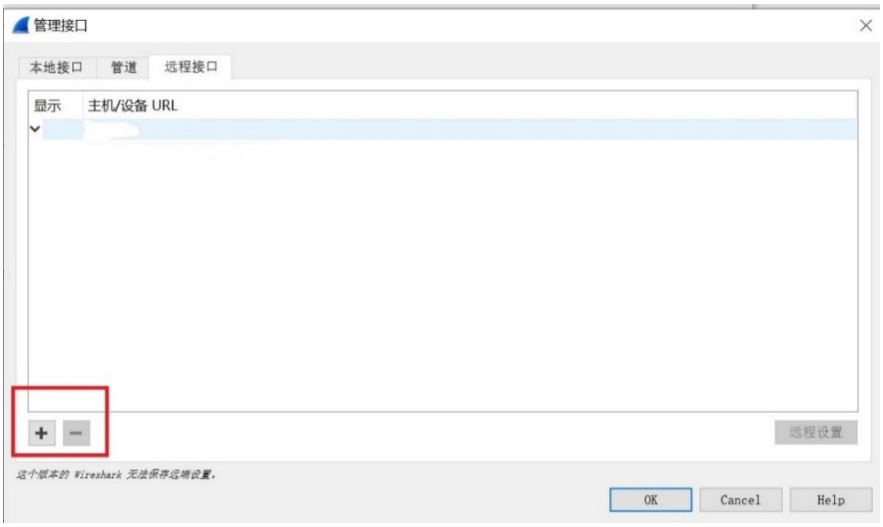
2. 配置Wireshark

1）在PC上打开Wireshark软件，选择“Capture > Options”（捕获>选项）。





2）选择“管理接口> 远程接口”。



3) 输入Device的IP地址（该地址必须和Wireshark路由可达）和绑定的RPCAP服务端口号4000。

<CR19K-L>ping -a 3.3.3.3 3.3.3.1

Ping 3.3.3.1 (3.3.3.1): 56 data bytes, press CTRL+C to break

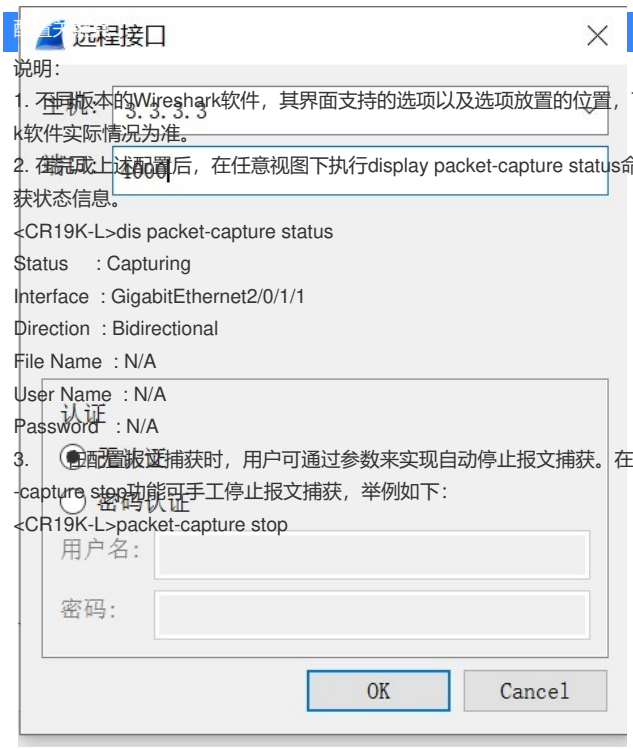
56 bytes from 3.3.3.1: icmp_seq=0 ttl=128 time=1.568 ms

