驱动学习整理

目录

[热插拔 4](#_Toc466377433)

[参考资料 8](#_Toc466377434)

[Sysfs以及设备模型 9](#_Toc466377435)

[内核空间与用户空间的映射关系 9](#_Toc466377436)

[设备模型底层容器 9](#_Toc466377437)

[struct kobj 9](#_Toc466377438)

[struct kobj\_type 10](#_Toc466377439)

[struct kset 10](#_Toc466377440)

[struct kobj\_attribute 10](#_Toc466377441)

[设备模型上层容器 11](#_Toc466377442)

[总线类型bus\_type 11](#_Toc466377443)

[Struct device 13](#_Toc466377444)

[Struct device\_driver 16](#_Toc466377445)

[从面向对象的角度 18](#_Toc466377446)

[Kobject，kset，ktype结构图 19](#_Toc466377447)

[Kobj type 22](#_Toc466377448)

[参考资料 23](#_Toc466377449)

[最小子系统+ramdisk+initrd+系统启动过程 24](#_Toc466377450)

[ramdisk+initrd 24](#_Toc466377451)

[BIOS(Basic Input Output System) 24](#_Toc466377452)

[系统引导 25](#_Toc466377453)

[MBR 25](#_Toc466377454)

[参考资料 29](#_Toc466377455)

[Paltform 30](#_Toc466377456)

[Platform设备驱动 30](#_Toc466377457)

[Platform模块的软件架构 30](#_Toc466377458)

[Platform模块向其它模块提供的API汇整 31](#_Toc466377459)

[总结大多数驱动框架 31](#_Toc466377460)

[Platform led驱动 31](#_Toc466377461)

[Platform input驱动 31](#_Toc466377462)

[Platform i2c驱动 32](#_Toc466377463)

[Platform spi驱动 32](#_Toc466377464)

[参考资料 33](#_Toc466377465)

[中断子系统 34](#_Toc466377466)

[中断 34](#_Toc466377467)

[IRQ编号 35](#_Toc466377468)

[中断处理程序 35](#_Toc466377469)

[上半部与下半部 36](#_Toc466377470)

[在驱动程序中申请中断 36](#_Toc466377471)

[flags:与中断相关的标志 38](#_Toc466377472)

[request\_threaded\_irq的工作流程 39](#_Toc466377473)

[下半部的几种机制 41](#_Toc466377474)

[软中断(softirqs) 41](#_Toc466377475)

[Tasklet 42](#_Toc466377476)

[work queue 42](#_Toc466377477)

[内核定时器 42](#_Toc466377478)

[参考资料 42](#_Toc466377479)

[Input子系统与多点触摸技术 44](#_Toc466377480)

[简介 44](#_Toc466377481)

[设备驱动层 45](#_Toc466377482)

[换个角度看input子系统 45](#_Toc466377483)

[软件设计流程 47](#_Toc466377484)

[与软件设计有关的API函数 47](#_Toc466377485)

[多点触摸技术A/B(Slot)协议 48](#_Toc466377486)

[A/B协议究竟是如何划分 48](#_Toc466377487)

[A协议实现方式 49](#_Toc466377488)

[B协议实现方式 50](#_Toc466377489)

[总结 51](#_Toc466377490)

[参考资料 51](#_Toc466377491)

[Android调试方法 53](#_Toc466377492)

[getevent，sendevent，input三命令 53](#_Toc466377493)

[Getevent 53](#_Toc466377494)

[Sendevent 59](#_Toc466377495)

[Input 59](#_Toc466377496)

[参考资料 61](#_Toc466377497)

[ARM概念梳理：Architecture, Core, CPU，SOC 62](#_Toc466377498)

[概念梳理 62](#_Toc466377499)

[ARM 64bit 62](#_Toc466377500)

[参考资料 63](#_Toc466377501)

[pmic与pmu的区别 63](#_Toc466377502)

[Linux中SD/MMC设备驱动流程 64](#_Toc466377503)

[SD（Secure Digital）与 MMC（Multimedia Card） 64](#_Toc466377504)

[SDIO（Secure Digital I/O） 64](#_Toc466377505)

[SD/SDIO/MMC/SPI之间的关系 64](#_Toc466377506)

[同一个控制器，支持SD/MMC/SDIO的所以卡，如何区分出现在卡槽里的是个什么卡 65](#_Toc466377507)

[SD/SDIO 的传输模式 65](#_Toc466377508)

[参考资料 66](#_Toc466377509)

[内核通知链 67](#_Toc466377510)

[notifier chain 定义和接口 67](#_Toc466377511)

[1、Atomic notifier chains 67](#_Toc466377512)

[2、Blocking notifier chains 68](#_Toc466377513)

[3、Raw notifier chains 68](#_Toc466377514)

[4、SRCU notifier chains 69](#_Toc466377515)

[5、notifier\_call\_chain 69](#_Toc466377516)

[notifier chain 使用方法 70](#_Toc466377517)

[参考资料 70](#_Toc466377518)

[Socket通信机制 71](#_Toc466377519)

[socket套接字： 71](#_Toc466377520)

[套接字描述符： 71](#_Toc466377521)

[文件描述符和文件指针的区别： 72](#_Toc466377522)

[基本的SOCKET接口函数 73](#_Toc466377523)

[socket()函数 74](#_Toc466377524)

[bind()函数 74](#_Toc466377525)

[网络字节序与主机字节序 76](#_Toc466377526)

[listen()、connect()函数 76](#_Toc466377527)

[accept()函数 76](#_Toc466377528)

[read()、write()等函数 77](#_Toc466377529)

[close()函数 78](#_Toc466377530)

[Netlink机制及其关键技术 79](#_Toc466377531)

[3.1 Netlink机制 79](#_Toc466377532)

[3.2 Netlink优点 80](#_Toc466377533)

[建立Netlink会话过程如下： 80](#_Toc466377534)

[参考资料 92](#_Toc466377535)

[Linux工作队列 93](#_Toc466377536)

[1. 什么是workqueue 93](#_Toc466377537)

[2. 数据结构 93](#_Toc466377538)

[3. 创建工作 95](#_Toc466377539)

[4. 调度 97](#_Toc466377540)

[5. 示例 98](#_Toc466377541)

[参考资料 99](#_Toc466377542)

# 热插拔

一个完整的**热插拔系统包括热插拔系统的硬件，支持热插拔的软件和操作系统**，**支持热插拔的设备驱动程序和支持热插拔的用户接口**。

**硬件支持：**插入->先数据，后电源；拔出->先电源，后数据(具体硬件机理不详)

**软件支持：**uevent, user space event. 内核与用户空间的一种通信机制，netlink通信机制

**Uevent**是**Kobject**的一部分，用于在Kobject状态发生改变时，例如增加、移除等，通知用户空间程序。用户空间程序收到这样的事件后，会做相应的处理。

该机制通常是用来支持热拔插设备的，例如U盘插入后，USB相关的驱动软件会动态创建用于表示该U盘的device结构（相应的也包括其中的kobject），并告知用户空间程序，为该U盘动态的创建/dev/目录下的设备节点，更进一步，可以通知其它的应用程序，将该U盘设备mount到系统中，从而动态的支持该设备。

**Uevent的机制：**设备模型中任何设备有事件需要上报时，会触发Uevent提供的接口。Uevent模块准备好上报事件的格式后，可以通过两个途径把事件上报到用户空间：一种是通过kmod模块，直接调用用户空间的可执行文件；另一种是通过netlink通信机制，将事件从内核空间传递给用户空间。

如图来自蜗居科技：http://www.wowotech.net/linux\_kenrel/uevent.html



##### 内部动作

通过kobject.h，uevent模块提供了如下的API（这些API的实现是在"lib/kobject\_uevent.c”文件中）：

1: /\* include/linux/kobject.h, line 206 \*/

2: int kobject\_uevent(struct kobject \*kobj, enum kobject\_action action);

3: int kobject\_uevent\_env(struct kobject \*kobj, enum kobject\_action action, char \*envp[]);

6: \_\_printf(2, 3)

7: int add\_uevent\_var(struct kobj\_uevent\_env \*env, const char \*format, ...);

9: int kobject\_action\_type(const char \*buf, size\_t count, enum kobject\_action \*type);

kobject\_uevent\_env，以envp为环境变量，上报一个指定action的uevent。环境变量的作用是为执行用户空间程序指定运行环境。具体动作如下：

* 查找kobj本身或者其parent是否从属于某个kset，如果不是，则报错返回（注2：由此可以说明，如果一个kobject没有加入kset，是不允许上报uevent的）
* 查看kobj->uevent\_suppress是否设置，如果设置，则忽略所有的uevent上报并返回（注3：由此可知，可以通过Kobject的uevent\_suppress标志，管控Kobject的uevent的上报）
* 如果所属的kset有uevent\_ops->filter函数，则调用该函数，过滤此次上报（注4：这佐证了3.2小节有关filter接口的说明，kset可以通过filter接口过滤不希望上报的event，从而达到整体的管理效果）
* 判断所属的kset是否有合法的名称（称作subsystem，和前期的内核版本有区别），否则不允许上报uevent
* 分配一个用于此次上报的、存储环境变量的buffer（结果保存在env指针中），并获得该Kobject在sysfs中路径信息（用户空间软件需要依据该路径信息在sysfs中访问它）
* 调用add\_uevent\_var接口（下面会介绍），将Action、路径信息、subsystem等信息，添加到env指针中
* 如果传入的envp不空，则解析传入的环境变量中，同样调用add\_uevent\_var接口，添加到env指针中
* 如果所属的kset存在uevent\_ops->uevent接口，调用该接口，添加kset统一的环境变量到env指针
* 根据ACTION的类型，设置kobj->state\_add\_uevent\_sent和kobj->state\_remove\_uevent\_sent变量，以记录正确的状态
* 调用add\_uevent\_var接口，添加格式为"SEQNUM=%llu”的序列号
* **如果定义了"CONFIG\_NET”，则使用netlink发送该uevent**
* **以uevent\_helper、subsystem以及添加了标准环境变量（HOME=/，PATH=/sbin:/bin:/usr/sbin:/usr/bin）的env指针为参数，调用kmod模块提供的call\_usermodehelper函数，上报uevent。**  
  其中uevent\_helper的内容是由内核配置项CONFIG\_UEVENT\_HELPER\_PATH(位于./drivers/base/Kconfig)决定的(可参考lib/kobject\_uevent.c, line 32)，该配置项指定了一个用户空间程序（或者脚本），用于解析上报的uevent，例如"/sbin/hotplug”。   
  call\_usermodehelper的作用，就是fork一个进程，以uevent为参数，执行uevent\_helper。

kobject\_uevent，和kobject\_uevent\_env功能一样，只是没有指定任何的环境变量。

add\_uevent\_var，以格式化字符的形式（类似printf、printk等），将环境变量copy到env指针中。

kobject\_action\_type，将enum kobject\_action类型的Action，转换为字符串。

上面所说的过程可以去除driver部分，简化如下：  
① 外设插入；  
② 总线发现（中断？ usb有中断hub\_irq，pci的中断没找到）新设备，调用device\_add，添加新设备到设备管理系统；  
③ device\_add中调用kobject\_uevent(, KOBJ\_ADD)，向userspace广播新设备加入event通知；这里发出通知的方式，就是netlink；  
④ 用户空间运行的daemon(udevd)收到event事件广播；udevd (udev 后台程序)  
⑤ udevd根据消息和环境变量，查询/sys的变化，按照规则(/etc/udev/rules.d/\*)，在/dev目录下自动创建设备节点；

## 参考资料

http://www.wowotech.net/linux\_kenrel/uevent.html 主要讲述的是头文件热插拔事件从内核空间到用户空间

http://blog.csdn.net/bingqingsuimeng/article/details/7924300 有源代码的讲解，比较清晰

http://www.cnblogs.com/image-eye/archive/2011/08/19/2145858.html 内核启动过程的驱动加载

http://blog.chinaunix.net/uid-25721104-id-3023525.html 讨论的关于热插拔

http://blog.csdn.net/zirconsdu/article/details/8792184 图解很清晰

http://blog.chinaunix.net/uid-27666459-id-5747129.html讲解call\_usermodehelper

ps：[**kobject\_uevent\_env**](http://lxr.free-electrons.com/ident?i=kobject_uevent_env)**里面有定义是通过**

**#ifdef CONFIG\_UEVENT\_HELPER**

**#if defined(CONFIG\_NET)**

**两种机制的哪一种**

# Sysfs以及设备模型

Sysfs被加载在 /sys/目录下,它的子目录包括

1）Block:在系统中发现的每个块设备在该目录下对应一个子目录。每个子目录中又包含一些属性文件,它们描述了这个块设备的各方面属性,如:设备大小。(loop块设备是使用文件来模拟的)

2）Bus:在内核中注册的每条总线在该目录下对应一个子目录,如: ide pci scsi usbpcmcia 其中每个总线目录内又包含两个子目录:devices和drivers ,devices目录包含了在整个系统中发现的属于该总线类型的设备,drivers目录包含了注册到该总线的所有驱动。

3）Class:将设备按照功能进行的分类,如/sys/class/net目录下包含了所有网络接口。

4）Devices:包含系统所有的设备。

5）Kernel:内核中的配置参数

6）Module:系统中所有模块的信息

7）Firmware:系统中的固件

8）Fs:描述系统中的文件系统

9）Power:系统中电源选项

## 内核空间与用户空间的映射关系

内核空间(internel) ——->用户空间(externel)  
内核对象(kernel objects) ——->目录(directories)  
对象属性(object attributes) ——->普通文件(regular files)  
对象关系(object relationships) ——->符号链接(symbolic links)

## 设备模型底层容器

### struct kobj

struct kobject {

const char \*name; //kobject的名称

struct list\_head entry; //kobject结构链表

struct kobject \*parent; //父kobject结构体

struct kset \*kset; //kset集合

struct kobj\_type \*ktype; //kobject的类型描述符

struct sysfs\_dirent \*sd; //sysfs文件目录

struct kref kref; //kobject引用计数

#ifdef CONFIG\_DEBUG\_KOBJECT\_RELEASE

struct [delayed\_work](http://lxr.free-electrons.com/ident?i=delayed_work) [release](http://lxr.free-electrons.com/ident?i=release);

#endif

unsigned int state\_initialized:1; //kobject是否初始化

unsigned int state\_in\_sysfs:1; //是否已经加入sysfs

unsigned int state\_add\_uevent\_sent:1;

unsigned int state\_remove\_uevent\_sent:1;

unsigned int uevent\_suppress:1;

};

### struct kobj\_type

struct kobj\_type {

void (\*release)(struct kobject \*kobj); //释放函数（驱动编写时提供），此函数会被kobject\_put函数调用

struct sysfs\_ops \*sysfs\_ops; //属性文件的操作函数（只有读和写操作）

struct attribute \*\*default\_attrs; //属性数组

const struct kobj\_ns\_type\_operations \*(\*child\_ns\_type)(struct kobject \*kobj);

const void \*(\*namespace)(struct kobject \*kobj);

};

### struct kset

struct kset {

struct list\_head list; //这个链表存放这个kset关联的所有kobject

spinlock\_t list\_lock; //维护此链表的锁

struct kobject kobj; //内嵌的kobject。这样kset本身也是一个kobject也被表现为一个目录

struct kset\_uevent\_ops \*uevent\_ops; //支持热插拔事件的函数集

};

### struct kobj\_attribute

struct kobj\_attribute {

struct attribute attr;

ssize\_t (\*show)(struct kobject \*kobj, struct kobj\_attribute \*attr,

char \*buf);

ssize\_t (\*store)(struct kobject \*kobj, struct kobj\_attribute \*attr,

const char \*buf, size\_t count);

};

## 设备模型上层容器

### 总线类型bus\_type

struct bus\_type {

const char \*name; /\* 总线类型名 \*/

struct bus\_attribute \*bus\_attrs; /\* 总线的属性 \*/

struct device\_attribute \*dev\_attrs; /\* 设备属性,为每个加入总线的设备建立属性链表 \*/

struct driver\_attribute \*drv\_attrs; /\* 驱动属性,为每个加入总线的驱动建立属性链表 \*/

/\* 驱动与设备匹配函数:当一个新设备或者驱动被添加到这个总线时，这个方法会被调用一次或多次，若指定的驱动程序能够处理指定的设备，则返回非零值。必须在总线层使用这个函数, 因为那里存在正确的逻辑，核心内核不知道如何为每个总线类型匹配设备和驱动程序 \*/

int (\*match)(struct device \*dev, struct device\_driver \*drv);

/\*在为用户空间产生热插拔事件之前，这个方法允许总线添加环境变量（参数和 kset 的uevent方法相同）\*/

int (\*uevent)(struct device \*dev, struct kobj\_uevent\_env \*env);

int (\*probe)(struct device \*dev); /\* \*/

int (\*remove)(struct device \*dev); /\* 设备移除调用操作 \*/

void (\*shutdown)(struct device \*dev);

int (\*suspend)(struct device \*dev, pm\_message\_t state);

int (\*resume)(struct device \*dev);

const struct dev\_pm\_ops \*pm;

struct subsys\_private \*p; /\* 一个很重要的域，包含了device链表和drivers链表 \*/

};

/\*\*

63 \* struct bus\_type - The bus type of the device

64 \*

65 \* @name: The name of the bus.

66 \* @dev\_name: Used for subsystems to enumerate devices like ("foo%u", dev->id).

67 \* @dev\_root: Default device to use as the parent.

68 \* @dev\_attrs: Default attributes of the devices on the bus.

69 \* @bus\_groups: Default attributes of the bus.

70 \* @dev\_groups: Default attributes of the devices on the bus.

71 \* @drv\_groups: Default attributes of the device drivers on the bus.

72 \* @match: Called, perhaps multiple times, whenever a new device or driver

73 \* is added for this bus. It should return a positive value if the

74 \* given device can be handled by the given driver and zero

75 \* otherwise. It may also return error code if determining that

76 \* the driver supports the device is not possible. In case of

77 \* -EPROBE\_DEFER it will queue the device for deferred probing.

78 \* @uevent: Called when a device is added, removed, or a few other things

79 \* that generate uevents to add the environment variables.

80 \* @probe: Called when a new device or driver add to this bus, and callback

81 \* the specific driver's probe to initial the matched device.

82 \* @remove: Called when a device removed from this bus.

83 \* @shutdown: Called at shut-down time to quiesce the device.

84 \*

85 \* @online: Called to put the device back online (after offlining it).

86 \* @offline: Called to put the device offline for hot-removal. May fail.

87 \*

88 \* @suspend: Called when a device on this bus wants to go to sleep mode.

89 \* @resume: Called to bring a device on this bus out of sleep mode.

90 \* @pm: Power management operations of this bus, callback the specific

91 \* device driver's pm-ops.

92 \* @iommu\_ops: IOMMU specific operations for this bus, used to attach IOMMU

93 \* driver implementations to a bus and allow the driver to do

94 \* bus-specific setup

95 \* @p: The private data of the driver core, only the driver core can

96 \* touch this.

97 \* @lock\_key: Lock class key for use by the lock validator

98 \*

99 \* A bus is a channel between the processor and one or more devices. For the

100 \* purposes of the device model, all devices are connected via a bus, even if

101 \* it is an internal, virtual, "platform" bus. Buses can plug into each other.

102 \* A USB controller is usually a PCI device, for example. The device model

103 \* represents the actual connections between buses and the devices they control.

104 \* A bus is represented by the bus\_type structure. It contains the name, the

105 \* default attributes, the bus' methods, PM operations, and the driver core's

106 \* private data.

107 \*/

108 struct bus\_type {

109 const char \*name;

110 const char \*dev\_name;

111 struct device \*dev\_root;

112 struct device\_attribute \*dev\_attrs; /\* use dev\_groups instead \*/

113 const struct attribute\_group \*\*bus\_groups;

114 const struct attribute\_group \*\*dev\_groups;

115 const struct attribute\_group \*\*drv\_groups;

116

117 int (\*match)(struct device \*dev, struct device\_driver \*drv);

118 int (\*uevent)(struct device \*dev, struct kobj\_uevent\_env \*env);

119 int (\*probe)(struct device \*dev);

120 int (\*remove)(struct device \*dev);

121 void (\*shutdown)(struct device \*dev);

122

123 int (\*online)(struct device \*dev);

124 int (\*offline)(struct device \*dev);

125

126 int (\*suspend)(struct device \*dev, pm\_message\_t state);

127 int (\*resume)(struct device \*dev);

128

129 const struct dev\_pm\_ops \*pm;

130

131 const struct iommu\_ops \*iommu\_ops;

132

133 struct subsys\_private \*p;

134 struct lock\_class\_key lock\_key;

135 };

### Struct device

709 /\*\*

710 \* struct device - The basic device structure

711 \* @parent: The device's "parent" device, the device to which it is attached.

