# LwIP协议栈的学习与应用

## 前言

LWIP(Light Weight Internet Protoco1)是瑞士计算机科学院(Swedish Institute of Computer Science)AdamDunkels等人开发的一套用于嵌入式系统的开放源代码TCP／IP协议栈。LWIP的含义是Light Weight(轻型)IP协议。LWIP可以移植到操作系统上，也可以在无操作系统的情况下独立运行。LWIP TCP／IP实现的重点是在保持TCP协议主要功能的基础上减少对RAM的占用。一般它只需要几十KB的RAM和40 KB左右的ROM就可以运行，这使LWIP协议栈适合在小型嵌入式系统中使用。

## 第一部分 协议栈的移植

### 准备工作

本文的硬件环境采用LPC2468作为主控MCU，LPC24xx是NXP半导体公司(由Philips公司创建) 推出的基于ARM7TDMI-S内核的微控制器，它在片上集成了10 Mbps／100 Mbps以太网控制器。PHY芯片采用DM9161AEP。 操作系统方面，我们选用的μC/OS II 2.88。开发环境采用KEIL MDK3.8。

### 第二章 操作系统适配层

为了使lwIP便于移植，与操作系统有关的功能函数调用和数据结构没有在代码中直接使用。而是当需要这样的函数时，操作系统适配层将加以使用。操作系统适配层向诸如定时器、处理同步、消息传送机制等的操作系统服务提供一套统一的接口。原则上，移植lwIP到其他操作系统时，仅仅需要实现适合该操作系统的操作系统模拟层。

操作系统适配层提供了由TCP使用的定时器功能。操作系统适配层提供的定时器是一次性的定时器，当超时发生时，调用一个已注册函数至少要200ms的间隔。

进程同步机制仅提供了信号量。即使在操作系统底层中信号量不可用，也可以通过其他信号原语像条件变量或互锁来模拟。

信息传递的实现使用一种简单机制，用一种称为“邮箱”的抽象方法。邮箱做两种操作：邮寄和提取。邮寄操作不会阻塞进程；邮寄到邮箱的消息由操作系统模拟层排入队列直到另一个进程来提取它们。即使操作系统底层对邮箱机制不支持，也容易用信号量实现。

信号量多用于任务间同步和互斥。 邮箱用于大数据的传送。 队列多用于处理有序的事件。 做比较“粗俗”的比喻，信号量就是中央政府发给官人做一方大员的官印，有很多种官印但是不能一印多发，得到官印者才能掌权鱼肉一方百姓（任务得到信号量才能运行），否则你就只要等官跑官。邮箱，就好给比当差的下达的抄家、拆房、收监等红头文件，拿到啥样的文件就干啥。消息队列，就是给任务发了一连串的邮件，官员（任务）拿到这一大摞文件，可以从底部或者顶部（LIFO or FIFO)一个一个拆开处理。（注：来自www.ouravr.com）

操作系统适配层的移植主要是在sys\_arch.c里面,主要有以下几部分:

**信号量相关:**

sys\_sem\_t sys\_sem\_new(u8\_t count)

创建一个新的信号量,并给信号量赋予初值 count。

void sys\_sem\_signal(sys\_sem\_t sem)

向指定的信号量发送信号。

void sys\_sem\_free(sys\_sem\_t sem)

释放指定的信号量

u32\_t sys\_arch\_sem\_wait(sys\_sem\_t sem, u32\_t timeout)

**邮箱(MailBox)相关:**

sys\_mbox\_t sys\_mbox\_new(int size) 函数

建立一个空的邮箱，如果创建成功，则返回邮箱的地址，如果创建失败则返回为空。

void sys\_mbox\_free(sys\_mbox\_t mbox) 函数

void sys\_mbox\_post(sys\_mbox\_t mbox, void \*msg) 函数

err\_t sys\_mbox\_trypost(sys\_mbox\_t mbox, void \*msg) 函数

u32\_t sys\_arch\_mbox\_fetch(sys\_mbox\_t mbox, void \*\*msg, u32\_t timeout)

u32\_t sys\_arch\_mbox\_tryfetch(sys\_mbox\_t mbox, void \*\*msg) 函数

这个函数是1.3后新有的,

### 网卡驱动层

网卡的驱动层主要分为2个方面：MAC和PHY的初始化，数据的收发控制。下面先介绍MAC和PHY的初始化：

以太网接口的自适应能力由DM9161AEP的自动协商功能体现出来。自动协商功能提供了一种在网络连接的两端之间交换配置信息的机制，在该机制下，这两端将自动选择最优的配置， DM9161AEP支持4种不同的以太网工作方式(10 Mbps半双工、10 Mbps全双工、100 Mbps半双工和100 Mbps全双工)，自动协商功能在芯片配置的基础上自动选择性能最高的工作方式。

