官网：<https://www.tcpdump.org/>

使用指南：<https://blog.csdn.net/weixin_73727639/article/details/137566242>

源码：<https://github.com/the-tcpdump-group/libpcap.git>

环境使用代码：<https://www.tcpdump.org/release/libpcap-1.10.4.tar.xz>

1. libpcap已经对c++调用做了处理，没有必要使用extend，不过为了代码清晰以及以防万一：

1 #ifdef \_\_cplusplus

2 extren "C"{

3 #endif

4 #include <pcap.h>

5 #ifdef \_\_cplusplus

6 }

7 #endif

1. libpcap直接获取默认的网络端口的时候会出现异常，所以需要特殊处理，筛选网口名称

72 pcap\_findalldevs(&alldevs, errbuf);

73 while(1)

74 {

75 if(alldevs->name == nullptr || alldevs->next == NULL)

76 {

77 goto goon;

78 }

79 else

80 {

81 std::string tmp\_name(alldevs->name);

82 if (std::string::npos != tmp\_name.find("ens"))

83 {

84 dev = alldevs->name;

85 }

86 std::cout << "devs name : " << alldevs->name << std::endl;

87 if(alldevs->next == nullptr || alldevs->next == NULL)

88 {

89 goto goon;

90 }

91 else

92 {

93 alldevs = alldevs->next;

94 }

95 }

96

97 }

98