在局域网进行IP包捕获的一种方法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/270/2021_2022__E5_9C_A8_E5_B1_80_E5_9F_9F_E7_c67_270959.htm 首先是几个结构的定义（网上搜索或者查阅相关文档）： er=1〉 //定义IP地址结构 struct IPADDRESS { unsigned short ip_a, ip_b, ip_c, ip_d. }. //定义IP数据包头的结构 struct IP_HEADER { unsigned short ip_version, /*IP的版本号 */ ip_hdr_len, /*IP包头的长度*/ ip_tos, /*IP包的服务类型*/ ip_total_len, /*IP包的总长度*/ ip_id, /*IP包的分段标识*/ ip_flags, /*IP包的分段标志*/ ip_frag_offset, /*IP包的分段偏移*/ ip_ttl, /*IP包的生存时间*/ ip_proto, /*IP包的高层协议*/ ip_hdr_chksum. /*IP包的校验和*/ struct IPADDRESS ip_src_addr, /*IP包的源IP地址*/ ip_dest_addr. /*IP包的目的IP地址*/ }ipheader. //IP包的链表结构 struct stru_ip_link { char rcv_ip_buf[MAX_IP_SIZE]. struct stru_ip_link *next. }. 然后是协议的定义（包含相应的头文件#include #include）： DWORD dwIoControlCode=SIO_RCVALL, /*接收所有的IP包*/ dwProtocol=IPPROTO_IP. /*协议类型为IP*/ 然后是相应的捕获处理： 1.加载 Winsock； 2.创建一个接收原始IP包的socket连接； 3.绑定到一个接口； 4.进行WSAIoctl设置，接收所有的IP数据包。 参考代码： if (WSAIoctl(s, dwIoControlCode, amp.dwBytesRet, NULL, NULL) == SOCKET_ERROR) ... 5.接着设定一个线程进行捕获：（1）创建一个接收IP包的链表头；（2）设置一个标识，为真，则不断进行IP包的捕获；（3）建立一个新的结点，将捕获的数据包加入到该结点；（4）如果链表的长度达到指定的长度，创建一个线程对该链表

的IP包进行解析；再设置一个在IP数据包链表不足给定的长度，而又中止IP捕获时，对链表的处理；（5）为下一个IP包链表创建一个链表头。 6.建立一个进行IP包解析并显示的线程，进行解析IP数据包，然后显示IP数据包。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com