712 \* In most cases, a parent device is some sort of bus or host

713 \* controller. If parent is NULL, the device, is a top-level device,

714 \* which is not usually what you want.

715 \* @p: Holds the private data of the driver core portions of the device.

716 \* See the comment of the struct device\_private for detail.

717 \* @kobj: A top-level, abstract class from which other classes are derived.

718 \* @init\_name: Initial name of the device.

719 \* @type: The type of device.

720 \* This identifies the device type and carries type-specific

721 \* information.

722 \* @mutex: Mutex to synchronize calls to its driver.

723 \* @bus: Type of bus device is on.

724 \* @driver: Which driver has allocated this

725 \* @platform\_data: Platform data specific to the device.

726 \* Example: For devices on custom boards, as typical of embedded

727 \* and SOC based hardware, Linux often uses platform\_data to point

728 \* to board-specific structures describing devices and how they

729 \* are wired. That can include what ports are available, chip

730 \* variants, which GPIO pins act in what additional roles, and so

731 \* on. This shrinks the "Board Support Packages" (BSPs) and

732 \* minimizes board-specific #ifdefs in drivers.

733 \* @driver\_data: Private pointer for driver specific info.

734 \* @power: For device power management.

735 \* See Documentation/power/devices.txt for details.

736 \* @pm\_domain: Provide callbacks that are executed during system suspend,

737 \* hibernation, system resume and during runtime PM transitions

738 \* along with subsystem-level and driver-level callbacks.

739 \* @pins: For device pin management.

740 \* See Documentation/pinctrl.txt for details.

741 \* @msi\_list: Hosts MSI descriptors

742 \* @msi\_domain: The generic MSI domain this device is using.

743 \* @numa\_node: NUMA node this device is close to.

744 \* @dma\_mask: Dma mask (if dma'ble device).

745 \* @coherent\_dma\_mask: Like dma\_mask, but for alloc\_coherent mapping as not all

746 \* hardware supports 64-bit addresses for consistent allocations

747 \* such descriptors.

748 \* @dma\_pfn\_offset: offset of DMA memory range relatively of RAM

749 \* @dma\_parms: A low level driver may set these to teach IOMMU code about

750 \* segment limitations.

751 \* @dma\_pools: Dma pools (if dma'ble device).

752 \* @dma\_mem: Internal for coherent mem override.

753 \* @cma\_area: Contiguous memory area for dma allocations

754 \* @archdata: For arch-specific additions.

755 \* @of\_node: Associated device tree node.

756 \* @fwnode: Associated device node supplied by platform firmware.

757 \* @devt: For creating the sysfs "dev".

758 \* @id: device instance

759 \* @devres\_lock: Spinlock to protect the resource of the device.

760 \* @devres\_head: The resources list of the device.

761 \* @knode\_class: The node used to add the device to the class list.

762 \* @class: The class of the device.

763 \* @groups: Optional attribute groups.

764 \* @release: Callback to free the device after all references have

765 \* gone away. This should be set by the allocator of the

766 \* device (i.e. the bus driver that discovered the device).

767 \* @iommu\_group: IOMMU group the device belongs to.

768 \*

769 \* @offline\_disabled: If set, the device is permanently online.

770 \* @offline: Set after successful invocation of bus type's .offline().

771 \*

772 \* At the lowest level, every device in a Linux system is represented by an

773 \* instance of struct device. The device structure contains the information

774 \* that the device model core needs to model the system. Most subsystems,

775 \* however, track additional information about the devices they host. As a

776 \* result, it is rare for devices to be represented by bare device structures;

777 \* instead, that structure, like kobject structures, is usually embedded within

778 \* a higher-level representation of the device.

779 \*/

780 struct device {

781 struct device \*parent;

782

783 struct device\_private \*p;

784

785 struct kobject kobj;

786 const char \*init\_name; /\* initial name of the device \*/

787 const struct device\_type \*type;

788

789 struct mutex mutex; /\* mutex to synchronize calls to

790 \* its driver.

791 \*/

792

793 struct bus\_type \*bus; /\* type of bus device is on \*/

794 struct device\_driver \*driver; /\* which driver has allocated this

795 device \*/

796 void \*platform\_data; /\* Platform specific data, device

797 core doesn't touch it \*/

798 void \*driver\_data; /\* Driver data, set and get with

799 dev\_set/get\_drvdata \*/

800 struct dev\_pm\_info power;

801 struct dev\_pm\_domain \*pm\_domain;

802

803 #ifdef CONFIG\_GENERIC\_MSI\_IRQ\_DOMAIN

804 struct irq\_domain \*msi\_domain;

805 #endif

806 #ifdef CONFIG\_PINCTRL

807 struct dev\_pin\_info \*pins;

808 #endif

809 #ifdef CONFIG\_GENERIC\_MSI\_IRQ

810 struct list\_head msi\_list;

811 #endif

812

813 #ifdef CONFIG\_NUMA

814 int numa\_node; /\* NUMA node this device is close to \*/

815 #endif

816 u64 \*dma\_mask; /\* dma mask (if dma'able device) \*/

817 u64 coherent\_dma\_mask;/\* Like dma\_mask, but for

818 alloc\_coherent mappings as

819 not all hardware supports

820 64 bit addresses for consistent

821 allocations such descriptors. \*/

822 unsigned long dma\_pfn\_offset;

823

824 struct device\_dma\_parameters \*dma\_parms;

825

826 struct list\_head dma\_pools; /\* dma pools (if dma'ble) \*/

827

828 struct dma\_coherent\_mem \*dma\_mem; /\* internal for coherent mem

829 override \*/

830 #ifdef CONFIG\_DMA\_CMA

831 struct cma \*cma\_area; /\* contiguous memory area for dma

832 allocations \*/

833 #endif

834 /\* arch specific additions \*/

835 struct dev\_archdata archdata;

836

837 struct device\_node \*of\_node; /\* associated device tree node \*/

838 struct fwnode\_handle \*fwnode; /\* firmware device node \*/

839

840 dev\_t devt; /\* dev\_t, creates the sysfs "dev" \*/

841 u32 id; /\* device instance \*/

842

843 spinlock\_t devres\_lock;

844 struct list\_head devres\_head;

845

846 struct klist\_node knode\_class;

847 struct class \*class;

848 const struct attribute\_group \*\*groups; /\* optional groups \*/

849

850 void (\*release)(struct device \*dev);

851 struct iommu\_group \*iommu\_group;

852

853 bool offline\_disabled:1;

854 bool offline:1;

855 };

### Struct device\_driver

/\*\*

231 \* struct device\_driver - The basic device driver structure

232 \* @name: Name of the device driver.

233 \* @bus: The bus which the device of this driver belongs to.

234 \* @owner: The module owner.

235 \* @mod\_name: Used for built-in modules.

236 \* @suppress\_bind\_attrs: Disables bind/unbind via sysfs.

237 \* @probe\_type: Type of the probe (synchronous or asynchronous) to use.

238 \* @of\_match\_table: The open firmware table.

239 \* @acpi\_match\_table: The ACPI match table.

240 \* @probe: Called to query the existence of a specific device,

241 \* whether this driver can work with it, and bind the driver

242 \* to a specific device.

243 \* @remove: Called when the device is removed from the system to

244 \* unbind a device from this driver.

245 \* @shutdown: Called at shut-down time to quiesce the device.

246 \* @suspend: Called to put the device to sleep mode. Usually to a

247 \* low power state.

248 \* @resume: Called to bring a device from sleep mode.

249 \* @groups: Default attributes that get created by the driver core

250 \* automatically.

251 \* @pm: Power management operations of the device which matched

252 \* this driver.

253 \* @p: Driver core's private data, no one other than the driver

254 \* core can touch this.

255 \*

256 \* The device driver-model tracks all of the drivers known to the system.

257 \* The main reason for this tracking is to enable the driver core to match

258 \* up drivers with new devices. Once drivers are known objects within the

259 \* system, however, a number of other things become possible. Device drivers

260 \* can export information and configuration variables that are independent

261 \* of any specific device.

262 \*/

263 struct device\_driver {

264 const char \*name;

265 struct bus\_type \*bus;

266

267 struct module \*owner;

268 const char \*mod\_name; /\* used for built-in modules \*/

269

270 bool suppress\_bind\_attrs; /\* disables bind/unbind via sysfs \*/

271 enum probe\_type probe\_type;

272

273 const struct of\_device\_id \*of\_match\_table;

274 const struct acpi\_device\_id \*acpi\_match\_table;

275

276 int (\*probe) (struct device \*dev);

277 int (\*remove) (struct device \*dev);

278 void (\*shutdown) (struct device \*dev);

279 int (\*suspend) (struct device \*dev, pm\_message\_t state);

280 int (\*resume) (struct device \*dev);

281 const struct attribute\_group \*\*groups;

282

283 const struct dev\_pm\_ops \*pm;

284

285 struct driver\_private \*p;

286 };

## 从面向对象的角度

- struct kobj（及其相关结构如kset, ktype等）属于最抽象的基类，代码最简洁，最不具体； 通常我们并不关注 kobject 本身，而应该关注那些嵌入了 kobject 的那些结构体。；ktype 是嵌入了 kobject 的对象的类型。每个嵌入了 kobject 的对象都需要一个相应的 ktype。ktype 用来控制当 kobject 创建和销毁时所发生的操作。 这些 kobject 可以是同样的 ktype，也可以分别属于不同的 ktype。kset 是 kobject 集合的基本容器类型。kset 是 kobject 的一组集合。kset 也包含它们自己的 kobject，但是你可以放心的忽略这些 kobjects，因为 kset 的核心代码会自动处理这些 kobject。

- struct device（及其相关结构如device\_driver，device\_type等）是对kobj的封装，是第一层派生类；

- 再上层的结构（如platform\_device等），是在struct device的基础上再封装一次，是第二层派生类。

因此，例如我们创建了一个struct platform\_device的实例，使用完毕后要释放它。那么这个过程按道理应该是：

- 系统内部先调用platform\_device的remove函数，它只处理自己层特有的变量；

- 完毕后，系统调用第一层派生类struct device的release函数，处理了自己这一层的特有变量；

- 最后，kobject的release函数，将整个空间释放掉。

整个过程应该会跟C++析构过程比较类似，上述的“系统内部”也应该类似于C++编译器自动生成的代码，因为C++中析构函数的逆向调用是自动进行的，并没有在派生类的析构函数中显示调用。类似地，在此处上层的release中也不会显式调用下层release，都是由系统内部完成的。

## Kobject，kset，ktype结构图

一个kobject结构如下图的kobject 类型部分，而一个kset结构如下图的kset 类型部分，一个kobject加入一个kset，主要是kobject结构体中的相关字段记录了对应的kset信息，①记录了kobject所对应 kset，其所指向的是kset所包含的kobject的地址，②记录了kobject所对应的kset的kset指针，③记录了kobject的类 型，④记录了kset所有的kobject的链子，这个链子是一个双向链表，每当有一个kobject加入到当前的kset,就会调用 list\_add\_tail()函数，把要加入kset的kobject连入链表的结尾，最终形成一个链表。



当有另外一个kobject要加入当前的kset，其中的①②③步跟第一个加入当前kset的kobject是一样的，即把要加入 的kobject的成员设置，使之指向当前的kset对应数据，而④需要把kobject添加到kset的list的尾部，下图表示了kobject b加入到kset A的图示：



当有一个kset，需要加入到当前的kset,其方法也跟一个kobject要加入到当前kset一样，即把要加入的kset中所 包含的kobject的成员设置，使这些成员指向对应的kset的对应数据。而当前kset要加入另一个kset，其方式也是跟一个kset加入到当前 kset一样，都是设备kset中的kobject，使kobject的成员指向要加入的kset的对应数据即可，下图显示了一个kset B加入到kset A中的图示。



由于一条总线要管理总线上的所有驱动，同时要管理总线上的有所设备，则需要再把所有设备和所有驱动都分开，分别设立一个设 备kset和一个设备驱动kset，用于管理所有的设备和设备驱动，如此，则总线kset实际上包含了两个kset（设备kset，设备驱动kset）， 设备kset又包含了所有的当前总线的设备的kobject，设备驱动kset包含了所有的当前总线的设备驱动的kobject；而所有的总线，又形成了 bus kset，归结起来就形成下图的层次关系：



经过上述的设备插入，或者驱动安装，系统就会出现只有设备，而没有设备驱动程序的情况，也会出现，只有设备驱动程序，没有对应的设备的情况，此时，设备或者设备驱动程序，就会暂时在各自的队列里等待，一旦有驱动程序安装，或新的设备插入，就都会自动的去扫描对应的链表，来检测是否有配对的可能。

综合上述三者的关系，如图：



## **Kobj type**

数据结构包含三个域：一个release方法用于释放kobject占用的资源；一个sysfs ops指针指向sysfs操作表和一个sysfs文件系统缺省属性列表。Sysfs操作表包括两个函数store()和show()。当用户态读取属性时，show()函数被调用，该函数编码指定属性值存入buffer中返回给用户态；而store()函数用于存储用户态传入的属性值。

## 参考资料

http://eeepage.info/sysfs/ 对新的sysfs的讲解非常到位

http://www.linuxidc.com/Linux/2012-05/60757.htm 同样讲解sysfs文件系统

http://blog.chinaunix.net/uid-24227137-id-3266449.html 讲解kobject,kset,sysfs

http://blog.csdn.net/xiahouzuoxin/article/details/8943863

# 最小子系统+ramdisk+initrd+系统启动过程

## ramdisk+initrd

ramdisk是一种基于内存的虚拟文件系统，通常用于放置内核的中间数据。

而initrd全称为"boot loader initialized RAM disk"，也就是由启动加载器所初始化的RamDisk设备，它的作用是完善内核的模块机制，让内核的初始化流程更具弹性；内核以及initrd，都由bootloader在机子启动后被加载至内存的指定位置，主要功能为按需加载模块以及按需改变根文件系统。initrd 大体上就是指包含根文件系统的ramdisk。initrd即initial ramdisk,它是在系统引导过程中挂载的一个临时根文件系统.激活系统所须加载的文件系统.



### BIOS(Basic Input Output System)

可以视为是一个永久地记录在ROM中的一个软件，是操作系统输入输出管理系统的一部分

包括：

**自检及初始化**

POST上电自检（如果内存没有插好，开机会滴滴的响，这就是上电自检查处了问题）

**初始化**

程序服务处理

硬件中断处理

枚举本地设备并对其初始化;’

BIOS在内存中建立中断向量表和中断服务程序

系统设置程序（开机按f2或者f12跳出来的配置界面就是配置这个参数）：准确的说法应是通过BIOS设置程序对CMOS参数进行设置

以硬盘启动为例，BIOS此时去读取硬盘驱动器的第一个扇区(MBR，512字节)，然后执行里面的代码；**将控制权转交给MBR**

### 系统引导

MBR，它是Master Boot Record的缩写。硬盘的0柱面、0磁头、1扇区称为主引导扇区。它由三个部分组成，**主引导程序(Bootloader)**、 **硬盘分区表DPT（Disk Partition table）**和**硬盘有效标志（55AA）**，其结构图如下所示：



        磁盘分区表包含以下三部分：

        1）Partition ID  （5：延伸  82：Swap   83：Linux   8e：LVM     fd：RAID）

        2）Partition起始磁柱

        3）Partition的磁柱数量

       通常情况下，诸如lilo、grub这些常见的引导程序都直接安装在MBR中。我们以grub为例来分析这个引导过程。

       grub引导也分为两个阶段stage1阶段和stage2阶段(有些较新的grub又定义了stage1.5阶段)。

        1)stage1：stage1是直接被写入到MBR中去的，也就是上图所看到的前446个字节空间中存放的是stage1的代码。BIOS将stage1载入内存中0x7c00处并跳转执行。stage1（/stage1/start.S）仅仅是将硬盘0头0道2扇区读入内存。而0头0道2扇区内容是源代码中的/stage2/start.S，编译后512字节，它是stage2或者stage1\_5的入口。

         2)stage2：严格来说这里还应该再区分个stage1.5的，就一并把stage1.5放在这里一起介绍了，免得大家看得心里乱哄哄的。好的，我们继续说0头0到2扇区的/stage2/start.S文件，当它的内容被读入到内存之后，它的主要作用就是负责将stage2或stage1.5从硬盘读到内存中。如果是stage2，它将被载入到0x820处；如果是stage1.5，它将被载入到0x2200处。这里的stage2或者stage1\_5不是/boot分区/boot/grub目录下的文件，因为这个时候grub还没有能力识别任何文件系统。

        如果start.S加载stage1.5：stage1.5它存放在硬盘0头0道3扇区向后的位置，stage1\_5作为stage1和stage2中间的桥梁，stage1\_5有识别文件系统的能力，此后grub才有能力去访问/boot分区/boot/grub目录下的 stage2文件，将stage2载入内存并执行。

        如果start.S加载stage2：同样，这个stage2也不是/boot分区/boot/grub目录下的stage2，这个时候start.S读取的是存放在/boot分区Boot Sector的stage2。这种情况下就有一个限制：因为start.S通过BIOS中断方式直接对硬盘寻址（而非通过访问具体的文件系统），其寻址范围有限，限制在8GB以内。因此这种情况需要将/boot分区分在硬盘8GB寻址空间之前。

        假如是情形2，我们将/boot/grub目录下的内容清空，依然能成功启动grub；假如是情形1，将/boot/grub目录下stage2删除后，则系统启动过程中grub会启动失败。



而最终 boot loader 的功能就是加载 kernel（内核）文件

 Linux 内核是可以通过动态加载内核模块的 (就请想成驱动程序即可)，这些内核模块就放置在 /lib/modules/ 目录内。 由于模块放置到磁盘根目录内 (要记得 /lib 不可以与 / 分别放在不同的分区)，因此在启动的过程中内核必须要挂载根目录，这样才能够读取内核模块提供加载驱动程序的功能。而且为了避免影响到磁盘内的文件系统，因此启动过程中根目录是以只读的方式来挂载。

一般来说，非必要的功能且可以编译成为模块的内核功能，目前的 Linux distributions 都会将它编译成为模块。因此 U盘, SATA, SCSI... 等磁盘设备的驱动程序通常都是以模块的方式来存在的。现在来思考一种情况，假设你的 linux 是安装在 SATA 磁盘上面的，你可以通过 BIOS 的 INT 13 取得 boot loader 与 kernel 文件来启动，然后 kernel 会开始接管系统并且检测硬件及尝试挂载根目录来取得额外的驱动程序。

问题是，内核根本不认识 SATA 磁盘，所以需要加载 SATA 磁盘的驱动程序，否则根本就无法挂载根目录。但是 SATA 的驱动程序在 /lib/modules 内，你根本无法挂载根目录，又怎么读取到 /lib/modules/ 内的驱动程序？是吧！是不是有点进退两难？在这个情况之下，你的 Linux 是无法顺利启动的！ 那怎办？没关系，我们可以透过虚拟文件系统来处理这个问题。

虚拟文件系统 (Initial RAM Disk) 一般使用的文件名为 /boot/initrd ，这个文件的特色是，它也能够通过boot loader 来加载到内存中， 然后这个文件会被解压缩并且在内存当中仿真成一个根目录，且此仿真在内存当中的文件系统能够提供一个可执行的程序，通过该程序来加载启动过程中所最需要的内核模块，通常这些模块就是 U盘, RAID, LVM, SCSI 等文件系统与磁盘接口的驱动程序。等载入完成后，会帮助内核重新调用 /sbin/init 来开始后续的正常启动流程，如图



