1. 简介

Tcpreplay是一系列工具的总称，包括tcpreplay、tcprewrite和tcpprep等工具，这也是Tcpreplay的第一个字母大写的原因。它用来在Unix系统或类Unix系统上重放网络包。这些包是由tcpdump、ethereal和wireshark等软件抓取到的，即pcap格式的数据包。

下载相关源码包或者文档请到：<http://tcpreplay.appneta.com>/

1. 列表

|  |  |
| --- | --- |
| 工具 | 功能 |
| tcpreplay | 重发pcap文件中的数据包。 |
| tcprewrite | 改写pcap数据包的2-4层的头部信息，即MAC地址、IP地址和PORT等。 |
| tcpprep | 区分pcap数据包的流向，即区分出客户端和服务器。 |

由于使用上的需要，本文只介绍和使用tcpreplay、tcprewrite两个工具。

1. 下载和安装

到 [http://tcpreplay.appneta.com/](http://tcpreplay.appneta.com/下载最新的tcpreplay的源码包tcpreplay-4.1.0.tar.gz) 下载最新的tcpreplay的源码包tcpreplay-4.1.0.tar.gz

首先要安装依赖包libpcap、libpcap-devel

解压：

|  |
| --- |
| #tar xzvf tcpreplay-4.1.0.tar.gz  #cd tcpreplay-4.1.0 |

编译安装：

|  |
| --- |
| #./configure  #make  make install |

1. 使用说明

tcpreplay

[样例1]

tcpreplay -t -i eth1 file.pcap

-t指定立即发出报文

-i eth1指定发出报文的网卡接口

file.pcap是指tcpreplay发送的是来自file.pcap这个文件中的数据包。

[样例2]

tcpreplay -t -l 100 -i eth1 file.pcap

-t指定立即发出报文

-l 100 指定循环发送100次

-i eth1指定发出报文的网卡接口

file.pcap是指tcpreplay发送的是来自file.pcap这个文件中的数据包。

[样例3]

tcpreplay -p 500 -l 100 -i eth1 file.pcap

-p 50指定发包速率为500pps

-l 100 指定循环发送100次

-i eth1指定发出报文的网卡接口

file.pcap是指tcpreplay发送的是来自file.pcap这个文件中的数据包。

[样例4]

tcpreplay -M 10 -l 100 -i eth1 file.pcap

-M 10 指定发包速率为10mbps

-l 100 指定循环发送100次

-i eth1指定发出报文的网卡接口

file.pcap是指tcpreplay发送的是来自file.pcap这个文件中的数据包。

tcprewrite

[样例1]

tcprewrite -i input.pcap -o output.pcap --enet-dmac=74:A4:B5:00:02:59

-i input.pcap指定输入的原始pcap文件

-o output.pcap指定修改后输出的pcap文件

--enet-dmac=74:A4:B5:00:02:59将目的mac修改成74:A4:B5:00:02:59

tcpdump

[样例1]

tcpdump -i eth0 'tcp and port 80' -s 0 -w file.pcap

-i eth0指定抓取报文的网络接口

-s 0 尽量不截断报文

-w file.pcap 将抓取文件输出到file.pcap中

'tcp and port 80' 设置filter条件

1. 应用场景

发包机和接收报文的程序在同一台主机上。

[适用场景]

程序的功能和逻辑性验证。

[操作步骤]

首先将抓取的报文保存成pcap文件，通过tcpdump –w file.pcap或wireshark保存为pcap后缀名；

然后通过tcpreplay -t -i eth0 file.pcap发包。

发包机和接收报文的程序在不同的主机上

[适用场景]

程序的性能和压力测试。

[操作步骤]

首先将抓取的报文保存成pcap文件，通过tcpdump –w file.pcap或wireshark保存为pcap后缀名；

程序部署在设备A上，发包机部署在设备B上，设备A和设备B在同一局域网，且设备A的MAC地址在MAC-A（例如74:A4:B5:00:02:59）；

然后通过tcprewrite -i iqiyi.pcap -o iqiyi.change.mac.pcap --enet-dmac=74:A4:B5:00:02:59修改pcap文件中的目的MAC为MAC-A；

最后通过tcpreplay -t -i eth0 iqiyi.change.mac.pcap发包。

1. 注意点：

**修改802.1q VLAN**

经常客户的抓包带有VLAN头域, 这些包如果不去掉VLAN头是没有办法在自己的交换机上replay的, tcprewrite提了去掉或添加VLAN的方法:

去掉vlan很简单:

#tcprewrite --enet-vlan=del --infile=input.pcap --outfile=output.pcap

添加vlan也很简单, 下面的命令将VLAN tag设成40, CFI设成1, VLAN priority设成4.

#tcprewrite --enet-vlan=add --enet-vlan-tag=40 --enet-vlan-cfi=1 --enet-vlan-pri=4 --infile=input.pcap --outfile=output.pcap

1. 参考文档：

linux man tcpreplay

linux man tcpreplay

<http://www.360doc.com/content/12/0223/20/8477600_189108612.shtml>

<http://blog.csdn.net/ttyttytty12/article/details/8125007>

<http://blog.chinaunix.net/uid-20401941-id-3069302.html>

<http://blog.chinaunix.net/uid-20648182-id-1907531.html>