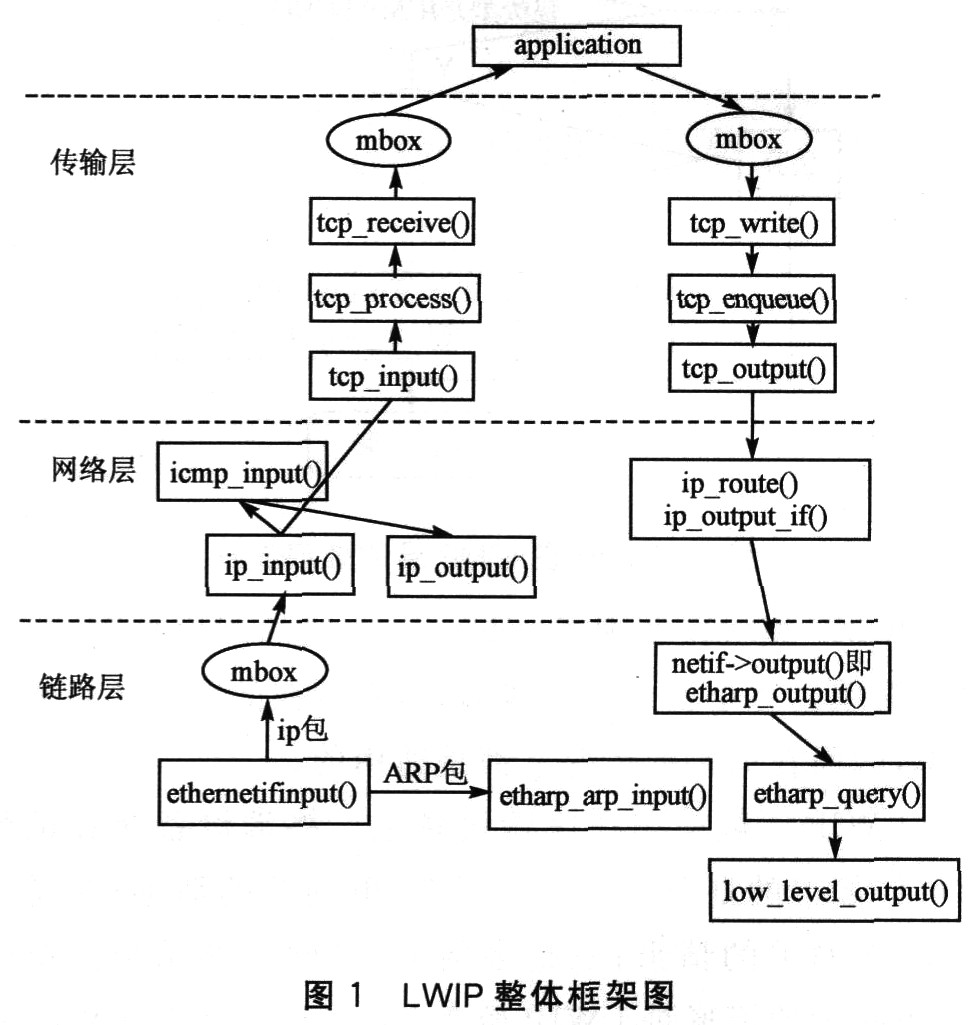
为了进行数据高效率的收发，我们设计了接收和发送两个线程进行并发处理。数据接收线程采用信号量机制，一直在等待ISR的数据接收信号。

### 第三章 应用示例

### 第四章 性能调优

## 第二部分 代码剖析

### 第一章 总揽



### 第二章 数据结构

**内存管理**

LwIP内存管理部分**（mem.h mem.c）**比较灵活，支持多种管理策略，有运行时库的自带的内存管理(MEM\_LIBC\_MALLOC)，有内存池管理(MEM\_USE\_POOLS)，有….，这些分配策略可以通过宏定义来更改，