一张图片关于bios以后的bootloader 这张图片 讲解的非常详细



## 参考资料

<http://blog.chinaunix.net/uid-23069658-id-3142047.html>

<http://blog.sina.com.cn/s/blog_c70e10380102w9b5.html>

<http://blog.csdn.net/miss_acha/article/details/50004717>

<http://www.2cto.com/os/201603/494064.html>

http://blog.itpub.net/8111049/viewspace-680043

<http://www.ibm.com/developerworks/cn/linux/l-initrd.html>

<http://bbs.chinaunix.net/thread-2046548-1-1.html>

http://bbs.chinaunix.net/thread-2046548-1-1.html

小知识：

\*.o 中间文件

\*.so 文件是动态链接库文件，相当于 win下的 .dll 文件。

\*.a 文件是静态库文件。

\*.ko 是内核模块文件，是内核加载的某个模块，一般是驱动程序。

具体的编译命令请百度

# Paltform

## Platform设备驱动

可以通过CPU bus直接寻址（例如在嵌入式系统常见的“寄存器”）。因此，由于这个共性，内核在设备模型的基础上（device和device\_driver），对这些设备进行了更进一步的封装，抽象出paltform bus、platform device和platform driver，以便驱动开发人员可以方便的开发这类设备的驱动。

Platform设备驱动包含三部分：**Platform总线**，**Platform设备**，**Platform设备驱动**

然而这三者是基于设备模型的概念：总线，设备与驱动。

## Platform模块的软件架构

内核中Platform设备有关的实现位include/linux/platform\_device.h和drivers/base/platform.c两个文件中，它的软件架构如下：



结合之前的知识讲解一下这幅图：每一个单独的结构体都是一个kobject（上图中的bus,device,device\_driver,platformbus,platform\_device,platform\_driver）；内核对这些东西又有一个整理，所有的bus是一个kset；所有的device是一个kset；所有的driver是一个kset；而ktype则是对这些kobject的附属操作。

Platform Bus，基于底层bus模块，抽象出一个虚拟的Platform bus，用于挂载Platform设备；

Platform Device，基于底层device模块，抽象出Platform Device，用于表示Platform设备；

Platform Driver，基于底层device\_driver模块，抽象出Platform Driver，用于驱动Platform设备。

其中Platform Device和Platform Driver会为其它Driver提供封装好的API

## Platform模块向其它模块提供的API汇整

Platform提供的接口包括：Platform Device和Platform Driver两个数据结构，以及它们的操作函数

用于抽象Platform设备的数据结构----“struct platform\_device”：

用于抽象Platform设备驱动的数据结构----“struct platform\_driver”：

具体的各类api请参考：<http://www.wowotech.net/device_model/platform_device.html>

## 总结大多数驱动框架

## Platform led驱动

最简单的了解platform平台的例子，可以理解为3部分，由驱动层，系统核心层，设备驱动三部分组成：

驱动层：硬件设备注册部分。

系统核心层：无

设备驱动层：设备端的实现，如led闪烁等

实际上之所以这里分成3部分，是为了与后面的设备驱动程序对应起来。

使用步骤示例：

(1)platform\_device\_register()：注册平台led设备。

(2)platform\_driver\_register()：注册平台led驱动。

## Platform input驱动

Linux系统提供了input子系统，按键、触摸屏、键盘、鼠标等输入都可以利用input接口函数来实现设备驱动。

在linux主要由驱动层，系统核心层(Input Core)和事件处理层（Event Handler）三部份组成。

驱动层：硬件设备注册部分，只是把输入设备注册到input子系统中，在驱动层的代码本身并不创建结点。对应文件如gpio\_key.c

Input core：向系统报告按键、触摸屏、键盘、鼠标等输入事件(event,通过input\_event结构体描述)，使得驱动层不需要关心文件操作接口。对应文件如Input.c

Event Handler：提供input设备接口。 对应文件如evdev.c,mousedev.c等。

**一般来说，如果要使用input子系统，只需要更改驱动层部分就可以了。**

## Platform i2c驱动

Linux系统中,i2c驱动由3部分组成，即i2c总线驱动、i2c core、i2c设备驱动。

I2c总线驱动：对i2c硬件体系结构中适配器端的实现，适配器可由CPU控制，或集成在CPU内部。对应文件如:i2c-at91.c

I2c core：提供了i2c总线驱动和设备驱动的注册、注销方法，i2c algorithm。与具体适配器无关的代码以及探测设备、检测设备地址的上层代码。对应文件如:i2c-core.c

I2c设备驱动：i2c体系硬件结构中设备端的实现，设备一般挂在受CPU控制的i2c适配器上，通过i2c适配器与CPU交换数据。对应文件如:at24.c,i2c-dev.c等。

对于常见的开发板来说，主芯片已经带了i2c总线，i2c总线驱动基本上提供了，不用怎么动。即使不带i2c总线，基本上也会提供io模拟的i2c，也就是说i2c总线驱动部分一般情况下不需要自己写或者更改。I2c core部分就更不用动了，呵呵。因此，写一个i2c设备的驱动，只需要写i2c设备驱动（这里对应于上面说的i2c驱动的3部分之一）就可以了。

大多数i2c设备驱动，内核已经提供了。而且简单的应用还可以利用i2c-dev.c来实现。

## Platform spi驱动

   Linux系统中，spi驱动由3部分组成，即spi总线驱动、spi core、spi设备驱动。

   Spi总线驱动:硬件spi驱动的实现，spi可为主芯片内部集成，也可以io口模拟。对应文件如：atmel\_spi.c

   Spi core:提供了spi总线驱动和设备驱动的注册、注销方法。

   Spi 设备驱动：spi体系结构中,spi设备端的实现。

综合上述几个比较简单的驱动可以看出一个共性：

这几个驱动基本都是由3部分组成：

（1） 总线驱动：与所选用的主芯片相关联，一般都有提供。

（2） 总线core：与具体的硬件无关，内核已经提供。

（3） 总线设备驱动：所操作的具体设备。根据实际应用需要，使用或更改内核已经提供的驱动，或者自己重新写一个驱动。

实际上，写一个设备驱动，我们所要做的工作基本上集中在第3部分，而这部分，内核也提供了大多数设备的驱动，即使没有提供，我们也可以根据已有的设备自己更改。

## 参考资料

<http://blog.chinaunix.net/uid-27041925-id-3884955.html>

<http://www.wowotech.net/device_model/platform_device.html>

http://blog.chinaunix.net/uid-25014876-id-111745.html

# 中断子系统

## 中断

Cpu在执行程序的过程中，出现某些突发时间急待处理，cpu必须暂时停止当前程序的执行，转去处理突发事件，处理完毕后又返回原程序被中断的位置继续执行。

外设产生中断是异步发生的，硬件设备生成中断的时候并不考虑与处理器的时钟同步——也就是说中断随时可以产生。内核随时可能因为新到来的中断而被打断。从物理学的角度看，中断是一种电信号，由硬件设备生成，并直接送入中断控制器的输入引脚。然后由中断控制器向处理器发送相应的信号。

中断是处理器和外设之间的一种通信机制，也是操作系统内核对外设进行管理的一种机制。外设通过发出特殊的电信号通知处理器发生了一次中断，处理器收到信号后就通知操作系统，然后操作系统负责做出相应的处理。

一个完整的设备中，与中断相关的硬件可以划分为3类，它们分别是：设备、中断控制器和CPU本身，下图展示了一个smp系统中的中断硬件的组成结构：



                          图  中断系统的硬件组成

**设备**  设备是发起中断的源，当设备需要请求某种服务的时候，它会发起一个硬件中断信号，通常，该信号会连接至中断控制器，由中断控制器做进一步的处理。在现代的移动设备中，发起中断的设备可以位于soc（system-on-chip）芯片的外部，也可以位于soc的内部，因为目前大多数soc都集成了大量的硬件IP，例如I2C、SPI、Display Controller等等。

Ps：中断优先寄存器，其英文缩写IP，实为“Interrupt Priority”的简写。

**中断控制器**  中断控制器负责收集所有中断源发起的中断，现有的中断控制器几乎都是可编程的，通过对中断控制器的编程，我们可以控制每个中断源的优先级、中断的电器类型，还可以打开和关闭某一个中断源，在smp系统中，甚至可以控制某个中断源发往哪一个CPU进行处理。对于ARM架构的soc，使用较多的中断控制器是VIC（Vector Interrupt Controller），进入多核时代以后，GIC（General Interrupt Controller）的应用也开始逐渐变多。

**CPU**  cpu是最终响应中断的部件，它通过对可编程中断控制器的编程操作，控制和管理者系统中的每个中断，当中断控制器最终判定一个中断可以被处理时，他会根据事先的设定，通知其中一个或者是某几个cpu对该中断进行处理，虽然中断控制器可以同时通知数个cpu对某一个中断进行处理，实际上，最后只会有一个cpu相应这个中断请求，但具体是哪个cpu进行响应是可能是随机的，中断控制器在硬件上对这一特性进行了保证，不过这也依赖于操作系统对中断系统的软件实现。在smp系统中，cpu之间也通过IPI（inter processor interrupt）中断进行通信

## IRQ编号

系统中每一个注册的中断源，都会分配一个唯一的编号用于识别该中断，我们称之为IRQ编号。IRQ编号贯穿在整个Linux的通用中断子系统中。在移动设备中，每个中断源的IRQ编号都会在arch相关的一些头文件中，例如arch/xxx/mach-xxx/include/irqs.h。驱动程序在请求中断服务时，它会使用IRQ编号注册该中断，中断发生时，cpu通常会从中断控制器中获取相关信息，然后计算出相应的IRQ编号，然后把该IRQ编号传递到相应的驱动程序中。

## 中断处理程序

      在响应一个特定中断的时候，内核会执行一个函数，该函数叫做中断处理程序或中断服务例程（interrupt service routine,ISR）。产生中断的每一个设备都有一个（中断处理程序通常不是和特定设备相关联，而是和特定中断相关联，也就是说，若一个设备可以产生 多种不同的中断，那么该设备就可以对应多个中断处理程序，相应的，该设备的驱动也就需要准备多个这样的函数。）相应的中断处理程序。一个设备的中断程序是它设备驱动程序的一部分——设备驱动程序是用于对设备进行管理的内核代码。

       在Linux中，中断处理程序看起来就是普普通通的C函数。只不过这些函数必须按照特定的类型声明，以便内核能够以标准的方式传递处理程序的信息。中断处理程序与其它内核函数的真正区别在于：中断处理程序是被内核调用来响应中断的，而它们运行于我们称之为中断上下文的特殊上下文中。

**执行在中断上下文中的代码需要注意的一些事项：**

**中断上下文中的代码不能进入休眠。**

**不能使用mutex，只能使用自旋锁，且仅当必须时。**

**中断处理函数不能直接与用户空间进行数据交换。**

**中断处理程序应该尽快结束。**

**中断处理程序不需要是可重入的，因为相同的中断处理函数不能同时在多个处理器上运行。**

**中断处理程序可能被一个优先级更高的中断处理程序所中断。为了避免这种情况，可以要求内核将中断处理程序标记为一个快速中断处理程序（将本地CPU上的所有中断禁用），不过在采取这个动作前要慎重考虑对系统的影响**

## 上半部与下半部

ISR的执行必须足够快速，这是由多种原因决定的。由于中断可以随时发生，因此ISR可以随时被执行，同时ISR打断了系统正常的流程，另外产生中断的外设也需要系统快速响应，最后由于linux不允许相同ISR中断嵌套，执行一个ISR时，当前中断线会在所有CPU上被屏蔽，这段屏蔽时间最好越短越好（否则会降低系统反应速度）。以上这些限制条件都要求ISR执行足够快速。由于速度的要求，ISR中不可能做太多的工作，而只能做一些必不可少的、跟硬件相关的工作，其他的工作就放到所谓的下半部里完成。

把中断处理划分为上半部和下半部是出于现实的考虑。上半部就是ISR，一接收到中断就立即执行，执行时禁止相同中断（必要时禁止所有中断），只做有严格时限且与硬件相关的工作，例如对接收的中断进行应答或复位硬件；而可以稍后执行或者与硬件无关的动作都放到下半部，在合适的时机下半部才开始执行。上半部和下半部的关键区别是，上半部简单快速，执行时禁止一部分或者全部中断；下半部稍后执行，而且执行期间可以响应所有中断。

举个网卡的例子，当网卡收到来自网络的数据包时，会立刻产生中断来通知内核，而内核收到中断后也会立刻调用网卡已注册的ISR，ISR会通知网卡“你的中断已经被组织收到”，并拷贝网卡收到的数据到内存。这些都是紧迫并与硬件相关的动作，如果内核不及时拷贝网卡缓存中的数据，网卡缓存很可能溢出，造成丢包现象。当数据都被拷贝到内存之后，ISR的任务算完成了，此时它将控制权转交给被它打断的程序。而处理内存中的数据的任务则落在下半部里，在内核觉得合适的时机（不太繁忙），下半部将会执行。

**上半部和下半部的划分可以参考以下原则：**

**1) 如果一个任务对时间非常敏感，把它放在上半部（ISR）里；**

**2) 如果一个任务跟硬件相关，把它放在上半部里；**

**3) 如果一个任务要保证不被其他中断（特别是相同的中断）打断，把它放在上半部里；**

**4) 其他所有的任务，都放在下半部。**

下半部负责推后完成的工作，但是并不需要指明一个具体的时间，只是将任务稍微推迟，待到系统不是那么繁忙并且中断恢复之后执行就可以了（一般情况下，ISR一返回，下半部就会执行）。不同于ISR的最关键之处是，下半部执行的时候允许响应所有的中断。内核的策略是，当中断不是特别多的时候，及时处理中断，所以do\_irq会调用do\_softirq。

当系统中断过多时，do\_softirq才会被推迟到内核的ksoftirq内核线程中去。如何判断中断过多呢，linux的认为发生中断嵌套了，就是中断过多。do\_irq在调用do\_softirq时会以此为判断条件。

## 在驱动程序中申请中断

Linux中断子系统向驱动程序提供了一系列的API，其中的一个用于向系统申请中断：



request\_threaded\_irq()是Linux kernel 2.6.30 之后新加的irq handler API，如何确定可以用到 request\_threaded\_irq() ?

Linux kernel config 需要定义CONFIG\_GENERIC\_HARDIQS

kernel config 才有支援threaded irq ；Moving interrupts to threads 介绍request\_threaded\_irq() 的由来

http://lwn.net/Articles/302043/

从realtime tree 移植而来，为了减少kernel 因为要等待每一个硬件中断处理的时间 ，就另外交给kernel thread 处理中断后续工作。

 优点：

1 减少 kernel 延迟时间

2 避免处理中断时要分辨是在硬体中断或软体中断？

3 更容易为kernel 中断处理除错，可能可完全取代tasklet

原本的中断处理分上半部(硬体中断处理，必须关闭中断无法处理新的中断)跟下半部( 软体中断处理)，因此上半部的硬体中断处理必须尽可能简短，让系统反应速度更快。  request\_threaded\_irq 是在将上半部的硬件中断处理缩短为只确定硬体中断来 自我们要处理的装置，唤醒kernel thread 执行后续中断任务。

  缺点：

对于非irq 中断的kernel threads ，需要在原本task\_struct 新增struct irqaction 多占 4/8 bytes 记忆体空间，linux kernel 2.6.29 之后(2.6.30)加入request\_threaded\_irq 跟传统top/bottom havles 的差异是threaded\_irq 受Linux kernel system 的 process scheduling 控制，不会因为写错的bottom half 代码造成整个系统 延迟的问题。

也可以透过RT/non RT 跟nice 等工具调整各个thread 优先权，丢给使用率较低的  cpu 以及受惠于kernel 原本可以对threads 做的各种控制，包括但不限于sleep, lock, allocate 新的记忆体区块。

受惠最大的是shared irq line 的多个中断处理。除了可以加速共享中断造成的延迟threaded\_irq 也可以降低在同一段程式码处理多个装置中断的复杂度。 threaded irq 在使用性上也比tasklet(接着top half 直接执行，无法sleep) /workqueue(kernel context?) 等需要在top half 增加跟bottom half 连结与沟通  的麻烦。

**Ps:最简单直观的理解，handler是顶半部，thread\_fn是底半部（个人猜测，不确定正确）**

**现在看来上面那句话确实不准确。感觉这个函数把中断重新定义了。不能说什么顶半部和底半部。**

理解自宋宝华：申请一个线程化的IRQ，kernel会为中断的底版本创建一个名字为irq/%d-%s的线程，%d对应着中断号。其中顶半部（硬中断）**handler**在做完必要的处理工作之后，会返回IRQ\_WAKE\_THREAD，之后kernel会唤醒irq/%d-%s线程，而该kernel线程会调用**thread\_fn**函数，因此，该线程成为底半部。

该机制目前在kernel中使用已经十分广泛，可以认为是继softirq（含tasklet）和workqueue之后的又一大中断底半部方式。

**irq**  需要申请的irq编号，对于ARM体系，irq编号通常在平台级的代码中事先定义好，有时候也可以动态申请。

**handler**  中断服务回调函数，该回调运行在中断上下文中，并且cpu的本地中断处于关闭状态，所以该回调函数应该只是执行需要快速响应的操作，执行时间应该尽可能短小，耗时的工作最好留给下面的thread\_fn回调处理。

**thread\_fn**  如果该参数不为NULL，内核会为该irq创建一个内核线程，当中断发生时，如果handler回调返回值是IRQ\_WAKE\_THREAD，内核将会激活中断线程，在中断线程中，该回调函数将被调用，所以，该回调函数运行在进程上下文中，允许进行阻塞操作。

**flags**  控制中断行为的位标志，IRQF\_XXXX，例如：IRQF\_TRIGGER\_RISING，IRQF\_TRIGGER\_LOW，IRQF\_SHARED等，在include/linux/interrupt.h中定义。

**name**  申请本中断服务的设备名称，同时也作为中断线程的名称，该名称可以在/proc/interrupts文件中显示。

**dev**  当多个设备的中断线共享同一个irq时，它会作为handler的参数，用于区分不同的设备。

## flags:与中断相关的标志

IRQF\_TRIGGER\_RISING：上升沿触发

IRQF\_TRIGGER\_FALLING：下降沿触发

IRQF\_TRIGGER\_HIGH：高电平触发

IRQF\_TRIGGER\_LOW：低电平触发

IRQF\_SAMPLE\_RANDOM：为系统随机发生器提供支持

IRQF\_SHARED：中断可在设备间共享

IRQF\_DISABLED：是否快速中断

IRQF\_ONESHOT:选项说明该中断已经被线程化了（而且是特殊的one shot类型的）

（虽然kernel的注释上是这样说，但是request\_threaded\_irq时还是必须要设定IRQF\_ONESHOT，否者它就会被错误的强制线程化了。

其实我觉得这个ONESHOT的命名也是很不好，它不仅仅表示one shot，而且还是thread irq的标志。）

## **request\_threaded\_irq的工作流程**

函数先是根据irq编号取出对应的irq\_desc实例的指针，然后分配了一个irqaction结构，用参数handler，thread\_fn，irqflags，devname，dev\_id初始化irqaction结构的各字段，同时做了一些必要的条件判断：该irq是否禁止申请？handler和thread\_fn不允许同时为NULL，最后把大部分工作委托给\_\_setup\_irq函数：



图 request\_threaded\_irq（部分）

进入\_\_setup\_irq函数，如果参数flag中设置了IRQF\_SAMPLE\_RANDOM标志，它会调用rand\_initialize\_irq，以便对随机数的生成产生影响。如果申请的不是一个线程嵌套中断（关于线程嵌套中断，请参阅[Linux中断（interrupt）子系统之三：中断流控处理层](http://blog.csdn.net/droidphone/article/details/7489756)中的handle\_nested\_irq一节），而且提供了thread\_fn参数，它将创建一个内核线程;这个函数会判断handler是否可以线程化，如果可以，就会将它线程化：



图 \_\_setup\_irq（部分—与最新内核有区别）

**最新内核:**

**\_setup\_irq->setup\_irq\_thread->kthread\_create->**[**kthread\_create\_on\_node**](http://lxr.free-electrons.com/ident?i=kthread_create_on_node)