56 bytes from 3.3.3.1: icmp_seq=1 ttl=128 time=0.777 ms

56 bytes from 3.3.3.1: icmp_seq=2 ttl=128 time=0.721 ms

56 bytes from 3.3.3.1: icmp_seq=3 ttl=128 time=0.679 ms

56 bytes from 3.3.3.1: icmp_seq=4 ttl=128 time=0.777 ms



说明：

1. 不同版本的Wireshark软件，其界面支持的选项以及选项放置的位置，可能存在差异，请以Wireshark软件实际情况为准。

2. 在完成上述配置后，在任意视图下执行display packet-capture status命令可以显示配置后的报文捕获状态信息。

<CR19K-L>dis packet-capture status

Status : Capturing

Interface : GigabitEthernet2/0/1/1

Direction : Bidirectional

File Name : N/A

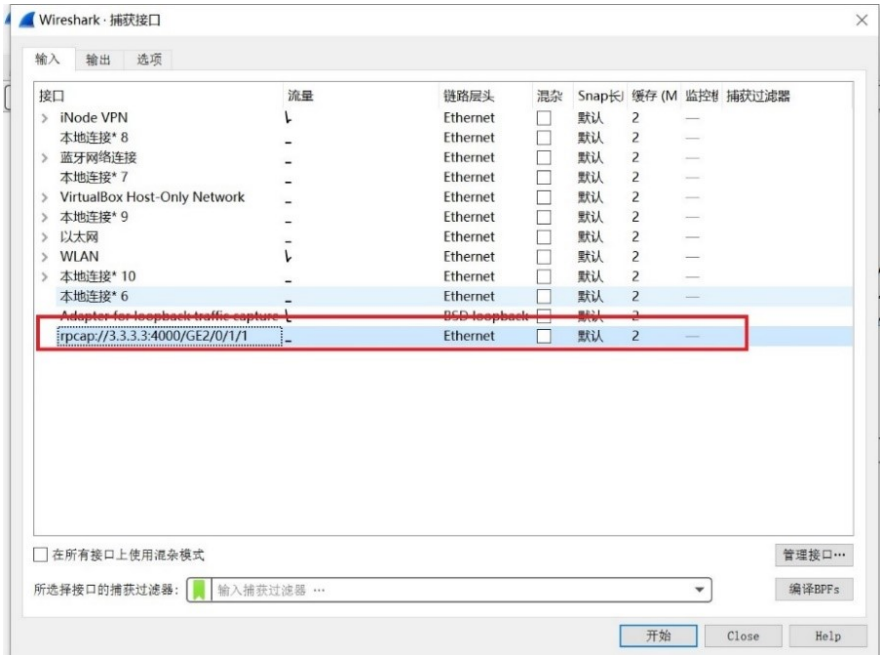
User Name : N/A

Password : N/A

3. 配置报文捕获时，用户可通过参数来实现自动停止报文捕获。在报文捕获过程中，使用packet-capture stop功能可手工停止报文捕获，举例如下：

<CR19K-L>packet-capture stop

4) 点击<OK>按钮，再点击<Start/开始>按钮启动捕获。此时在报文捕获窗口可看到捕获到的报文。



此时设备上可以看到端口已经被监听：

```
<CR19K-L>dis tcp
 *: TCP connection with authentication
 Local Addr:port       Foreign Addr:port     State       Chassis Slot  Cpu PCB
 3.3.3.3:58883         3.3.3.1:60467         ESTABLISHED 2       0     0   0xfffffffffffffb6
 3.3.3.3:4000          3.3.3.1:60466         ESTABLISHED 2       0     0   0xfffffffffffffb4
```

从设备上ping g2/0/1/1下一跳，此时在报文捕获窗口可看到捕获到的ping报文。

[CR19K-L]ping 66.1.1.2

Ping 66.1.1.2 (66.1.1.2): 56 data bytes, press CTRL+C to break

56 bytes from 66.1.1.2: icmp_seq=0 ttl=255 time=0.755 ms

56 bytes from 66.1.1.2: icmp_seq=1 ttl=255 time=0.481 ms

56 bytes from 66.1.1.2: icmp_seq=2 ttl=255 time=0.450 ms

56 bytes from 66.1.1.2: icmp_seq=3 ttl=255 time=0.439 ms

56 bytes from 66.1.1.2: icmp_seq=4 ttl=255 time=0.430 ms

--- Ping statistics for 66.1.1.2 ---

5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss

round-trip min/avg/max/std-dev = 0.430/0.511/0.755/0.123 ms

捕获报文：


3.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
icmp
No. Time Source Destination Protocol Info