MEM\_SIZE 是表示静态大小

**pbuf**

pbuf是lwIP包的内部表示，被设计为最小化栈的特殊需要。pbufs类似于BSD实现中的mbufs。pbuf结构支持为包内容动态分配内存和让包数据驻留在静态内存中。pbufs能被一个称为pbuf链的链接到一个链表中，以至一个包能跨越多个pbufs。

pbufs有三种类型:PBUF\_RAM,PBUF\_ROM和PBUF\_POOL。图1表示PBUF\_RAM类型，包含有存在内存中由pbuf子系统管理的包数据。图2显示了一个pbuf链表，第1个是PBUF\_RAM类型，第2个是PBUF\_ROM类型，意味着它包含有不被pubf子系统管理的内存数据。图3描述了PBUF\_POOL，其包含有从固定大小pbuf池中分配来的pbuf。一个pbuf链可以包含多个不同类型的pbuf。

这三种类型有不同的用处。PBUF\_POOL类型主要由网络设备驱动使用，因为分配单个pbuf快速且适合中断句柄使用。PBUF\_ROM类型由应用程序发送那些在应用程序内存空间中的数据时使用。这些数据不会在pbuf递交给TCP/IP栈后被修改，因此这个类型主要用于当数据在ROM中时。PBUF\_ROM中指向数据的头部被存在链表中其前一个PUBF\_RAM类型的pbuf中，如图2所示。

PBUF\_RAM类型也用于应用程序发送动态产生的数据。这情况下，pbuf系统不仅为应用程序数据分配内存，也为将指向（prepend）数据的头部分配内存。如图1所示。pbuf系统不能预知哪种头部将指向（prepend）那些数据，只假定最坏的情况。头部的大小在编译时确定。

本质上，进来的pbuf是PBUF\_POOL类型，而出去的pbuf是PBUF\_ROM或PBUF\_RAM类型。

从图1，图2可以看出pbuf的内部结构。pbuf结构包含有两个指针，两个长度字段，一个标志字段，和一个参考计数。Next字段指向统一链表中的下一个pbuf。有效载荷指针指向该pbuf中数据的起始点。Len字段包含有该pbuf数据内同的长度。tot\_len字段是当前pbuf和所有链表接下来中的len字段值的总和。简单说，tot\_len字段是len字段及下一个pbuf中tot\_len字段值的总和。Flags字段表示pbuf类型而ref字段包含一个参考计数。Next和payload字段是本地指针，其大小由处理器体系结构决定。两个长度字段是16位无符号整数，而flags和ref字段都是4比特大小。Pbuf的总大小决定于使用的处理器体系结构。在32位指针和4字节校正的体系结构上，总大小是16字节，而在16位指针和1自己校正的体系结构上，总大小是9字节。

pbuf模块提供了操作pbuf的函数。pbuf\_alloc()可以分配前面提到的三种类型的pbuf。pbuf\_ref()增加引用计数,pbuf\_free()释放分配的空间，它先减少引用计数，当引用计数为0时就释放pbuf。pbuf\_realloc()收缩空间以使pbuf只占用刚好的空间保存数据。pbuf\_header()调整payload指针和长度字段，以使一个头部指向pbuf中的数据。pbuf\_chain()和pbuf\_dechain()用于链表化pbuf。

### 第二章 ARP

**ARP协议**（**A**ddress **R**esolution **P**rotocol），或称**地址解析协议**。ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。他是IPv4中网络层必不可少的协议，不过在IPv6中已不再适用，并被icmp v6所替代。

**功能**

在局域网中，网络中实际传输的是“帧”（frame），帧里面是有目标主机的MAC地址的。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址，但这个目标MAC地址是通过地址解析协议获得的。所谓“地址解析”就是主机在发送帧前将目标IP地址转换成目标MAC地址的过程。