如果irq\_desc结构中断action链表不为空，说明这个irq已经被其它设备申请过，也就是说，这是一个共享中断，所以接下来会判断这个新申请的中断与已经申请的旧中断的以下几个标志是否一致：

一定要设置了IRQF\_SHARED标志

电气触发方式要完全一样（IRQF\_TRIGGER\_XXXX）

IRQF\_PERCPU要一致

IRQF\_ONESHOT要一致

检查这些条件都是因为多个设备试图共享一根中断线，试想一下，如果一个设备要求上升沿中断，一个设备要求电平中断，当中断到达时，内核将不知如何选择合适的流控操作。完成检查后，函数找出action链表中最后一个irqaction实例的指针。

如果这不是一个共享中断，或者是共享中断的第一次申请，函数将初始化irq\_desc结构中断线程等待结构：wait\_for\_threads，disable\_irq函数会使用该字段等待所有irq线程的结束。接下来设置中断控制器的电气触发类型，然后处理一些必要的IRQF\_XXXX标志位。如果没有设置IRQF\_NOAUTOEN标志，则调用irq\_startup()打开该irq，在irq\_startup()函数中irq\_desc中的enable\_irq/disable\_irq嵌套深度字段depth设置为0，代表该irq已经打开，如果在没有任何disable\_irq被调用的情况下，enable\_irq将会打印一个警告信息。

接着，设置cpu和irq的亲缘关系

然后，把新的irqaction实例链接到action链表的最后

最后，唤醒中断线程，注册相关的/proc文件节点

至此，irq的申请宣告完毕，当中断发生时，处理的路径将会沿着：irq\_desc.handle\_irq，irqaction.handler，irqaction.thread\_fn（irqaction.handler的返回值是IRQ\_WAKE\_THREAD）这个过程进行处理。下图表明了某个irq被申请后，各个数据结构之间的关系：



## 下半部的几种机制

## 软中断(softirqs)

软中断是一组在编译期间静态分配的下半部接口，一共有个32个。一个软中断不会抢占另一个软中断，唯一能够抢占软中断的是ISR。不同的软中断可以同时在多个CPU上执行，甚至同一个软中断也可以在所有CPU上同时执行，所以软中断必须设计成可重入函数，同时往往需要使用锁机制来保护共享数据

软中断保留给系统中对时间要求最严格以及最重要的下半部使用。在2.6版本中，只有两个子系统（网络和SCSI）直接使用了软中断。此外内核定时器和tasklet都是建立在软中断基础上的。

软中断运行时可以响应中断，但是不能休眠（因为此时仍然处于中断上下文）。当一个CPU正在执行某个软中断时，这个CPU会禁止软中断，但是别的CPU仍然可以执行新触发的软中断（相同的或不同的都可以），这也是软中断的优势——可以在多CPU上并行执行；但相应的tradeoff是，你要小心的保护好共享数据以避免竞争。在实践中，大部分软中断处理程序都采用per-CPU变量来避免显示的加锁，从而提高性能。

## Tasklet

tasklet是一种基于软中断的延时处理机制，是中断底半部的一种处理方式。基本上要使用就是申请中断，通过宏创建tasklet与处理函数的关联，在顶半部调用tasklet\_schedule使系统在适当的时候进行调（就是把tasklet\_struct结构体挂到tasklet\_vec链表或者挂接到tasklet\_hi\_vec链表上，并调度软中断TASKLET\_SOFTIRQ或者HI\_SOFTIRQ；Tasklet\_action在软中断TASKLET\_SOFTIRQ被调度到后会被执行，它从tasklet\_vec链表中把tasklet\_struct结构体都取下来，然后逐个执行。如果t->count的值等于0，说明这个tasklet在调度之后，被disable掉了，所以会将tasklet结构体重新放回到tasklet\_vec链表，并重新调度TASKLET\_SOFTIRQ软中断，在之后enable这个tasklet之后重新再执行它。）；

## work queue

前面提到的软中断和tasklet都运行于中断上下文，因此不可以睡眠；如果需要在下半部中睡眠，那就只能使用工作队列了。工作队列可以把下半部的操作交给一个内核线程来执行——也就是说运行在进程上下文中，因而是可以睡眠的。

Ps：参考request\_threaded\_irq

## 内核定时器

前面提到的下半部机制都是将操作推迟到除了现在之外的其他时间，而内核定时器可以确保将操作推迟到某个确定的时间来执行。如果必须确保在某一个确定的时间间隔以后再运行下半部操作，那么需要使用内核定时器。内核定时器其实也是在软中断基础上实现的。

## 参考资料

http://blog.csdn.net/21cnbao/article/details/8090398 request\_threaded\_irq

http://www.kuqin.com/shuoit/20140104/337421.html 讲述了什么是tasklet

http://blog.csdn.net/lizuobin2/article/details/51793911 这篇讲的比较好，

把中断对应机制分的很详细；但是只是做了一个详细的划分，机制原理讲述不清

http://blog.csdn.net/songjinshi/article/details/23262923 讲述调用调度程序的时机

http://blog.sina.com.cn/s/blog\_70a9dd840100uqfh.html 讲述了什么是isr，

也涉及了中断上下文以及中断上半部和下半部

http://blog.sina.com.cn/s/blog\_65373f1401018w15.html

http://blog.sina.com.cn/s/blog\_510ac74901015fgz.html

http://blog.csdn.net/DroidPhone/article/details/7445825 中断子系统的一系列文章

http://blog.csdn.net/lickylin/article/details/12657373

http://blog.chinaunix.net/xmlrpc.php?r=blog/article&uid=21977330&id=3755609

# Input子系统与多点触摸技术

## 简介

Linux 的输入子系统不仅支持鼠标、键盘等常规输入设备,而且还支持蜂鸣器、触摸屏等设备。输入子系统又叫 input 子系统。其构建非常灵活,只需要调用一些简单的函数,就可以将一个输入设备的功能呈现给应用程序。

输入设备(如按键,键盘，触摸屏，鼠标等)是典型的字符设备，其一般的工作机制是低层在按键，触摸等动作发生时产生一个中断(或驱动通过timer定时查询)，然后cpu通过SPI，I2C或者外部存储器总线读取键值，坐标等数据，放一个缓冲区，字符设备驱动管理该缓冲区，而驱动的read()接口让用户可以读取键值，坐标等数据。

在Linux中，输入子系统是由输入子系统设备驱动层、输入子系统核心层(Input Core)和输入子系统事件处理层(Event Handler)组成。

其中**设备驱动层**提供对硬件各寄存器的读写访问和将底层硬件对用户输入访问的响应转换为标准的输入事件，再通过核心层提交给事件处理层；

而**核心层**对下提供了设备驱动层的编程接口，对上又提供了事件处理层的编程接口；

而**事件处理层**就为我们用户空间的应用程序提供了统一访问设备的接口和驱动层提交来的事件处理。

所以这使得我们输入设备的驱动部分不在用关心对设备文件的操作，而是要关心对各硬件寄存器的操作和提交的输入事件。

下面是输入子系统结构图：



## ****设备驱动层****

**输入子系统设备驱动层实现原理**

在Linux中，Input设备用input\_dev结构体描述，定义在input.h中。设备的驱动只需按照如下步骤就可实现了。

1).在驱动模块加载函数中设置Input设备支持input子系统的哪些事件；

2).将Input设备注册到input子系统中；

3).在Input设备发生输入操作时(如：键盘被按下/抬起、触摸屏被触摸/抬起/移动、鼠标被移动/单击/抬起时等)，提交所发生的事件及对应的键值/坐标等状态。

linux中输入设备驱动的分层：



## 换个角度看input子系统

 整体来看，Input子系统有一个主线，称为三方关系，input\_dev对应于实际的device端，input\_handler从名字也可以猜出来是对device的处理。“处理”这个词语不单单指的是对device数据的处理，比如report等；它其实可以包括系统在该device事件发生时想做的任何动作。至于input\_handle，它是连接input\_dev与input\_handler。

struct input\_handle {

    ...

struct input\_dev \*dev;//对应dev结构体

struct input\_handler \*handler;//对应handler结构体

    struct list\_head    d\_node;//链入input\_dev的h\_list代表的链表

    struct list\_head    h\_node;//链入input\_handler的h\_list代表的链表

};

至此，三方关系形成完毕。我们实现了最终的目的，通过input\_dev，可以遍历所有与它有关的input\_handler；通过input\_handler，也可以遍历所有与它有关的input\_dev。

图解如下：图中单向箭头表示指针，双向箭头表示list\_head。可以看出，从任何一个双向箭头出发，通过handle的过度，完全实现了我们的最终目标。掌握了这点，再看input\_report那些流程的时候就非常容易了，dev想要report数据的时候无非是调用了handler的event函数指针指向的函数，我们可以在这个函数里定义任何想让系统去做的任务，比如cpu调频等，而不仅限于数据上报。熟悉面向对象编程的人可能想到了，其实这个设计运用了面向对象的observer设计模式。



## 软件设计流程

[](http://blog.chinaunix.net/link.php?url=http://blog.chinaunix.net/link.php?url%3Dhttp://blog.chinaunix.net/attachment/201108/1/23770712_1312213167mtdZ.gif)

图 3 input子系统软件设计流程

## 与软件设计有关的API函数

**分配一个输入设备**

Struct input\_dev \*input\_allocate\_device\*(void);

**注册一个输入设备**

Int input\_register\_device (struct input\_dev \*dev);

**驱动实现-事件支持**

Set\_bit告诉in/out子系统它支持哪些事件

Set\_bit (EV\_KEY, button\_dev.evbit)

Struct input\_dev中有两个成员，一个是evbit;一个是keybit.分别用来表示设备所支持的事件类型和按键类型。

**事件类型**

Linux中输入设备的事件类型有(这里只列出了常用的一些，更多请看linux/input.h中)：

EV\_SYN 0x00 同步事件

EV\_KEY 0x01 按键事件

EV\_REL 0x02 相对坐标

EV\_ABS 0x03 绝对坐标

EV\_MSC 0x04 其它

EV\_LED 0x11 LED

EV\_SND 0x12 声音

EV\_REP 0x14 Repeat

EV\_FF 0x15 力反馈

EV\_PWR     0x16   电源管理事件

驱动实现-报告事件

Void input\_event(struct input\_dev \* dev, unsigned int type, unsigned int code, int value);//报告指定type ,code的输入事件

Void input\_report\_key(struct input\_dev \*dev, unsigned int code, int value);//报告键值

Void input\_report\_rel(struct input\_dev \*dev, unsigned int code, int value);//报告相对坐标

Void input\_report\_abs(struct input\_dev \*dev, unsigned int code, int value);//报告绝对坐标

Void input\_sync(struct input\_dev \*dev);//报告同步事件

**在触摸屏驱动设计中，一次坐标及按下状态的整个报告过程如下：**

**Input\_report\_abs(input\_dev,ABS\_X,x);//X坐标**

**Input\_report\_abs(input\_dev,ABS\_Y,y);//Y坐标**

**Input\_report\_abs(input\_dev,ABS\_PRESSURE,pres);//压力**

**input\_sync(struct input\_dev \*dev);//同步**

1.6.5释放与注销设备

Void input\_free\_device(struct input\_dev \*dev);

Void input\_unregister\_device(struct input\_dev \*);

## 多点触摸技术A/B(Slot)协议

### A/B协议究竟是如何划分

B协议又称为slot协议，slot直译为位置、槽，有两层含义，一层是位置，另一层是容器。在Input子系统中，它扮演的就是这两个角色。它产生于这样一个背景：

如果从Device获取的当前数据与上一个数据相同，我们有必要再上报当前数据吗？如果我们不管两次数据是否一致都上报，那就是A协议；如果我们选择不上报，那么既然需要比较，总需要把上一次数据存起来吧，slot就是做这个事情的，显然这就是Slot(B)协议。

### A协议实现方式

A协议不会使用slot，多指处理中，它的报点序列如下（每一个序列都以input\_report\_\*\*\*函数实现）：

手指按下的动作：

**ABS\_MT\_POSITION\_X x[0]**

**ABS\_MT\_POSITION\_Y y[0]**

**SYN\_MT\_REPORT**

**ABS\_MT\_POSITION\_X x[1]**

**ABS\_MT\_POSITION\_Y y[1]**

**SYN\_MT\_REPORT**

**…**

**SYN\_REPORT**

上面的序列中需要说明的是系统以SYN\_MT\_REPORT为一个点的信息的结尾，以SYN\_REPORT为一次事件的结尾。也就是说多指触摸的时候，android的中间件部分每收到一次SYN\_MT\_REPORT就形成一个点信息，收到一个点之后并不会立即处理，而是一个事件完成之后才会处理，SYN\_REPORT就是这个事件的标志。A协议比较简单，我们也可以发现在上面的序列中根本就没有轨迹跟踪的信息，有的只是点坐标等信息

#### 系统如果去判断当前的多个点各属于哪一条线

我们假设前一次事件共有5个点，本次触摸也有5个点，系统会分别计算前一次5个点与本次5个点的距离，distance[prev\_i, curr\_j] (i=0,1,...,4; j=0,1,...4)，这样会产生总共5\*5=25个数字。然后对这25个数字进行排序，android用的是堆排序。（我们在系统上如果用多指，一般最多也是双值，也就是4个数据，这里采用了堆排序，不知是出于什么情况考虑，感觉换个方法可能更实用些。）下面的任务就是判断哪些当前点与前一次的点最近，那么赋予它们相同的id，应用收到这个信息后，就可以知道当前点属于哪条线了。

#### 手抬起来的时候又用什么样的序列来通知系统

SYN\_MT\_REPORT

SYN\_REPORT

只有SYNC，没有其它任何信息，系统就会认为此次事件为UP。

### B协议实现方式

B协议使用了slot，还有一个新面孔TRACKING\_ID.

手指按下的动作：

ABS\_MT\_SLOT 0

ABS\_MT\_TRACKING\_ID \*\*

ABS\_MT\_POSITION\_X x[0]

ABS\_MT\_POSITION\_Y y[0]

ABS\_MT\_SLOT 1

ABS\_MT\_TRACKING\_ID \*\*

ABS\_MT\_POSITION\_X x[1]

ABS\_MT\_POSITION\_Y y[1]

SYN\_REPORT

没有SYN\_MT\_REPORT，那么它用什么来跟踪当前点属于哪一条线呢，用的就是ABS\_MT\_TRACKING\_ID，当前序列中某点的ID值，如果与前一次序列中某点的ID值相等，那么他们就属于同一条线。既然如此，那么android系统中还需要做排序等运算吗？当然不需要。

#### 手指全部抬起的时候序列又是怎样的

ABS\_MT\_SLOT 0

ABS\_MT\_TRACKING\_ID -1

SYN\_REPORT

ABS\_MT\_SLOT 1

ABS\_MT\_TRACKING\_ID -1

SYN\_REPORT

这里上报的ABS\_MT\_TRACKING\_ID为-1，也只有这里该值才可以小于零，收到该值，系统就会清除对应的ID。看似简单的两个协议内容到这里就分析完毕了。

#### 附上android 4.0上报方式（linux必须2.6.38以上）

1. #include <linux/input/mt.h>

1. //down
2. input\_mt\_slot(ts->input\_dev, id);
3. //input\_report\_abs(ts->input\_dev, ABS\_MT\_TRACKING\_ID, id);
4. input\_mt\_report\_slot\_state(data->input\_dev, MT\_TOOL\_FINGER, true);
5. input\_report\_abs(ts->input\_dev, ABS\_MT\_TOUCH\_MAJOR, w);
6. input\_report\_abs(ts->input\_dev, ABS\_MT\_POSITION\_X, x);
7. input\_report\_abs(ts->input\_dev, ABS\_MT\_POSITION\_Y, y);

ps：个人感觉注释的那一行是在初次手指摁下才会执行，移动的时候就不执行这句话了  
//up

1. input\_mt\_slot(ts->input\_dev, id);
2. //input\_report\_abs(ts->input\_dev, ABS\_MT\_TRACKING\_ID, -1);
3. input\_mt\_report\_slot\_state(ts->input\_dev, MT\_TOOL\_FINGER, false);

ps：同理，注释的这句应该是在slot为0的时候不执行

1. //init
2. //\_\_set\_bit(INPUT\_PROP\_DIRECT, ts->input\_dev->propbit);
3. input\_mt\_init\_slots(ts->input\_dev, 255);

**上面两条ps是在本人看了内核文档介绍多触点以后的感觉，不一定对**

### 总结

看了上面的分析，明显可以看出B协议要优于A协议，但事实上并不如此简单。B协议需要硬件上的支持，ID值并不是随便赋值的，而是硬件上跟踪了点的轨迹；如果硬件上满足不了这个条件，那么采用B协议只能闹成笑话。另外，B协议的复杂性如果掌握不好往往会带来一些莫名其妙的问题，比如如果因为某些因素（同步等），在UP的时候少清除了一个slot的信息，那么下次单击的时候你也会惊奇地发现竟然有两个点（采用了B协议，slot已经保存了点信息，除非明确清除）。

## 参考资料

http://blog.csdn.net/droidphone/article/details/8434768 多点触控的input TP

http://blog.csdn.net/yaozhenguo2006/article/details/6775751 input\_event 函数

http://blog.csdn.net/loongembedded/article/details/51166888

http://blog.csdn.net/loongembedded/article/details/51167111 input事件类型

http://blog.csdn.net/tianruxishui/article/details/7173045 写得不错，

https://www.kernel.org/doc/Documentation/input/multi-touch-protocol.txt 源码的文档

<http://www.arm9home.net/read.php?tid=24754> 对源码文档的翻译

http://blog.chinaunix.net/uid-20776117-id-3212095.html 内部函数剖析

<http://blog.chinaunix.net/xmlrpc.php?r=blog/article&uid=29151914&id=3921536>

<http://blog.chinaunix.net/xmlrpc.php?r=blog/article&uid=29151914&id=3887032>

ps：其实源码的说明文档介绍的很清楚，但是不细节，所以需要在了解一定的基础上去看看说明文档

# Android调试方法

## getevent，sendevent，input三命令

### Getevent

**Usage**: getevent [-t] [-n] [-sswitchmask] [-**S**] [-v [mask]] [-d] [-p] [-i] [-l] [-q] [-c count] [-r] [device]

-t: show time stamps

-n: don't print newlines

-s: print **switch** states **for** given bits

-**S**: print all **switch** states

-v: verbosity mask (errs=1， dev=2， name=4， info=8， vers=16， pos. events=32，props=64)

-d: show **HID** descriptor， **if** available

-p: show possible events (errs， dev， name， pos. events)

-i: show all device info and possible events

-l: label event types and names **in** plain text

-q: quiet (clear verbosity mask)

-c: print given number of events then exit

-r: print rate events are received

键入getevent后，我们能够看到设备中的一些列输入硬件驱动信息，同样下面会出现很多输入指令信号，通常情况下，这些信号量都在刷屏

#### 格式说明

root@android:/ # getevent

**/dev/input/event5: 0005 0002 00000001**

**device的名字： 事件类型 键码类别 具体的数值**

**/dev/input/event5: 0000 0000 00000000**

**表示一次输入结束（全为0表示一次输入的结束）**

其实这些Lable已经在其input.h头文件中定义好，其中type的定义如下：

/\*

\* **Event types**

\*/

**#define EV\_SYN 0x00**

**#define EV\_KEY 0x01**

**#define EV\_REL 0x02**

**#define EV\_ABS 0x03**

**#define EV\_MSC 0x04**

**#define EV\_SW 0x05**

**#define EV\_LED 0x11**

**#define EV\_SND 0x12**

**#define EV\_REP 0x14**

**#define EV\_FF 0x15**

**#define EV\_PWR 0x16**

**#define EV\_FF\_STATUS 0x17**

**#define EV\_MAX 0x1f**

**#define EV\_CNT (EV\_MAX+1)**

一般来说，常用的是EV\_KEY、EV\_REL、EV\_ABS、EV\_SYN，分别对应键盘按键、相对坐标、绝对坐标、同步事件。EV\_SYN则表示一组完整事件已经完成，需要处理，EV\_SYN的code定义事件分发的类型。

