blog.chinaunix.net

# Libpcap库主要函数说明-chinaltang-ChinaUnix博客

3-4 分钟

---

Libpcap库主要函数说明

函数名称：pcap_t *pcap_open_live(char *device, int snaplen, int promisc, int to_ms, char *ebuf)
函数功能：获得用于捕获网络数据包的数据包捕获描述字。
参数说明：device 参数为指定打开的网络设备名。snaplen参数定义捕获数据的最大字节数。promisc指定是否将网络接口置于混杂模式。to_ms参数指*定超时时间（毫秒）。ebuf参数则仅在pcap_open_live()函数出错返回NULL时用于传递错误消息。

函数名称：pcap_t *pcap_open_offline(char *fname, char *ebuf)
函数功能：打开以前保存捕获数据包的文件，用于读取。
参数说明：fname参数指定打开的文件名。该文件中的数据格式与tcpdump和tcpslice兼容。”-“为标准输入。ebuf参数则仅在pcap_open_offline()函数出错返回NULL时用于传递错误消息。

函数名称：pcap_dumper_t *pcap_dump_open(pcap_t *p, char *fname)
函数功能：打开用于保存捕获数据包的文件，用于写入。
参数说明：fname 参数为”-“时表示标准输出。出错时返回NULL。p参数为调用pcap_open_offline()或pcap_open_live()函数后返回的pcap结构指针。fname参数指定打开的文件名。如果返回NULL，则可调用pcap_geterr()函数获取错误消 息。

函数名称：char *pcap_lookupdev(char *errbuf)
函数功能：用于返回可被pcap_open_live()或pcap_lookupnet()函数调用的网络设备名指针。参数说明：如果函数出错，则返回NULL，同时errbuf中存放相关的错误消息。

函数名称：int pcap_lookupnet(char *device, bpf_u_int32 *netp,bpf_u_int32 *maskp, char *errbuf)
函数功能：获得指定网络设备的网络号和掩码。
参数说明：netp参数和maskp参数都是bpf_u_int32指针。如果函数出错，则返回-1，同时errbuf中存放相关的错误消息。

函数名称：int pcap_dispatch(pcap_t *p, int cnt,pcap_handler callback, u_char *user)
函数功能：捕获并处理数据包。
参数说明：cnt 参数指定函数返回前所处理数据包的最大值。cnt=-1表示在一个缓冲区中处理所有的数据包。cnt=0表示处理所有数据包，直到产生以下错误之一：读取到EOF；超时读取。callback参数指定一个带有三个参数的回调函数，这三个参数为：一个从pcap_dispatch()函数传递过来的 u_char指针，一个pcap_pkthdr结构的指针，和一个数据包大小的u_char指针。如果成功则返回读取到的字节数。读取到EOF时则返回零值。出错时则返回-1，此时可调用pcap_perror()或pcap_geterr()函数获取错误消息。

函数名称：int pcap_loop(pcap_t *p, int cnt,pcap_handler callback, u_char *user)
函数功能：功能基本与pcap_dispatch()函数相同，只不过此函数在cnt个数据包被处理或出现错误时才返回，但读取超时不会返回。而如果为 pcap_open_live()函数指定了一个非零值的超时设置，然后调用pcap_dispatch()函数，则当超时发生时 pcap_dispatch()函数会返回。cnt参数为负值时pcap_loop()函数将始终循环运行，除非出现错误。

函数名称：void pcap_dump(u_char *user, struct pcap_pkthdr *h,u_char *sp)
函数功能：向调用pcap_dump_open()函数打开的文件输出一个数据包。该函数可作为pcap_dispatch()函数的回调函数。

函数名称：int pcap_compile(pcap_t *p, struct bpf_program *fp,char *str, int optimize, bpf_u_int32 netmask)
函数功能：将str参数指定的字符串编译到过滤程序中。
参数说明：fp是一个bpf_program结构的指针，在pcap_compile()函数中被赋值。optimize参数控制结果代码的优化。netmask参数指定本地网络的网络掩码。

函数名称：int pcap_setfilter(pcap_t *p, struct bpf_program *fp)
函数功能：指定一个过滤程序。
参数说明：fp参数是bpf_program结构指针，通常取自pcap_compile()函数调用。出错时返回-1；成功时返回0。

函数名称：u_char *pcap_next(pcap_t *p, struct pcap_pkthdr *h)
函数功能：返回指向下一个数据包的u_char指针。

函数名称：int pcap_datalink(pcap_t *p)
函数功能：返回数据链路层类型，例如DLT_EN10MB。

函数名称：int pcap_snapshot(pcap_t *p)
函数功能：返回pcap_open_live被调用后的snapshot参数值。

函数名称：int pcap_is_swapped(pcap_t *p)
函数功能：返回当前系统主机字节与被打开文件的字节顺序是否不同。

函数名称：int pcap_major_version(pcap_t *p)
函数功能：返回写入被打开文件所使用的pcap函数的主版本号。

函数名称：int pcap_minor_version(pcap_t *p)
函数功能：返回写入被打开文件所使用的pcap函数的辅版本号。

函数名称：int pcap_stats(pcap_t *p, struct pcap_stat *ps)
函数功能：向pcap_stat结构赋值。成功时返回0。这些数值包括了从开始捕获数据以来至今共捕获到的数据包统计。如果出错或不支持数据包统计，则返回-1，且可调用pcap_perror()或pcap_geterr()函数来获取错误消息。

函数名称：FILE *pcap_file(pcap_t *p)
函数功能：返回被打开文件的文件名。

函数名称：int pcap_fileno(pcap_t *p)
函数功能：返回被打开文件的文件描述字号码。

函数名称：void pcap_perror(pcap_t *p, char *prefix)
函数功能：在标准输出设备上显示最后一个pcap库错误消息。以prefix参数指定的字符串为消息头。

函数名称：char *pcap_geterr(pcap_t *p)
函数功能：返回最后一个pcap库错误消息。

函数名称：char *pcap_strerror(int error)
函数功能：如果strerror()函数不可用，则可调用pcap_strerror函数替代。

函数名称：void pcap_close(pcap_t *p)
函数功能：关闭p参数相应的文件，并释放资源。

函数名称：void pcap_dump_close(pcap_dumper_t *p)
函数功能：关闭相应的被打开文件。
Libpcap开发库安装