**原理**

在每台安装有TCP/IP协议的电脑或 route 里都有一个ARP缓存表，表里的IP地址与MAC地址是一对应的，如表甲所示。

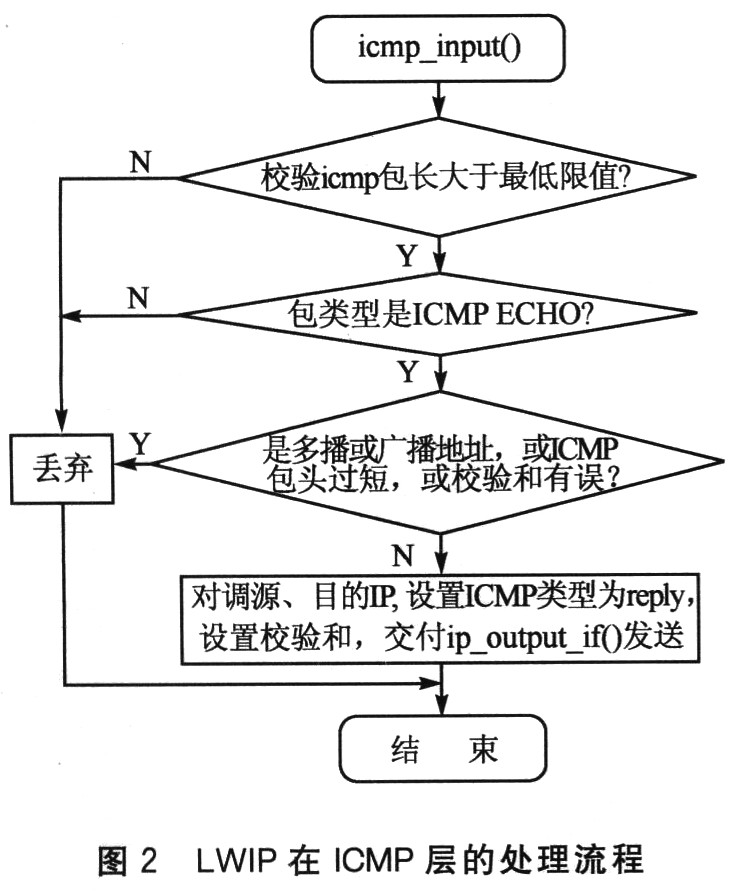
|  |  |  |
| --- | --- | --- |
| **主机名称** | **IP地址** | **MAC地址** |
| A | 192.168.38.10 | 00-AA-00-62-D2-02 |
| B | 192.168.38.11 | 00-BB-00-62-C2-02 |
| C | 192.168.38.12 | 00-CC-00-62-C2-02 |
| D | 192.168.38.13 | 00-DD-00-62-C2-02 |
| E | 192.168.38.14 | 00-EE-00-62-C2-02 |
| ... | ... |  |

以主机A（192.168.38.10）向主机B（192.168.38.11）发送数据为例。当发送数据时，主机A会在自己的ARP缓存表中寻找是否有目标IP地址。如果找到了，也就知道了目标MAC地址为(00-BB-00-62-C2-02)，直接把目标MAC地址写入帧里面发送就可以了；如果在ARP缓存表中没有找到相对应的IP地址，主机A就会在网络上发送一个广播(ARP request)，目标MAC地址是“FF.FF.FF.FF.FF.FF”，这表示向同一网段内的所有主机发出这样的询问：“192.168.38.11的MAC地址是什么？”网络上其他主机并不响应ARP询问，只有主机B接收到这个帧时，才向主机A做出这样的回应(ARP response)：“192.168.38.11的MAC地址是(00-BB-00-62-C2-02)”。这样，主机A就知道了主机B的MAC地址，它就可以向主机B发送信息了。同时它还更新了自己的ARP缓存表，下次再向主机B发送信息时，直接从ARP缓存表里查找就可以了。ARP缓存表采用了老化机制，在一段时间内如果表中的某一行没有使用，就会被删除，这样可以大大减少ARP缓存表的长度，加快查询速度。

ARP协议是一个网络层的协议，实现的功能是网络设备的MAC地址到IP地址的映射。在以太网中每个网络设备都有一个唯一的48位（6字节）MAC地址，数据报都是按照MAC地址发送的，其地址范围是由相关组织按照不同设备制造商统一分配的，这样保证了网络上设备地址不会冲突。但是TCP/IP协议是以32位（4字节）IP地址作为通讯地址的，怎样使MAC地址和IP地址对应上呢，这里就用到了ARP协议。

ARP的工作过程大致是这样的：比如网络中的一台主机想要知道MAC地址为01：02：03：04：05：06的机器的IP地址，于是它就向网上发送一个ARP查询数据报（目标MAC全为FF的广播报文），网络上的所有机器收到这个广播后将查询的MAC与自己的MAC比对，如果不一致，则不回应该报文。若一致则向该主机发出ARP回复数据报（这时就是只针对发送方的单播报文了），告诉主机自己的IP（比如192.9.200.128）。这样主机就会在ARP映射表中记录这一项192.9.200.128-----〉01：02：03：04：05：06。以后，发往这个IP地址的IP/TCP/UDP等数据报就会对应到它的MAC地址。在Windows命令提示符窗口输入arp -a查询ARP表项可以看到 MAC-〉IP的映射。

### 第三章 ICMP



## 第三部分 其他

参考文献：

嵌入式网络系统设计-基于Atmel ARM7系列