在触摸事件上的几个常见的Label说明如下表所示：

| **标签名** | **说明** |
| --- | --- |
| ABS\_X | 对应触摸屏的X坐标 |
| ABS\_Y | 对应触摸屏的Y坐标 |
| ABS\_PRESSURE | 压力值，一般触摸屏也只是区分是否有按下去，按下去的话值会大于多少，没有按的话值小于多少。 |
| ABS\_TOOL\_WIDTH | 触摸工具的宽度 |
| ABS\_MT\_POSITION\_X | 接触面的形心的X坐标值 |
| ABS\_MT\_POSITION\_Y | 接触面的形心的Y坐标值 |
| ABS\_MT\_TOUCH\_MAJOR | 触摸手指大小 |
| ABS\_MT\_WIDTH\_MAJOR | 触摸面积大小 |

了解了这些Label的含义我们再看看信号量就简单多了，如我们列举几个常见的事件与信号，如下表所示：

| **操作** | **输出信号** |
| --- | --- |
| 按下电源键 | /dev/input/event0: EV\_KEY KEY\_POWER DOWN /dev/input/event0: EV\_SYN SYN\_REPORT 000000 /dev/input/event0: EV\_KEY KEY\_POWER UP /dev/input/event0: EV\_SYN SYN\_REPORT 000000 |
| 音量键下 | /dev/input/event8: EV\_KEY KEY\_VOLUMEDOWN DOWN /dev/input/event8: EV\_SYN SYN\_REPORT 00000000 /dev/input/event8: EV\_KEY KEY\_VOLUMEDOWN UP /dev/input/event8: EV\_SYN SYN\_REPORT 00000000 |
| 音量键上 | /dev/input/event8: EV\_KEY KEY\_VOLUMEUP DOWN /dev/input/event8: EV\_SYN SYN\_REPORT 00000000 /dev/input/event8: EV\_KEY KEY\_VOLUMEUP UP /dev/input/event8: EV\_SYN SYN\_REPORT 00000000 |
| 按下物理按键“1” | /dev/input/event0: EV\_KEY KEY\_1 DOWN /dev/input/event0: EV\_KEY KEY\_1 UP |
| 按下物理按键“q” | /dev/input/event0: EV\_KEY KEY\_Q DOWN /dev/input/event0: EV\_KEY KEY\_Q UP |
| 按下软键盘上的“q”字母 | /dev/input/event0: EV\_ABS ABS\_X 0000001b /dev/input/event0: EV\_ABS ABS\_Y 000001d5 /dev/input/event0: EV\_KEY BTN\_TOUCH DOWN /dev/input/event0: EV\_SYN SYN\_REPORT 00000000 /dev/input/event0: EV\_KEY BTN\_TOUCH UP /dev/input/event0: EV\_SYN SYN\_REPORT 00000000 |
| 按下软件键盘上的的“1”按键 | /dev/input/event0: EV\_ABS ABS\_X 00000019 /dev/input/event0: EV\_ABS ABS\_Y 000001d7 /dev/input/event0: EV\_KEY BTN\_TOUCH DOWN /dev/input/event0: EV\_SYN SYN\_REPORT 00000000 /dev/input/event0: EV\_KEY BTN\_TOUCH UP /dev/input/event0: EV\_SYN SYN\_REPORT 00000000 |

从上表中，我们发现要是按下的是物理按键，其输入出来的信息我们很容易读懂，如果按下的是软键盘中的按键，给出的信号信息就是一些位置坐标信息。我们无法直接读懂，当然，我们可以根据这些位置坐标信息，再拿到Android设备的屏幕尺寸，计算比例也能够直接获得按键的具体内容。

当然，输出条件不会是想我们表格中的这么规范，中间会夹杂则各式各样的信息，有些可能是你不关心的。这里我们把一些无关的信号量过滤去掉了。实际查看上对应信息条件比较多，大家可以将Android设备连接如自己的电脑进行调试，这里我们就不做一一的解释了。

Ps:以上结果仅供参考。实际消息会有一些偏差

The getevent tool runs on the device and provides information about input devices and a live dump of kernel input events.

This tool is useful for ensuring device drivers are reporting the expected set of capabilities for each input device and are generating the desired stream of input events.

Showing device capabilities

Use the -p option to see all of the keys and axes a device reports. The following example lists the Linux key codes and other events a particular keyboard says it supports.

$ adb shell su -- getevent -p  
  
  name:     "Motorola Bluetooth Wireless Keyboard"  
  events:  
    KEY (0001): 0001  0002  0003  0004  0005  0006  0007  0008  
                0009  000a  000b  000c  000d  000e  000f  0010  
                0011  0012  0013  0014  0015  0016  0017  0018  
                0019  001a  001b  001c  001d  001e  001f  0020  
                0021  0022  0023  0024  0025  0026  0027  0028  
                0029  002a  002b  002c  002d  002e  002f  0030  
                0031  0032  0033  0034  0035  0036  0037  0038  
                0039  003a  003b  003c  003d  003e  003f  0040  
                0041  0042  0043  0044  0045  0046  0047  0048  
                0049  004a  004b  004c  004d  004e  004f  0050  
                0051  0052  0053  0055  0056  0057  0058  0059  
                005a  005b  005c  005d  005e  005f  0060  0061  
                0062  0063  0064  0066  0067  0068  0069  006a  
                006b  006c  006d  006e  006f  0071  0072  0073  
                0074  0075  0077  0079  007a  007b  007c  007d  
                007e  007f  0080  0081  0082  0083  0084  0085  
                0086  0087  0088  0089  008a  008c  008e  0090  
                0096  0098  009b  009c  009e  009f  00a1  00a3  
                00a4  00a5  00a6  00ab  00ac  00ad  00b0  00b1  
                00b2  00b3  00b4  00b7  00b8  00b9  00ba  00bb  
                00bc  00bd  00be  00bf  00c0  00c1  00c2  00d9  
                00f0  0110  0111  0112  01ba  
    REL (0002): 0000  0001  0008  
    ABS (0003): 0028  : value 223, min 0, max 255, fuzz 0, flat 0, resolution 0  
                0029  : value 0, min 0, max 255, fuzz 0, flat 0, resolution 0  
                002a  : value 0, min 0, max 255, fuzz 0, flat 0, resolution 0  
                002b  : value 0, min 0, max 255, fuzz 0, flat 0, resolution 0  
    MSC (0004): 0004  
    LED (0011): 0000  0001  0002  0003  0004  
  input props:  
    <none>

Use the -i option to get more information, including HID mapping tables and debugging information.

Use the -l option to display textual labels for all event codes. Example:

$ adb shell su -- getevent -lp /dev/input/event1  
  
  name:     "Melfas MMSxxx Touchscreen"  
  events:  
    ABS (0003): ABS\_MT\_SLOT           : value 0, min 0, max 9, fuzz 0, flat 0, resolution 0  
                ABS\_MT\_TOUCH\_MAJOR    : value 0, min 0, max 30, fuzz 0, flat 0, resolution 0  
                ABS\_MT\_POSITION\_X     : value 0, min 0, max 720, fuzz 0, flat 0, resolution 0  
                ABS\_MT\_POSITION\_Y     : value 0, min 0, max 1280, fuzz 0, flat 0, resolution 0  
                ABS\_MT\_TRACKING\_ID    : value 0, min 0, max 65535, fuzz 0, flat 0, resolution 0  
                ABS\_MT\_PRESSURE       : value 0, min 0, max 255, fuzz 0, flat 0, resolution 0  
  input props:  
    INPUT\_PROP\_DIRECT

Showing live events

The following example shows a two-finger multi-touch gesture for a touchscreen using the Linux multi-touch input protocol "B". The -l option displays textual labels and the -t option displays timestamps.

$ adb shell su -- getevent -lt /dev/input/event1  
  
[   78826.389007] EV\_ABS       ABS\_MT\_TRACKING\_ID   0000001f  
[   78826.389038] EV\_ABS       ABS\_MT\_PRESSURE      000000ab  
[   78826.389038] EV\_ABS       ABS\_MT\_POSITION\_X    000000ab  
[   78826.389068] EV\_ABS       ABS\_MT\_POSITION\_Y    0000025b  
[   78826.389068] EV\_ABS       ABS\_MT\_SLOT          00000001  
[   78826.389068] EV\_ABS       ABS\_MT\_TRACKING\_ID   00000020  
[   78826.389068] EV\_ABS       ABS\_MT\_PRESSURE      000000b9  
[   78826.389099] EV\_ABS       ABS\_MT\_POSITION\_X    0000019e  
[   78826.389099] EV\_ABS       ABS\_MT\_POSITION\_Y    00000361  
[   78826.389099] EV\_SYN       SYN\_REPORT           00000000  
[   78826.468688] EV\_ABS       ABS\_MT\_SLOT          00000000  
[   78826.468688] EV\_ABS       ABS\_MT\_TRACKING\_ID   ffffffff  
[   78826.468719] EV\_ABS       ABS\_MT\_SLOT          00000001  
[   78826.468719] EV\_ABS       ABS\_MT\_TRACKING\_ID   ffffffff  
[   78826.468719] EV\_SYN       SYN\_REPORT           00000000

**Note:** getevent timestamps use the format $SECONDS.$MICROSECONDS in the CLOCK\_MONOTONIC timebase. For details, refer to getevent.c.

### Sendevent

### Input

**Usage: input [<source>] <command> [<arg>...]**

**The sources are:**

**mouse**

**keyboard**

**joystick**

**touchnavigation**

**touchpad**

**trackball**

**stylus**

**dpad**

**touchscreen**

**gamepad**

**The commands and default sources are:**

**text <string> (Default: touchscreen)**

**keyevent [--longpress] <key code number or name> ... (Default: keyboard)**

**tap <x> <y> (Default: touchscreen)**

**swipe <x1> <y1> <x2> <y2> [duration(ms)] (Default: touchscreen)**

**press (Default: trackball)**

**roll <dx> <dy> (Default: trackball)**

#### 基本用法

input keyevent [key code or name]//用来对应按键的触发

Keycode需要参考:$ROOT\_DIR/frameworks/base/core/java/android/view/KEYEVENT.java

Input tap x y //对应触摸点

Input swipe x1 y1 x2 y2 //对应滑动触摸

Input text “text” //输入text内容

ps 三个有用的调试函数

﻿﻿

#define hardirq\_count() (preempt\_count() & HARDIRQ\_MASK)  
#define softirq\_count() (preempt\_count() & SOFTIRQ\_MASK)  
#define irq\_count() (preempt\_count() & (HARDIRQ\_MASK | SOFTIRQ\_MASK \  
     | NMI\_MASK))

/\*  
 \* Are we doing bottom half or hardware interrupt processing?  
 \* Are we in a softirq context? Interrupt context?  
 \*/  
#define in\_irq()   (hardirq\_count())      //判断当前是否在硬件中断上下文  
#define in\_softirq()  (softirq\_count())  //判断当前是否在软件中断上下文  
#define in\_interrupt()  (irq\_count())    //判断当前是否在硬件、软件、底半部中断上下文

## 参考资料

<http://blog.csdn.net/shift_wwx/article/details/49760735> **input**

<http://blog.csdn.net/hudan2714/article/details/8003585> **input**

http://blog.csdn.net/shift\_wwx/article/details/11481797 **input**

<http://myeyeofjava.iteye.com/blog/1999615> **getevent**

<http://www.codeceo.com/article/android-keyboard-monitor.html> **getevent**

# ARM概念梳理：Architecture, Core, CPU，SOC

### 概念梳理

1）ARM architecture

ARM architecture，是指ARM公司开发的、基于精简指令集架构（RISC, Reduced Instruction Set Computing architecture）的指令集架构（Instruction set architecture）。我们常说的ARMv7、ARMv8、ARMv8-A，就是指ARM architecture。类似的基于RISC的architecture也有很多，例如MIPS、AVR、Blackfin等等，都是这个概念。

2）ARM core

ARM core是基于ARM architecture开发出来的IP core，它是介于architecture和最终的CPU(MCU)之间的中间产品，这也是ARM商业模式的独特之处。

有两种类型的ARM core：一种是ARM公司自己发布的，如我们耳熟能详的ARM7、ARM9、ARM Cortex M3、ARM Cortex A57等等；另一种是ARM授权其它公司开发的Core，如苹果的A6/A6X等等。下面链接是维基百科上的ARM core的列表，共大家参考：

<http://en.wikipedia.org/wiki/List_of_ARM_microarchitectures>

3）ARM CPU（MCU）

其它的芯片厂商，如Phillips、ST、TI等，会基于ARM公司发布的Core，开发自己的ARM处理器，这称作ARM CPU（也可称为MCU）。这些是我们工作过程中接触最多的，如LPCxxxx、STM32xxx、OMAPxxxx、S3Cxxxx等等。

4）ARM Soc

对于一些比较专业的应用场景，如视频、音频等，为了追求更小的size、更低的功耗，厂商会在芯片上，集成除处理器之外的东西，如视频编解码器、DSP等。这些集成了其它功能的芯片，称作片上系统（SOC），如TI的DM37x Video SOC。

注1：其实ARM的技术和商业模式，正体现了软件工程中抽象和封装的思想。

### ARM 64bit

我们以一款64bit ARM CPU为例，反向阐述一下ARM处理的诞生过程，同时罗列一些学习、研究方向。

1）我们熟悉一个CPU（假设它的型号是WW9000）的第一手资料，是芯片厂家发布的Datasheet，例如WW9000\_SPEC.pdf。

2）WW9000是基于ARM Cortex-A57 Core封装而来的，该ARM core的资料可以从下面链接下载

<http://infocenter.arm.com/help/topic/com.arm.doc.ddi0488g/DDI0488G_cortex_a57_mpcore_trm.pdf>

3）ARM Cortex-A57 Core又是基于ARMv8-A architecture，该结构的资料可以通过如下方式获取：

Go to [ARM Infocenter](http://infocenter.arm.com/) and navigate through ARM architecture / Reference Manuals

注2：[ARM Infocenter](http://infocenter.arm.com/)中资料是非常全面的，没事时可以多逛逛。

## 参考资料

<http://www.wowotech.net/armv8a_arch/arm_concept.html>

## pmic与pmu的区别

pmu是cpu这边的，pmic是外设；pmic是供电给主芯片的，pmu负责把这些电分配给cpu的各个单元，也负责问pmic要合适的电；pmu是cpu内部负责电源管理的单元

ps:个人猜测pmic对应很多单元

# Linux中SD/MMC设备驱动流程

SD（Secure Digital）与 MMC（Multimedia Card）

SD 是一种 flash memory card 的标准，也就是一般常见的 SD 记忆卡，而 MMC 则是较早的一种记忆卡标准，目前已经被 SD 标准所取代。在维基百科上有相当详细的 SD/MMC 规格说明：

## SDIO（Secure Digital I/O）

SDIO 是目前我们比较关心的技术，SDIO 故名思义，就是 SD 的 I/O 接口（interface）的意思，不过这样解释可能还有点抽像。更具体的说明，SD 本来是记忆卡的标准，但是现在也可以把 SD 拿来插上一些外围接口使用，这样的技术便是 SDIO。

所以 SDIO 本身是一种相当单纯的技术，透过 SD 的 I/O 接脚来连接外部外围，并且透过 SD 上的 I/O 数据接位与这些外围传输数据，而且 SD 协会会员也推出很完整的 SDIO stack 驱动程序，使得 SDIO 外围（我们称为 SDIO 卡）的开发与应用变得相当热门。 现在已经有非常多的手机或是手持装置都支持 SDIO 的功能（SD 标准原本就是针对 mobile device 而制定），而且许多 SDIO 外围也都被开发出来，让手机外接外围更加容易，并且开发上更有弹性（不需要内建外围）。目前常见的 SDIO 外围（SDIO 卡）有：

 Wi-Fi card（无线网络卡）

 CMOS sensor card（照相模块）

   GPS card

 GSM/GPRS modem card

 Bluetooth card

 Radio/TV card（很好玩）

SDIO 的应用将是未来嵌入式系统最重要的接口技术之一，并且也会取代目前 GPIO 式的 SPI 接口。

## **SD/SDIO/MMC/SPI之间的关系**

SD/SDIO/MMC是三种不同的卡，这3种卡的管脚很类似，卡的样子也类似。最开始是先由MMC 卡，然后在MMC的基础上做了修改有了SD卡，SD卡的基础上有了SDIO卡。所以SD/SDIO/MMC的协 议大同小异，只有少量差异。 SPI在SD的大军里，只是一种传输模式。若是慢速的情况下，可选择SPI传输模式，这样SD接口 就变成SPI协议了。Host也要根据SPI的协议对卡进行操作。 具体的区别需参考各协议。

## **同一个控制器，支持SD/MMC/SDIO的所以卡，如何区分出现在卡槽里的是个什么卡**

这个需要软件来区分。软件不停的循环访问卡，对卡按照一定的顺序发出对应格式的命令，那么不同的卡会做出不同的反应。几个CMD发完，根据不用的反应就可以分出是什么卡了。比如已经判断出是SD卡了，但是不知道是什么类型的SD卡。那么我们就发一个CMD8，如果 没有response，那么这个卡就是SD1.X的卡；如果有response，那么就是SD2.0以上的卡。

## SD/SDIO 的传输模式

SD 传输模式有以下 3 种：

 SPI mode（required）

 1-bit mode

 4-bit mode

SDIO 同样也支持以上 3 种传输模式。依据 SD 标准，所有的 SD（记忆卡）与 SDIO（外围）都必须支持 SPI mode，因此 SPI mode 是「required」。此外，早期的 MMC 卡（使用 SPI 传输）也能接到 SD 插糟（SD slot），并且使用 SPI mode 或 1-bit mode 来读取。 SD 的 MMC Mode SD 也能读取 MMC 内存，虽然 MMC 标准上提到，MMC 内存不见得要支持 SPI mode（但是一定要支持 1-bit mode），但是市面上能看到的 MMC 卡其实都有支持 SPI mode。因此，我们可以把 SD 设定成 SPI mode 的传输方式来读取 MMC 记忆卡。 SD 的 MMC Mode 就是用来读取 MMC 卡的一种传输模式。不过，SD 的 MMC Mode 虽然也是使用 SPI mode，但其物理特性仍是有差异的：  MMC 的 SPI mode 最大传输速率为 20 Mbit/s；  SD 的 SPI mode 最大传输速率为 25 Mbit/s。 为避免混淆，有时也用 SPI/MMC mode 与 SPI/SD mode 的写法来做清楚区别



## 参考资料

http://blog.csdn.net/evilcode/article/details/7408921

http://blog.csdn.net/evilcode/article/details/7418323

<http://wenku.baidu.com/link?url=lPg26KHW_IUD6de7wxooapFMfzJNXAhuyRabcnj0WpmlT23LpGG5KRwEXIrUFqe8UfIqL1_i3CMUIZYxrNNsOmz1Dsvv_7-foXWH0ZwZIAa>

# 内核通知链

大多数内核子系统都是相互独立的，因此某个子系统可能对其它子系统产生的事件感兴趣。为了满足这个需求，也即是让某个子系统在发生某个事件时通知其它的子系统，Linux内核提供了通知链的机制。通知链表**只能够在内核的子系统之间使用**，而不能够在内核与用户空间之间进行事件的通知。通知链表是一个**单链表的函数链表**，链表上的每一个节点都注册了一个函数。当某个事情发生时，链表上所有节点对应的函数就会被执行。所以对于通知链表来说有一个通知方与一个接收方。在通知这个事件时所运行的函数由被通知方决定，实际上也即是被通知方注册了某个函数，在发生某个事件时这些函数就得到执行。通知链技术可以概括为：事件的接收者将事件发生时应该执行的操作通过函数指针方式保存在链表中，然后当事件发生时通知者依次执行链表中每一个元素的回调函数。

## ****notifier chain 定义和接口****

1. **struct** notifier\_block {
2. **int** (\*notifier\_call)(**struct** notifier\_block \*, unsigned **long**, **void** \*);  // 回调函数接口
3. **struct** notifier\_block \*next;  // 指向下一个通知结构
4. **int** priority;                 // 当前通知链的优先级 ，一般默认为0。
5. };

可以看到通知链的基础数据结构比较简单，有回调函数接口、下一节点指针、优先级三个成员，其中回调函数的三个参数分别为：指向当前结构的指针、事件类型、参数。

内核提供了4种常用的通知链：

## ****1、Atomic notifier chains****

原子通知链：通知链元素的回调函数（当事件发生时要执行的函数）只能在中断上下文中运行，不允许阻塞

1. **struct** atomic\_notifier\_head {
2. spinlock\_t lock;
3. **struct** notifier\_block \*head;
4. };

由宏 ATOMIC\_NOTIFIER\_HEAD(name) 初始化链表头，其注册、注销及通知接口分别为：

1. **int** atomic\_notifier\_chain\_register(**struct** atomic\_notifier\_head \*nh, **struct** notifier\_block \*n);
2. **int** atomic\_notifier\_chain\_unregister(**struct** atomic\_notifier\_head \*nh, **struct** notifier\_block \*n);
3. **int** atomic\_notifier\_call\_chain(**struct** atomic\_notifier\_head \*nh, unsigned **long** val, **void** \*v);

## ****2、Blocking notifier chains****

可阻塞通知链：通知链元素的回调函数在进程上下文中运行，允许阻塞

1. **struct** blocking\_notifier\_head {
2. **struct** rw\_semaphore rwsem;
3. **struct** notifier\_block \*head;
4. };

由宏 BLOCKING\_NOTIFIER\_HEAD(name) 初始化链表头，其注册、注销及通知接口分别为：

1. **int** blocking\_notifier\_chain\_register(**struct** blocking\_notifier\_head \*nh, **struct** notifier\_block \*nb);
2. **int** blocking\_notifier\_chain\_unregister(**struct** blocking\_notifier\_head \*nh, **struct** notifier\_block \*nb);
3. **int** blocking\_notifier\_call\_chain(**struct** blocking\_notifier\_head \*nh, unsigned **long** val, **void** \*v);

## 3、Raw notifier chains

原始通知链：对通知链元素的回调函数没有任何限制，所有锁和保护机制都由调用者维护

1. **struct** raw\_notifier\_head {
2. **struct** notifier\_block \*head;
3. };

由宏 RAW\_NOTIFIER\_HEAD(name) 初始化链表头，其注册、注销及通知接口分别为：

1. **int** raw\_notifier\_chain\_register(**struct** raw\_notifier\_head \*nh, **struct** notifier\_block \*nb);
2. **int** raw\_notifier\_chain\_unregister(**struct** raw\_notifier\_head \*nh, **struct** notifier\_block \*nb);
3. **int** raw\_notifier\_call\_chain(**struct** raw\_notifier\_head \*nh, unsigned **long** val, **void** \*v);

## 4、SRCU notifier chains

可阻塞通知链的一种变体

1. **struct** srcu\_notifier\_head {
2. **struct** mutex mutex;
3. **struct** srcu\_struct srcu;
4. **struct** notifier\_block \*head;
5. };

该链表头必须动态申请 srcu\_init\_notifier\_head 和释放 srcu\_cleanup\_notifier\_head，其注册、注销及通知接口分别为：

1. **int** srcu\_notifier\_chain\_register(**struct** srcu\_notifier\_head \*nh, **struct** notifier\_block \*nb);
2. **int** srcu\_notifier\_chain\_unregister(**struct** srcu\_notifier\_head \*nh, **struct** notifier\_block \*nb);
3. **int** srcu\_notifier\_call\_chain(**struct** srcu\_notifier\_head \*nh, unsigned **long** val, **void** \*v);

## ****5、notifier\_call\_chain****

当有事件触发时，通知者调用 notifier\_call\_chain 函数通知事件的到达，这个函数会遍历nl指向的通知链中所有的元素，然后依次调用每一个的回调函数，完成通知动作。

1. **static** **int** \_\_kprobes notifier\_call\_chain(**struct** notifier\_block \*\*nl,
2. unsigned **long** val, **void** \*v,
3. **int** nr\_to\_call, **int** \*nr\_calls)

参数nl是通知链的头部，val表示事件类型，v用来指向通知链上的函数执行时需要用到的参数，一般不同的通知链，参数类型也不一样，例如当通知一个网卡被注册时，v就指向net\_device结构，nr\_to\_call表示准备最多通知几个，-1表示整条链都通知，nr\_calls非空的话，返回通知了多少个。每个被执行的 notifier\_block 回调函数的**返回值**可能取值为以下几个：  
NOTIFY\_DONE：表示对相关的事件类型不关心  
NOTIFY\_OK：顺利执行  
NOTIFY\_BAD：执行有错  
NOTIFY\_STOP：停止执行后面的回调函数  
NOTIFY\_STOP\_MASK：停止执行的掩码  
notifier\_call\_chain 把最后一个被调用的回调函数的返回值作为它的返回值。

## notifier chain 使用方法

在常见的环境中，我们通常会对 notifier chain 做一定的封装再使用。比如在电源管理子系统中，做了如下的定义和封装：

1. **static** BLOCKING\_NOTIFIER\_HEAD(pm\_chain\_head);         // 初始化链表头部
3. **int** register\_pm\_notifier(**struct** notifier\_block \*nb)   // 注册函数
4. {
5. **return** blocking\_notifier\_chain\_register(&pm\_chain\_head, nb);
6. }
7. EXPORT\_SYMBOL\_GPL(register\_pm\_notifier);
9. **int** unregister\_pm\_notifier(**struct** notifier\_block \*nb)  // 注销函数
10. {
11. **return** blocking\_notifier\_chain\_unregister(&pm\_chain\_head, nb);
12. }
13. EXPORT\_SYMBOL\_GPL(unregister\_pm\_notifier);
15. **int** pm\_notifier\_call\_chain(unsigned **long** val)          // 通知函数
16. {
17. **return** (blocking\_notifier\_call\_chain(&pm\_chain\_head, val, NULL)
18. == NOTIFY\_BAD) ? -EINVAL : 0;
19. }

**Ps :blocking\_notifier\_chain\_register一次性执行两遍会使原本为单链的call变成一个环，死循环**

## 参考资料

<http://blog.csdn.net/g_salamander/article/details/8081724>

http://blog.csdn.net/wuhzossibility/article/details/8079025

# Socket通信机制

## ****socket****套接字：

     socket起源于Unix，而Unix/[Linux](http://lib.csdn.net/base/linux)基本哲学之一就是“一切皆文件”，都可以用“打开open –> 读写write/read –> 关闭close”模式来操作。Socket就是该模式的一个实现，socket即是一种特殊的文件，一些socket函数就是对其进行的操作（读/写IO、打开、关闭）.  
     说白了Socket是应用层与TCP/IP协议族通信的中间软件抽象层，**它是一组接口**。在设计模式中，Socket其实就是一个门面模式，它把复杂的TCP/IP协议族隐藏在Socket接口后面，对用户来说，一组简单的接口就是全部，让Socket去组织数据，以符合指定的协议。

       注意：其实socket也没有层的概念，它只是一个facade设计模式的应用，让编程变的更简单。是一个软件抽象层。在网络编程中，我们大量用的都是通过socket实现的。

## ****套接字描述符：****

     其实就是一个整数，我们最熟悉的句柄是0、1、2三个，0是标准输入，1是标准输出，2是标准错误输出。0、1、2是整数表示的，对应的FILE \*结构的表示就是stdin、stdout、stderr

套接字API最初是作为UNIX操作系统的一部分而开发的，所以套接字API与系统的其他I/O设备集成在一起。特别是，当应用程序要为因特网通信而创建一个套接字（socket）时，操作系统就返回一个小整数作为描述符（descriptor）来标识这个套接字。然后，应用程序以该描述符作为传递参数，通过调用函数来完成某种操作（例如通过网络传送数据或接收输入的数据）。

在许多操作系统中，套接字描述符和其他I/O描述符是集成在一起的，所以应用程序可以对文件进行套接字I/O或I/O读/写操作。

当应用程序要创建一个套接字时，操作系统就返回一个小整数作为描述符，应用程序则使用这个描述符来引用该套接字需要I/O请求的应用程序请求操作系统打开一个文件。操作系统就创建一个文件描述符提供给应用程序访问文件。从应用程序的角度看，文件描述符是一个整数，应用程序可以用它来读写文件。下图显示，操作系统如何把文件描述符实现为一个指针数组，这些指针指向内部[**数据结构**](http://lib.csdn.net/base/datastructure)。



     对于每个程序系统都有一张单独的表。精确地讲，系统为每个运行的进程维护一张单独的文件描述符表。当进程打开一个文件时，系统把一个指向此文件内部数据结构的指针写入文件描述符表，并把该表的索引值返回给调用者 。应用程序只需记住这个描述符，并在以后操作该文件时使用它。操作系统把该描述符作为索引访问进程描述符表，通过指针找到保存该文件所有的信息的数据结构。

**针对套接字的系统数据结构：**

   1）、套接字API里有个函数socket，它就是用来创建一个套接字。套接字设计的总体思路是，单个系统调用就可以创建任何套接字，因为套接字是相当笼统的。一旦套接字创建后，应用程序还需要调用其他函数来指定具体细节。例如调用socket将创建一个新的描述符条目：



   2）、虽然套接字的内部数据结构包含很多字段，但是系统创建套接字后，大多数字字段没有填写。应用程序创建套接字后在该套接字可以使用之前，必须调用其他的过程来填充这些字段。

## ****文件描述符和文件指针的区别：****

**文件描述符：**在linux系统中打开文件就会获得文件描述符，它是个很小的正整数。每个进程在PCB（Process Control Block）中保存着一份文件描述符表，文件描述符就是这个表的索引，每个表项都有一个指向已打开文件的指针。

**文件指针：**[**C语言**](http://lib.csdn.net/base/c)中使用文件指针做为I/O的句柄。文件指针指向进程用户区中的一个被称为FILE结构的数据结构。FILE结构包括一个缓冲区和一个文件描述符。而文件描述符是文件描述符表的一个索引，因此从某种意义上说文件指针就是句柄的句柄（在Windows系统上，文件描述符被称作文件句柄）。

详细内容请看[linux文件系统](http://blog.csdn.net/hguisu/article/details/6122513#t7)：<http://blog.csdn.net/hguisu/article/details/6122513#t7>

## 基本的SOCKET接口函数

在生活中，A要电话给B，A拨号，B听到电话铃声后提起电话，这时A和B就建立起了连接，A和B就可以讲话了。等交流结束，挂断电话结束此次交谈。  打电话很简单解释了这工作原理：“open—write/read—close”模式。



    服务器端先初始化Socket，然后与端口绑定(bind)，对端口进行监听(listen)，调用accept阻塞，等待客户端连接。在这时如果有个客户端初始化一个Socket，然后连接服务器(connect)，如果连接成功，这时客户端与服务器端的连接就建立了。客户端发送数据请求，服务器端接收请求并处理请求，然后把回应数据发送给客户端，客户端读取数据，最后关闭连接，一次交互结束。

**这些接口的实现都是内核来完成。具体如何实现，可以看看linux的内核**

## socket()函数

int **socket**(int protofamily, int type, int protocol);//返回sockfd

  sockfd是描述符。

  socket函数对应于普通文件的打开操作。普通文件的打开操作返回一个文件描述字，而**socket()**用于创建一个socket描述符（socket descriptor），它唯一标识一个socket。这个socket描述字跟文件描述字一样，后续的操作都有用到它，把它作为参数，通过它来进行一些读写操作。

      正如可以给fopen的传入不同参数值，以打开不同的文件。创建socket的时候，也可以指定不同的参数创建不同的socket描述符，socket函数的三个参数分别为：

protofamily：即协议域，又称为协议族（family）。常用的协议族有，AF\_INET(IPV4)、AF\_INET6(IPV6)、AF\_LOCAL（或称AF\_UNIX，Unix域socket）、AF\_ROUTE等等。协议族决定了socket的地址类型，在通信中必须采用对应的地址，如AF\_INET决定了要用ipv4地址（32位的）与端口号（16位的）的组合、AF\_UNIX决定了要用一个绝对路径名作为地址。

type：指定socket类型。常用的socket类型有，SOCK\_STREAM、SOCK\_DGRAM、SOCK\_RAW、SOCK\_PACKET、SOCK\_SEQPACKET等等（socket的类型有哪些？）。

protocol：故名思意，就是指定协议。常用的协议有，IPPROTO\_TCP、IPPTOTO\_UDP、IPPROTO\_SCTP、IPPROTO\_TIPC等，它们分别对应TCP传输协议、UDP传输协议、STCP传输协议、TIPC传输协议（这个协议我将会单独开篇讨论！）。

**注意**：并不是上面的type和protocol可以随意组合的，如SOCK\_STREAM不可以跟IPPROTO\_UDP组合。当protocol为0时，会自动选择type类型对应的默认协议。

当我们调用**socket**创建一个socket时，返回的socket描述字它存在于协议族（address family，AF\_XXX）空间中，但没有一个具体的地址。如果想要给它赋值一个地址，就必须调用bind()函数，否则就当调用connect()、listen()时系统会自动随机分配一个端口。

## bind()函数

正如上面所说bind()函数把一个地址族中的特定地址赋给socket。例如对应AF\_INET、AF\_INET6就是把一个ipv4或ipv6地址和端口号组合赋给socket。

int bind(int sockfd, const struct sockaddr \*addr, socklen\_t addrlen);

函数的三个参数分别为：

sockfd：即socket描述字，它是通过socket()函数创建了，唯一标识一个socket。bind()函数就是将给这个描述字绑定一个名字。

addr：一个const struct sockaddr \*指针，指向要绑定给sockfd的协议地址。这个地址结构根据地址创建socket时的地址协议族的不同而不同，如ipv4对应的是：

struct sockaddr\_in {

sa\_family\_t sin\_family; /\* address family: AF\_INET \*/

in\_port\_t sin\_port; /\* port in network byte order \*/

struct in\_addr sin\_addr; /\* internet address \*/

};

/\* Internet address. \*/

struct in\_addr {

uint32\_t s\_addr; /\* address in network byte order \*/

};

ipv6对应的是：

struct sockaddr\_in6 {

sa\_family\_t sin6\_family; /\* AF\_INET6 \*/

in\_port\_t sin6\_port; /\* port number \*/

uint32\_t sin6\_flowinfo; /\* IPv6 flow information \*/

struct in6\_addr sin6\_addr; /\* IPv6 address \*/

uint32\_t sin6\_scope\_id; /\* Scope ID (new in 2.4) \*/

};

struct in6\_addr {

unsigned char s6\_addr[16]; /\* IPv6 address \*/

};

Unix域对应的是：

#define UNIX\_PATH\_MAX 108

struct sockaddr\_un {

sa\_family\_t sun\_family; /\* AF\_UNIX \*/

char sun\_path[UNIX\_PATH\_MAX]; /\* pathname \*/

};

addrlen：对应的是地址的长度。

通常服务器在启动的时候都会绑定一个众所周知的地址（如ip地址+端口号），用于提供服务，客户就可以通过它来接连服务器；而客户端就不用指定，有系统自动分配一个端口号和自身的ip地址组合。这就是为什么通常服务器端在listen之前会调用bind()，而客户端就不会调用，而是在connect()时由系统随机生成一个。

## 网络字节序与主机字节序

**主机字节序**就是我们平常说的大端和小端模式：不同的CPU有不同的字节序类型，这些字节序是指整数在内存中保存的顺序，这个叫做主机序。引用标准的Big-Endian和Little-Endian的定义如下：

　　a) Little-Endian就是低位字节排放在内存的低地址端，高位字节排放在内存的高地址端。

　　b) Big-Endian就是高位字节排放在内存的低地址端，低位字节排放在内存的高地址端。

**网络字节序**：4个字节的32 bit值以下面的次序传输：首先是0～7bit，其次8～15bit，然后16～23bit，最后是24~31bit。这种传输次序称作大端字节序。**由于TCP/IP首部中所有的二进制整数在网络中传输时都要求以这种次序，因此它又称作网络字节序。**字节序，顾名思义字节的顺序，就是大于一个字节类型的数据在内存中的存放顺序，一个字节的数据没有顺序的问题了。

所以：在将一个地址绑定到socket的时候，请先将主机字节序转换成为网络字节序，而不要假定主机字节序跟网络字节序一样使用的是Big-Endian。由于这个问题曾引发过血案！公司项目代码中由于存在这个问题，导致了很多莫名其妙的问题，所以请谨记对主机字节序不要做任何假定，务必将其转化为网络字节序再赋给socket。

## listen()、connect()函数

如果作为一个服务器，在调用socket()、bind()之后就会调用listen()来监听这个socket，如果客户端这时调用connect()发出连接请求，服务器端就会接收到这个请求。

int listen(int sockfd, int backlog);

int connect(int sockfd, const struct sockaddr \*addr, socklen\_t addrlen);

listen函数的第一个参数即为要监听的socket描述字，第二个参数为相应socket可以排队的最大连接个数。socket()函数创建的socket默认是一个主动类型的，listen函数将socket变为被动类型的，等待客户的连接请求。

connect函数的第一个参数即为客户端的socket描述字，第二参数为服务器的socket地址，第三个参数为socket地址的长度。客户端通过调用connect函数来建立与TCP服务器的连接。

## accept()函数

TCP服务器端依次调用socket()、bind()、listen()之后，就会监听指定的socket地址了。TCP客户端依次调用socket()、connect()之后就向TCP服务器发送了一个连接请求。TCP服务器监听到这个请求之后，就会调用accept()函数取接收请求，这样连接就建立好了。之后就可以开始网络I/O操作了，即类同于普通文件的读写I/O操作。

int accept(int sockfd, struct sockaddr \*addr, socklen\_t \*addrlen); //返回连接connect\_fd

参数sockfd

参数sockfd就是上面解释中的监听套接字，这个套接字用来监听一个端口，当有一个客户与服务器连接时，它使用这个一个端口号，而此时这个端口号正与这个套接字关联。当然客户不知道套接字这些细节，它只知道一个地址和一个端口号。

参数addr

这是一个结果参数，它用来接受一个返回值，这返回值指定客户端的地址，当然这个地址是通过某个地址结构来描述的，用户应该知道这一个什么样的地址结构。如果对客户的地址不感兴趣，那么可以把这个值设置为NULL。

参数len

如同大家所认为的，它也是结果的参数，用来接受上述addr的结构的大小的，它指明addr结构所占有的字节个数。同样的，它也可以被设置为NULL。

如果accept成功返回，则服务器与客户已经正确建立连接了，此时服务器通过accept返回的套接字来完成与客户的通信。

注意：

      accept默认会阻塞进程，直到有一个客户连接建立后返回，它返回的是一个新可用的套接字，这个套接字是连接套接字。

此时我们需要区分两种套接字，

       监听套接字: 监听套接字正如accept的参数sockfd，它是监听套接字，在调用listen函数之后，是服务器开始调用socket()函数生成的，称为监听socket描述字(监听套接字)

       连接套接字：一个套接字会从主动连接的套接字变身为一个监听套接字；而accept函数返回的是已连接socket描述字(一个连接套接字)，它代表着一个网络已经存在的点点连接。

        一个服务器通常通常仅仅只创建一个监听socket描述字，它在该服务器的生命周期内一直存在。内核为每个由服务器进程接受的客户连接创建了一个已连接socket描述字，当服务器完成了对某个客户的服务，相应的已连接socket描述字就被关闭。

        自然要问的是：为什么要有两种套接字？原因很简单，如果使用一个描述字的话，那么它的功能太多，使得使用很不直观，同时在内核确实产生了一个这样的新的描述字。

连接套接字socketfd\_new 并没有占用新的端口与客户端通信，依然使用的是与监听套接字socketfd一样的端口号

## read()、write()等函数

万事具备只欠东风，至此服务器与客户已经建立好连接了。可以调用网络I/O进行读写操作了，即实现了网咯中不同进程之间的通信！网络I/O操作有下面几组：

read()/write()

recv()/send()

readv()/writev()

recvmsg()/sendmsg()

recvfrom()/sendto()

我推荐使用recvmsg()/sendmsg()函数，这两个函数是最通用的I/O函数，实际上可以把上面的其它函数都替换成这两个函数。它们的声明如下：

#include <unistd.h>

ssize\_t read(int fd, void \*buf, size\_t count);

ssize\_t write(int fd, const void \*buf, size\_t count);

#include <sys/types.h>

#include <sys/socket.h>

ssize\_t send(int sockfd, const void \*buf, size\_t len, int flags);

ssize\_t recv(int sockfd, void \*buf, size\_t len, int flags);

ssize\_t sendto(int sockfd, const void \*buf, size\_t len, int flags,

const struct sockaddr \*dest\_addr, socklen\_t addrlen);

ssize\_t recvfrom(int sockfd, void \*buf, size\_t len, int flags,

struct sockaddr \*src\_addr, socklen\_t \*addrlen);

ssize\_t sendmsg(int sockfd, const struct msghdr \*msg, int flags);

ssize\_t recvmsg(int sockfd, struct msghdr \*msg, int flags);

read函数是负责从fd中读取内容.当读成功时，read返回实际所读的字节数，如果返回的值是0表示已经读到文件的结束了，小于0表示出现了错误。如果错误为EINTR说明读是由中断引起的，如果是ECONNREST表示网络连接出了问题。

write函数将buf中的nbytes字节内容写入文件描述符fd.成功时返回写的字节数。失败时返回-1，并设置errno变量。 在网络程序中，当我们向套接字文件描述符写时有俩种可能。1)write的返回值大于0，表示写了部分或者是全部的数据。2)返回的值小于0，此时出现了错误。我们要根据错误类型来处理。如果错误为EINTR表示在写的时候出现了中断错误。如果为EPIPE表示网络连接出现了问题(对方已经关闭了连接)。

其它的我就不一一介绍这几对I/O函数了，具体参见man文档或者baidu、Google，下面的例子中将使用到send/recv。

## close()函数

在服务器与客户端建立连接之后，会进行一些读写操作，完成了读写操作就要关闭相应的socket描述字，好比操作完打开的文件要调用fclose关闭打开的文件。

#include <unistd.h>

int close(int fd);

close一个TCP socket的缺省行为时把该socket标记为以关闭，然后立即返回到调用进程。该描述字不能再由调用进程使用，也就是说不能再作为read或write的第一个参数。

注意：close操作只是使相应socket描述字的引用计数-1，只有当引用计数为0的时候，才会触发TCP客户端向服务器发送终止连接请求。

## Netlink机制及其关键技术

### 3.1 Netlink机制

Linux操作系统中当CPU处于内核状态时，可以分为有用户上下文的状态和执行硬件、软件中断两种。其中当处于有用户上下文时，由于内核态和用户态的内存映射机制不同，不可直接将本地变量传给用户态的内存区；处于硬件、软件中断时，无法直接向用户内存区传递数据，代码执行不可中断。针对传统的进程间通信机制，他们均无法直接在内核态和用户态之间使用，原因如下表：

|  |  |
| --- | --- |
| 通信方法 | 无法介于内核态与用户态的原因 |
| 管道（不包括命名管道） | 局限于父子进程间的通信。 |
| 消息队列 | 在硬、软中断中无法无阻塞地接收数据。 |
| 信号量 | 无法介于内核态和用户态使用。 |
| 内存共享 | 需要信号量辅助，而信号量又无法使用。 |
| 套接字 | 在硬、软中断中无法无阻塞地接收数据。 |

1\*（引自 参考文献5）

    解决内核态和用户态通信机制可分为两类：

1. 处于有用户上下文时，可以使用Linux提供的copy\_from\_user()和copy\_to\_user()函数完成，但由于这两个函数可能阻塞，因此不能在硬件、软件的中断过程中使用。
2. 处于硬、软件中断时。

2.1   可以通过Linux内核提供的spinlock自旋锁实现内核线程与中断过程的同步，由于内核线程运行在有上下文的进程中，因此可以在内核线程中使用套接字或消息队列来取得用户空间的数据，然后再将数据通过临界区传递给中断过程.

2.2   通过Netlink机制实现。Netlink 套接字的通信依据是一个对应于进程的标识，一般定为该进程的 ID。Netlink通信最大的特点是对对中断过程的支持，它在内核空间接收用户空间数据时不再需要用户自行启动一个内核线程，而是通过另一个软中断调用用户事先指定的接收函数。通过软中断而不是自行启动内核线程保证了数据传输的及时性。

### 3.2 Netlink优点

Netlink相对于其他的通信机制具有以下优点：

1. 使用Netlink通过自定义一种新的协议并加入协议族即可通过socket API使用Netlink协议完成数据交换，而ioctl和proc文件系统均需要通过程序加入相应的设备或文件。
2. Netlink使用socket缓存队列，是一种异步通信机制，而ioctl是同步通信机制，如果传输的数据量较大，会影响系统性能。
3. Netlink支持多播，属于一个Netlink组的模块和进程都能获得该多播消息。
4. Netlink允许内核发起会话，而ioctl和系统调用只能由用户空间进程发起

## 建立Netlink会话过程如下：



内核使用与标准socket API类似的一套API完成通信过程。首先通过netlink\_kernel\_create()创建套接字，该函数的原型如下：

struct sock \*netlink\_kernel\_create(struct net \*net,  
  
int unit,unsigned int groups,  
  
void (\*input)(struct sk\_buff \*skb),  
  
struct mutex \*cb\_mutex,  
  
struct module \*module);

其中net参数是网络设备命名空间指针，input函数是netlink socket在接受到消息时调用的回调函数指针，module默认为THIS\_MODULE.

然后用户空间进程使用标准Socket API来创建套接字，将进程ID发送至内核空间，用户空间创建使用socket()创建套接字，该函数的原型如下：

int socket(int domain, int type, int protocol);

其中domain值为PF\_NETLINK，即Netlink使用协议族。protocol为Netlink提供的协议或者是用户自定义的协议，Netlink提供的协议包括NETLINK\_ROUTE, NETLINK\_FIREWALL, NETLINK\_ARPD, NETLINK\_ROUTE6和 NETLINK\_IP6\_FW。

接着使用bind函数绑定。Netlink的bind()函数把一个本地socket地址(源socket地址)与一个打开的socket进行关联。完成绑定，内核空间接收到用户进程ID之后便可以进行通讯。

用户空间进程发送数据使用标准socket API中sendmsg()函数完成，使用时需添加struct msghdr消息和nlmsghdr消息头。一个netlink消息体由nlmsghdr和消息的payload部分组成，输入消息后，内核会进入nlmsghdr指向的缓冲区。

内核空间发送数据使用独立创建的sk\_buff缓冲区，Linux定义了如下宏方便对于缓冲区地址的设置，如下所示：

#define NETLINK\_CB(skb) (\*(struct netlink\_skb\_parms\*)&((skb)->cb))

在对缓冲区设置完成消息地址之后，可以使用netlink\_unicast()来发布单播消息，netlink\_unicast()原型如下：

int netlink\_unicast(struct sock \*sk, struct sk\_buff \*skb, u32 pid, int nonblock);

参数sk为函数netlink\_kernel\_create()返回的socket，参数skb存放消息，它的data字段指向要发送的netlink消息结构，而skb的控制块保存了消息的地址信息，前面的宏NETLINK\_CB(skb)就用于方便设置该控制块，参数pid为接收消息进程的pid，参数nonblock表示该函数是否为非阻塞，如果为1，该函数将在没有接收缓存可利用时立即返回，而如果为0，该函数在没有接收缓存可利用时睡眠。

内核模块或子系统也可以使用函数netlink\_broadcast来发送广播消息：

void netlink\_broadcast(struct sock \*sk, struct sk\_buff \*skb, u32 pid, u32 group, int allocation);

前面的三个参数与netlink\_unicast相同，参数group为接收消息的多播组，该参数的每一个代表一个多播组，因此如果发送给多个多播组，就把该参数设置为多个多播组组ID的位或。参数allocation为内核内存分配类型，一般地为GFP\_ATOMIC或GFP\_KERNEL，GFP\_ATOMIC用于原子的上下文（即不可以睡眠），而GFP\_KERNEL用于非原子上下文。

接收数据时程序需要申请足够大的空间来存储netlink消息头和消息的payload部分。然后使用标准函数接口recvmsg()来接收netlink消息

其他相关说明

    Netlink 是一种特殊的 socket，它是 Linux 所特有的，类似于 BSD 中的AF\_ROUTE 但又远比它的功能强大，目前在最新的 Linux 内核（2.6.14）中使用netlink 进行应用与内核通信的应用很多，包括：路由 daemon（NETLINK\_ROUTE），1-wire 子系统（NETLINK\_W1），用户态 socket 协议（NETLINK\_USERSOCK），防火墙（NETLINK\_FIREWALL），socket 监视（NETLINK\_INET\_DIAG），netfilter 日志（NETLINK\_NFLOG），ipsec 安全策略（NETLINK\_XFRM），SELinux 事件通知（NETLINK\_SELINUX），iSCSI 子系统（NETLINK\_ISCSI），进程审计（NETLINK\_AUDIT），转发信息表查询（NETLINK\_FIB\_LOOKUP），netlink connector(NETLINK\_CONNECTOR),netfilter 子系统（NETLINK\_NETFILTER），IPv6 防火墙（NETLINK\_IP6\_FW），DECnet 路由信息（NETLINK\_DNRTMSG），内核事件向用户态通知（NETLINK\_KOBJECT\_UEVENT），通用 netlink（NETLINK\_GENERIC）。

    Netlink 是一种在内核与用户应用间进行双向数据传输的非常好的方式，用户态应用使用标准的 socket API 就可以使用 netlink 提供的强大功能，内核态需要使用专门的内核 API 来使用 netlink。

Netlink 相对于系统调用，ioctl 以及 /proc 文件系统而言具有以下优点：

    1，为了使用 netlink，用户仅需要在 include/linux/netlink.h 中增加一个新类型的 netlink 协议定义即可， 如 #define NETLINK\_MYTEST 17 然后，内核和用户态应用就可以立即通过 socket API 使用该 netlink 协议类型进行数据交换。但系统调用需要增加新的系统调用，ioctl 则需要增加设备或文件， 那需要不少代码，proc 文件系统则需要在 /proc 下添加新的文件或目录，那将使本来就混乱的 /proc 更加混乱。

    2. netlink是一种异步通信机制，在内核与用户态应用之间传递的消息保存在socket缓存队列中，发送消息只是把消息保存在接收者的socket的接收队列，而不需要等待接收者收到消息，但系统调用与 ioctl 则是同步通信机制，如果传递的数据太长，将影响调度粒度。

    3．使用 netlink 的内核部分可以采用模块的方式实现，使用 netlink 的应用部分和内核部分没有编译时依赖，但系统调用就有依赖，而且新的系统调用的实现必须静态地连接到内核中，它无法在模块中实现，使用新系统调用的应用在编译时需要依赖内核。

    4．netlink 支持多播，内核模块或应用可以把消息多播给一个netlink组，属于该neilink 组的任何内核模块或应用都能接收到该消息，内核事件向用户态的通知机制就使用了这一特性，任何对内核事件感兴趣的应用都能收到该子系统发送的内核事件，在后面的文章中将介绍这一机制的使用。

    5．内核可以使用 netlink 首先发起会话，但系统调用和 ioctl 只能由用户应用发起调用。

    6．netlink 使用标准的 socket API，因此很容易使用，但系统调用和 ioctl则需要专门的培训才能使用。

**用户态使用 netlink**

   用户态应用使用标准的socket APIs， socket(), bind(), sendmsg(), recvmsg() 和 close() 就能很容易地使用 netlink socket，查询手册页可以了解这些函数的使用细节，本文只是讲解使用 netlink 的用户应该如何使用这些函数。注意，使用 netlink 的应用必须包含头文件 linux/netlink.h。当然 socket 需要的头文件也必不可少，sys/socket.h。

   为了创建一个 netlink socket，用户需要使用如下参数调用 socket():

|  |
| --- |
| socket(AF\_NETLINK, SOCK\_RAW, netlink\_type) |

   第一个参数必须是 AF\_NETLINK 或 PF\_NETLINK，在 Linux 中，它们俩实际为一个东西，它表示要使用netlink，第二个参数必须是SOCK\_RAW或SOCK\_DGRAM，第三个参数指定netlink协议类型，如前面讲的用户自定义协议类型NETLINK\_MYTEST， NETLINK\_GENERIC是一个通用的协议类型，它是专门为用户使用的，因此，用户可以直接使用它，而不必再添加新的协议类型。内核预定义的协议类型有：

#define NETLINK\_ROUTE 0  
#define NETLINK\_W1 1  
#define NETLINK\_USERSOCK 2   
#define NETLINK\_FIREWALL 3  
#define NETLINK\_INET\_DIAG 4  
#define NETLINK\_NFLOG 5  
#define NETLINK\_XFRM 6   
#define NETLINK\_SELINUX 7   
#define NETLINK\_ISCSI 8   
#define NETLINK\_AUDIT 9   
#define NETLINK\_FIB\_LOOKUP 10   
#define NETLINK\_CONNECTOR 11   
#define NETLINK\_NETFILTER 12   
#define NETLINK\_IP6\_FW 13   
#define NETLINK\_DNRTMSG 14   
#define NETLINK\_KOBJECT\_UEVENT 15   
#define NETLINK\_GENERIC 16

[复制代码](http://blog.sina.com.cn/s/blog_62ec291601010qgh.html)

   对于每一个netlink协议类型，可以有多达 32多播组，每一个多播组用一个位表示，netlink 的多播特性使得发送消息给同一个组仅需要一次系统调用，因而对于需要多拨消息的应用而言，大大地降低了系统调用的次数。

   函数 bind() 用于把一个打开的 netlink socket 与 netlink 源 socket 地址绑定在一起。netlink socket 的地址结构如下：

struct sockaddr\_nl {  
sa\_family\_t nl\_family;  
unsigned short nl\_pad;  
\_\_u32 nl\_pid;  
\_\_u32 nl\_groups;  
};

[复制代码](http://blog.sina.com.cn/s/blog_62ec291601010qgh.html)

   字段 nl\_family 必须设置为 AF\_NETLINK 或着 PF\_NETLINK，字段 nl\_pad 当前没有使用，因此要总是设置为 0，字段 nl\_pid 为接收或发送消息的进程的 ID，如果希望内核处理消息或多播消息，就把该字段设置为 0，否则设置为处理消息的进程 ID。字段 nl\_groups 用于指定多播组，bind 函数用于把调用进程加入到该字段指定的多播组，如果设置为 0，表示调用者不加入任何多播组。

   传递给 bind 函数的地址的 nl\_pid 字段应当设置为本进程的进程 ID，这相当于 netlink socket 的本地地址。但是，对于一个进程的多个线程使用 netlink socket 的情况，字段 nl\_pid 则可以设置为其它的值，如：

|  |
| --- |
| pthread\_self() << 16 | getpid(); |

   因此字段 nl\_pid 实际上未必是进程 ID,它只是用于区分不同的接收者或发送者的一个标识，用户可以根据自己需要设置该字段。函数 bind 的调用方式如下：

|  |
| --- |
| bind(fd, (struct sockaddr\*)&nladdr, sizeof(struct sockaddr\_nl)); |

   fd为前面的 socket 调用返回的文件描述符，参数 nladdr 为 struct sockaddr\_nl 类型的地址。为了发送一个 netlink 消息给内核或其他用户态应用，需要填充目标 netlink socket 地址，此时，字段 nl\_pid 和 nl\_groups 分别表示接收消息者的进程 ID 与多播组。如果字段 nl\_pid 设置为 0，表示消息接收者为内核或多播组，如果 nl\_groups为 0，表示该消息为单播消息，否则表示多播消息。使用函数 sendmsg 发送 netlink 消息时还需要引用结构 struct msghdr、struct nlmsghdr 和 struct iovec，结构 struct msghdr 需如下设置：

struct msghdr msg;  
memset(&msg, 0, sizeof(msg));  
msg.msg\_name = (void \*)&(nladdr);  
msg.msg\_namelen = sizeof(nladdr);

[复制代码](http://blog.sina.com.cn/s/blog_62ec291601010qgh.html)

其中 nladdr 为消息接收者的 netlink 地址。

   struct nlmsghdr 为 netlink socket 自己的消息头，这用于多路复用和多路分解 netlink 定义的所有协议类型以及其它一些控制，netlink 的内核实现将利用这个消息头来多路复用和多路分解已经其它的一些控制，因此它也被称为netlink 控制块。因此，应用在发送 netlink 消息时必须提供该消息头。

struct nlmsghdr {  
\_\_u32 nlmsg\_len;  
\_\_u16 nlmsg\_type;  
\_\_u16 nlmsg\_flags;  
\_\_u32 nlmsg\_seq;  
\_\_u32 nlmsg\_pid;  
};

[复制代码](http://blog.sina.com.cn/s/blog_62ec291601010qgh.html)

字段 nlmsg\_len 指定消息的总长度，包括紧跟该结构的数据部分长度以及该结构的大小，字段 nlmsg\_type 用于应用内部定义消息的类型，它对 netlink 内核实现是透明的，因此大部分情况下设置为 0，字段 nlmsg\_flags 用于设置消息标志，可用的标志包括：

#define NLM\_F\_REQUEST 1   
#define NLM\_F\_MULTI 2   
#define NLM\_F\_ACK 4   
#define NLM\_F\_ECHO 8   
#define NLM\_F\_ROOT 0x100   
#define NLM\_F\_MATCH 0x200   
#define NLM\_F\_ATOMIC 0x400   
#define NLM\_F\_DUMP (NLM\_F\_ROOT|NLM\_F\_MATCH)   
#define NLM\_F\_REPLACE 0x100   
#define NLM\_F\_EXCL 0x200   
#define NLM\_F\_CREATE 0x400   
#define NLM\_F\_APPEND 0x800

[复制代码](http://blog.sina.com.cn/s/blog_62ec291601010qgh.html)

标志NLM\_F\_REQUEST用于表示消息是一个请求，所有应用首先发起的消息都应设置该标志。

标志NLM\_F\_MULTI 用于指示该消息是一个多部分消息的一部分，后续的消息可以通过宏NLMSG\_NEXT来获得。

宏NLM\_F\_ACK表示该消息是前一个请求消息的响应，顺序号与进程ID可以把请求与响应关联起来。

标志NLM\_F\_ECHO表示该消息是相关的一个包的回传。

标志NLM\_F\_ROOT 被许多 netlink 协议的各种数据获取操作使用，该标志指示被请求的数据表应当整体返回用户应用，而不是一个条目一个条目地返回。有该标志的请求通常导致响应消息设置NLM\_F\_MULTI标志。注意，当设置了该标志时，请求是协议特定的，因此，需要在字段 nlmsg\_type 中指定协议类型。

标志 NLM\_F\_MATCH 表示该协议特定的请求只需要一个数据子集，数据子集由指定的协议特定的过滤器来匹配。

标志 NLM\_F\_ATOMIC 指示请求返回的数据应当原子地收集，这预防数据在获取期间被修改。

标志 NLM\_F\_DUMP 未实现。

标志 NLM\_F\_REPLACE 用于取代在数据表中的现有条目。

标志 NLM\_F\_EXCL\_ 用于和 CREATE 和 APPEND 配合使用，如果条目已经存在，将失败。

标志 NLM\_F\_CREATE 指示应当在指定的表中创建一个条目。

标志 NLM\_F\_APPEND 指示在表末尾添加新的条目。

内核需要读取和修改这些标志，对于一般的使用，用户把它设置为 0 就可以，只是一些高级应用（如 netfilter 和路由 daemon 需要它进行一些复杂的操作），字段 nlmsg\_seq 和 nlmsg\_pid 用于应用追踪消息，前者表示顺序号，后者为消息来源进程 ID。下面是一个示例：

#define MAX\_MSGSIZE 1024  
char buffer[] = "An example message";  
struct nlmsghdr nlhdr;  
nlhdr = (struct nlmsghdr \*)malloc(NLMSG\_SPACE(MAX\_MSGSIZE));  
strcpy(NLMSG\_DATA(nlhdr),buffer);  
nlhdr->nlmsg\_len = NLMSG\_LENGTH(strlen(buffer));  
nlhdr->nlmsg\_pid = getpid();  
nlhdr->nlmsg\_flags = 0;

[复制代码](http://blog.sina.com.cn/s/blog_62ec291601010qgh.html)

结构 struct iovec 用于把多个消息通过一次系统调用来发送，下面是该结构使用示例：

struct iovec iov;  
iov.iov\_base = (void \*)nlhdr;  
iov.iov\_len = nlh->nlmsg\_len;  
msg.msg\_iov = &iov;  
msg.msg\_iovlen = 1;

[复制代码](http://blog.sina.com.cn/s/blog_62ec291601010qgh.html)

在完成以上步骤后，消息就可以通过下面语句直接发送：

|  |
| --- |
| sendmsg(fd, &msg, 0); |

应用接收消息时需要首先分配一个足够大的缓存来保存消息头以及消息的数据部分，然后填充消息头，添完后就可以直接调用函数 recvmsg() 来接收。

#define MAX\_NL\_MSG\_LEN 1024   
struct sockaddr\_nl nladdr;  
struct msghdr msg;  
struct iovec iov;  
struct nlmsghdr \* nlhdr;  
nlhdr = (struct nlmsghdr \*)malloc(MAX\_NL\_MSG\_LEN);  
iov.iov\_base = (void \*)nlhdr;  
iov.iov\_len = MAX\_NL\_MSG\_LEN;  
msg.msg\_name = (void \*)&(nladdr);  
msg.msg\_namelen = sizeof(nladdr);  
msg.msg\_iov = &iov;  
msg.msg\_iovlen = 1;  
recvmsg(fd, &msg, 0);

[复制代码](http://blog.sina.com.cn/s/blog_62ec291601010qgh.html)

注意：fd为socket调用打开的netlink socket描述符。

在消息接收后，nlhdr指向接收到的消息的消息头，nladdr保存了接收到的消息的目标地址，宏NLMSG\_DATA(nlhdr)返回指向消息的数据部分的指针。

在linux/netlink.h中定义了一些方便对消息进行处理的宏，这些宏包括：

|  |
| --- |
| #define NLMSG\_ALIGNTO 4  #define NLMSG\_ALIGN(len) ( ((len)+NLMSG\_ALIGNTO-1) & ~(NLMSG\_ALIGNTO-1) ) |

宏NLMSG\_ALIGN(len)用于得到不小于len且字节对齐的最小数值。

|  |
| --- |
| #define NLMSG\_LENGTH(len) ((len)+NLMSG\_ALIGN(sizeof(struct nlmsghdr))) |

宏NLMSG\_LENGTH(len)用于计算数据部分长度为len时实际的消息长度。它一般用于分配消息缓存。

|  |
| --- |
| #define NLMSG\_SPACE(len) NLMSG\_ALIGN(NLMSG\_LENGTH(len)) |

宏NLMSG\_SPACE(len)返回不小于NLMSG\_LENGTH(len)且字节对齐的最小数值，它也用于分配消息缓存。

|  |
| --- |
| #define NLMSG\_DATA(nlh) ((void\*)(((char\*)nlh) + NLMSG\_LENGTH(0))) |

宏NLMSG\_DATA(nlh)用于取得消息的数据部分的首地址，设置和读取消息数据部分时需要使用该宏。

|  |
| --- |
| #define NLMSG\_NEXT(nlh,len) ((len) -= NLMSG\_ALIGN((nlh)->nlmsg\_len), \  (struct nlmsghdr\*)(((char\*)(nlh)) + NLMSG\_ALIGN((nlh)->nlmsg\_len))) |

宏NLMSG\_NEXT(nlh,len)用于得到下一个消息的首地址，同时len也减少为剩余消息的总长度，该宏一般在一个消息被分成几个部分发送或接收时使用。

|  |
| --- |
| #define NLMSG\_OK(nlh,len) ((len) >= (int)sizeof(struct nlmsghdr) && \  (nlh)->nlmsg\_len >= sizeof(struct nlmsghdr) && \  (nlh)->nlmsg\_len <= (len)) |

宏NLMSG\_OK(nlh,len)用于判断消息是否有len这么长。

|  |
| --- |
| #define NLMSG\_PAYLOAD(nlh,len) ((nlh)->nlmsg\_len - NLMSG\_SPACE((len))) |

宏NLMSG\_PAYLOAD(nlh,len)用于返回payload的长度。

函数close用于关闭打开的netlink socket。

**netlink内核API**

netlink的内核实现在.c文件net/core/af\_netlink.c中，内核模块要想使用netlink，也必须包含头文件linux/netlink.h。内核使用netlink需要专门的API，这完全不同于用户态应用对netlink的使用。如果用户需要增加新的netlink协议类型，必须通过修改linux/netlink.h来实现，当然，目前的netlink实现已经包含了一个通用的协议类型NETLINK\_GENERIC以方便用户使用，用户可以直接使用它而不必增加新的协议类型。前面讲到，为了增加新的netlink协议类型，用户仅需增加如下定义到linux/netlink.h就可以：

|  |
| --- |
| #define NETLINK\_MYTEST 17 |

只要增加这个定义之后，用户就可以在内核的任何地方引用该协议。

在内核中，为了创建一个netlink socket用户需要调用如下函数：

|  |
| --- |
| struct sock \* netlink\_kernel\_create(int unit, void (\*input)(struct sock \*sk, int len)); |

参数unit表示netlink协议类型，如NETLINK\_MYTEST，参数input则为内核模块定义的netlink消息处理函数，当有消息到达这个netlink socket时，该input函数指针就会被引用。函数指针input的参数sk实际上就是函数netlink\_kernel\_create返回的struct sock指针，sock实际是socket的一个内核表示数据结构，用户态应用创建的socket在内核中也会有一个struct sock结构来表示。下面是一个input函数的示例：

|  |
| --- |
| void input (struct sock \*sk, int len) { struct sk\_buff \*skb; struct nlmsghdr \*nlh = NULL; u8 \*data = NULL; while ((skb = skb\_dequeue(&sk->receive\_queue)) != NULL) { nlh = (struct nlmsghdr \*)skb->data; data = NLMSG\_DATA(nlh); } } |

函数input()会在发送进程执行sendmsg()时被调用，这样处理消息比较及时，但是，如果消息特别长时，这样处理将增加系统调用sendmsg()的执行时间，对于这种情况，可以定义一个内核线程专门负责消息接收，而函数input的工作只是唤醒该内核线程，这样sendmsg将很快返回。

函数skb = skb\_dequeue(&sk->receive\_queue)用于取得socket sk的接收队列上的消息，返回为一个struct sk\_buff的结构，skb->data指向实际的netlink消息。

函数skb\_recv\_datagram(nl\_sk)也用于在netlink socket nl\_sk上接收消息，与skb\_dequeue的不同指出是，如果socket的接收队列上没有消息，它将导致调用进程睡眠在等待队列nl\_sk->sk\_sleep，因此它必须在进程上下文使用，刚才讲的内核线程就可以采用这种方式来接收消息。

下面的函数input就是这种使用的示例：

|  |
| --- |
| void input (struct sock \*sk, int len) { wake\_up\_interruptible(sk->sk\_sleep); } |

当内核中发送netlink消息时，也需要设置目标地址与源地址，而且内核中消息是通过struct sk\_buff来管理的， linux/netlink.h中定义了一个宏：

|  |
| --- |
| #define NETLINK\_CB(skb) (\*(struct netlink\_skb\_parms\*)&((skb)->cb)) |

来方便消息的地址设置。下面是一个消息地址设置的例子：

|  |
| --- |
| NETLINK\_CB(skb).pid = 0; NETLINK\_CB(skb).dst\_pid = 0; NETLINK\_CB(skb).dst\_group = 1; |

字段pid表示消息发送者进程ID，也即源地址，对于内核，它为 0， dst\_pid 表示消息接收者进程 ID，也即目标地址，如果目标为组或内核，它设置为 0，否则 dst\_group 表示目标组地址，如果它目标为某一进程或内核，dst\_group 应当设置为 0。

在内核中，模块调用函数 netlink\_unicast 来发送单播消息：

|  |
| --- |
| int netlink\_unicast(struct sock \*sk, struct sk\_buff \*skb, u32 pid, int nonblock); |

参数sk为函数netlink\_kernel\_create()返回的socket，参数skb存放消息，它的data字段指向要发送的netlink消息结构，而skb的控制块保存了消息的地址信息，前面的宏NETLINK\_CB(skb)就用于方便设置该控制块，参数pid为接收消息进程的pid，参数nonblock表示该函数是否为非阻塞，如果为1，该函数将在没有接收缓存可利用时立即返回，而如果为0，该函数在没有接收缓存可利用时睡眠。

内核模块或子系统也可以使用函数netlink\_broadcast来发送广播消息：

|  |
| --- |
| void netlink\_broadcast(struct sock \*sk, struct sk\_buff \*skb, u32 pid, u32 group, int allocation); |

前面的三个参数与netlink\_unicast相同，参数group为接收消息的多播组，该参数的每一个代表一个多播组，因此如果发送给多个多播组，就把该参数设置为多个多播组组ID的位或。参数allocation为内核内存分配类型，一般地为GFP\_ATOMIC或GFP\_KERNEL，GFP\_ATOMIC用于原子的上下文（即不可以睡眠），而GFP\_KERNEL用于非原子上下文。

在内核中使用函数sock\_release来释放函数netlink\_kernel\_create()创建的netlink socket：

|  |
| --- |
| void sock\_release(struct socket \* sock); |

注意函数netlink\_kernel\_create()返回的类型为struct sock，因此函数sock\_release应该这种调用：

|  |
| --- |
| sock\_release(sk->sk\_socket); |

sk为函数netlink\_kernel\_create()的返回值。

sk为函数netlink\_kernel\_create()的返回值。在源代码包中给出了一个使用 netlink 的示例，它包括一个内核模块 netlink-exam-kern.c 和两个应用程序 netlink-exam-user-recv.c, netlink-exam-user-send.c。内核模块必须先插入到内核，然后在一个终端上运行用户态接收程序，在另一个终端上运行用户态发送程序，发送程序读取参数指定的文本文件并把它作为 netlink 消息的内容发送给内核模块，内核模块接受该消息保存到内核缓存中，它也通过proc接口出口到 procfs，因此用户也能够通过 /proc/netlink\_exam\_buffer 看到全部的内容，同时内核也把该消息发送给用户态接收程序，用户态接收程序将把接收到的内容输出到屏幕上。

## 参考资料

<http://blog.chinaunix.net/uid-23069658-id-3405954.html>

<http://blog.sina.com.cn/s/blog_62ec291601010qgh.html>

<http://blog.chinaunix.net/uid-20788470-id-1841640.html>

<http://blog.csdn.net/hguisu/article/details/7445768/>

# Linux工作队列

1. 什么是workqueue       Linux中的Workqueue机制就是为了简化内核线程的创建。通过调用workqueue的接口就能创建内核线程。并且可以根据当前系统CPU的个数创建线程的数量，使得线程处理的事务能够并行化。workqueue是内核中实现简单而有效的机制，他显然简化了内核daemon的创建，方便了用户的编程.

      工作队列**（workqueue）**是另外一种将工作推后执行的形式.工作队列可以把工作推后，交由一个内核线程去执行，也就是说，这个下半部分可以在进程上下文中执行。最重要的就是工作队列允许被重新调度甚至是睡眠。

**workqueue与tasklet类似，都是允许内核代码请求某个函数在将来的时间被调用（抄《ldd3》上的）每个workqueue就是一个内核进程。**

2. [数据结构](http://lib.csdn.net/base/31)     我们把推后执行的任务叫做工作（work），描述它的数据结构为work\_struct:

1. **struct work\_struct {**
2. atomic\_long\_t data;       /\*工作处理函数func的参数\*/
3. #define WORK\_STRUCT\_PENDING 0        /\* T if work item pending execution \*/
4. #define WORK\_STRUCT\_STATIC 1        /\* static initializer (debugobjects) \*/
5. #define WORK\_STRUCT\_FLAG\_MASK (3UL)
6. #define WORK\_STRUCT\_WQ\_DATA\_MASK (~WORK\_STRUCT\_FLAG\_MASK)
7. **struct list\_head entry;        /\*连接工作的指针\*/**
8. work\_func\_t func;              /\*工作处理函数\*/
9. #ifdef CONFIG\_LOCKDEP
10. **struct lockdep\_map lockdep\_map;**
11. #endif
12. };

      这些工作以队列结构组织成工作队列（workqueue），其数据结构为workqueue\_struct:

1. **struct workqueue\_struct {**
2. **struct cpu\_workqueue\_struct \*cpu\_wq;**
3. **struct list\_head list;**
4. **const char \*name;   /\*workqueue name\*/**
5. int singlethread;   /\*是不是单线程 - 单线程我们首选第一个CPU -0表示采用默认的工作者线程event\*/
6. int freezeable;  /\* Freeze threads during suspend \*/
7. int rt;
8. };

     如果是多线程，Linux根据当前系统CPU的个数创建cpu\_workqueue\_struct 其结构体就是:

1. truct cpu\_workqueue\_struct {
2. spinlock\_t lock;/\*因为工作者线程需要频繁的处理连接到其上的工作，所以需要枷锁保护\*/
3. **struct list\_head worklist;**
4. wait\_queue\_head\_t more\_work;
5. **struct work\_struct \*current\_work; /\*当前的work\*/**
6. **struct workqueue\_struct \*wq;   /\*所属的workqueue\*/**
7. **struct task\_struct \*thread; /\*任务的上下文\*/**
8. } \_\_\_\_cacheline\_aligned;

       在该结构主要维护了一个任务队列，以及内核线程需要睡眠的等待队列，另外还维护了一个任务上下文，即task\_struct。  
       三者之间的关系如下：



3. 创建工作 **3.1 创建工作queue  
a. create\_singlethread\_workqueue(name)**        该函数的实现机制如下图所示，函数返回一个类型为struct workqueue\_struct的指针变量，该指针变量所指向的内存地址在函数内部调用kzalloc动态生成。所以driver在不再使用该work queue的情况下调用:

        void destroy\_workqueue(struct workqueue\_struct \*wq)来释放此处的内存地址。



        图中的cwq是一per-CPU类型的地址空间。对于create\_singlethread\_workqueue而言，即使是对于多CPU系统，内核也只负责创建一个worker\_thread内核进程。该内核进程被创建之后，会先定义一个图中的wait节点，然后在一循环体中检查cwq中的worklist，如果该队列为空，那么就会把wait节点加入到cwq中的more\_work中，然后休眠在该等待队列中。

        Driver调用queue\_work（struct workqueue\_struct \*wq, struct work\_struct \*work）向wq中加入工作节点。work会依次加在cwq->worklist所指向的链表中。queue\_work向cwq->worklist中加入一个work节点，同时会调用wake\_up来唤醒休眠在cwq->more\_work上的worker\_thread进程。wake\_up会先调用wait节点上的autoremove\_wake\_function函数，然后将wait节点从cwq->more\_work中移走。

        worker\_thread再次被调度，开始处理cwq->worklist中的所有work节点...当所有work节点处理完毕，worker\_thread重新将wait节点加入到cwq->more\_work，然后再次休眠在该等待队列中直到Driver调用queue\_work...

**b. create\_workqueue**

       相对于create\_singlethread\_workqueue, create\_workqueue同样会分配一个wq的工作队列，但是不同之处在于，对于多CPU系统而言，对每一个CPU，都会为之创建一个per-CPU的cwq结构，对应每一个cwq，都会生成一个新的worker\_thread进程。但是当用queue\_work向cwq上提交work节点时，是哪个CPU调用该函数，那么便向该CPU对应的cwq上的worklist上增加work节点。

**c.小结**       当用户调用workqueue的初始化接口create\_workqueue或者create\_singlethread\_workqueue对workqueue队列进行初始化时，内核就开始为用户分配一个workqueue对象，并且将其链到一个全局的workqueue队列中。然后Linux根据当前CPU的情况，为workqueue对象分配与CPU个数相同的cpu\_workqueue\_struct对象，每个cpu\_workqueue\_struct对象都会存在一条任务队列。紧接着，Linux为每个cpu\_workqueue\_struct对象分配一个内核thread，即内核daemon去处理每个队列中的任务。至此，用户调用初始化接口将workqueue初始化完毕，返回workqueue的指针。

        workqueue初始化完毕之后，将任务运行的上下文环境构建起来了，但是具体还没有可执行的任务，所以，需要定义具体的work\_struct对象。然后将work\_struct加入到任务队列中，Linux会唤醒daemon去处理任务。

       上述描述的workqueue内核实现原理可以描述如下：



**3.2  创建工作**       要使用工作队列，首先要做的是创建一些需要推后完成的工作。可以通过DECLARE\_WORK在编译时静态地建该结构：  
       DECLARE\_WORK(name,void (\*func) (void \*), void \*data);  
      这样就会静态地创建一个名为name，待执行函数为func，参数为data的work\_struct结构。  
      同样，也可以在运行时通过指针创建一个工作：  
      INIT\_WORK(structwork\_struct \*work, woid(\*func) (void \*), void \*data);

4. 调度 **a. schedule\_work**

       在大多数情况下, 并不需要自己建立工作队列，而是只定义工作, 将工作结构挂接到内核预定义的事件工作队列中调度, 在kernel/workqueue.c中定义了一个静态全局量的工作队列static struct workqueue\_struct \*keventd\_wq;默认的工作者线程叫做events/n，这里n是处理器的编号，每个处理器对应一个线程。比如，单处理器的系统只有events/0这样一个线程。而双处理器的系统就会多一个events/1线程。  
       调度工作结构, 将工作结构添加到全局的事件工作队列keventd\_wq，调用了queue\_work通用模块。对外屏蔽了keventd\_wq的接口，用户无需知道此参数，相当于使用了默认参数。keventd\_wq由内核自己维护，创建，销毁。这样work马上就会被调度，一旦其所在的处理器上的工作者线程被唤醒，它就会被执行。

**b. schedule\_delayed\_work(&work,delay);**      有时候并不希望工作马上就被执行，而是希望它经过一段延迟以后再执行。在这种情况下，同时也可以利用timer来进行延时调度，到期后才由默认的定时器回调函数进行工作注册。延迟delay后，被定时器唤醒，将work添加到工作队列wq中。

      工作队列是没有优先级的，基本按照FIFO的方式进行处理。

## ****5. 示例****

1. #include <linux/module.h>
2. #include <linux/init.h>
3. #include <linux/workqueue.h>
5. **static struct workqueue\_struct \*queue=NULL;**
6. **static struct work\_struct   work;**
8. staticvoid work\_handler(**struct work\_struct \*data)**
9. {
10. printk(KERN\_ALERT"work handler function.\n");
11. }
13. **static int \_\_init test\_init(void)**
14. {
15. queue=create\_singlethread\_workqueue("hello world");/\*创建一个单线程的工作队列\*/
16. **if (!queue)**
17. **goto err;**
19. INIT\_WORK(&work,work\_handler);
20. schedule\_work(&work);
22. return0;
23. err:
24. **return-1;**
25. }
27. **static   void \_\_exit test\_exit(void)**
28. {
29. destroy\_workqueue(queue);
30. }
31. MODULE\_LICENSE("GPL");
32. module\_init(test\_init);
33. module\_exit(test\_exit);

6. workqueue的API  
workqueue的API自2.6.20后发生了变化

1. #include <linux/workqueue.h>
2. struct workqueue\_struct;
3. struct work\_struct;
4. struct workqueue\_struct \***create\_workqueue**(const char \*name);
5. void **destroy\_workqueue**(struct workqueue\_struct \*queue);
6. **INIT\_WORK**(\_work, \_func);
7. **INIT\_DELAYED\_WORK**(\_work, \_func);
8. int **queue\_work**(struct workqueue\_struct \*wq, struct work\_struct \*work);
9. int **queue\_delayed\_work**(struct workqueue\_struct \*wq,struct delayed\_work \*dwork, unsigned long delay);
10. int **queue\_delayed\_work\_on**(int cpu, struct workqueue\_struct \*wq,

struct delayed\_work \*dwork, unsigned long delay);

1. int **cancel\_work\_sync**(struct work\_struct \*work);
2. int **cancel\_delayed\_work\_sync**(struct delayed\_work \*dwork);
3. void **flush\_workqueue**(struct workqueue\_struct \*wq);

Workqueue编程接口

|  |  |  |
| --- | --- | --- |
| 序号 | 接口函数 | 说明 |
| 1 | create\_workqueue | 用于创建一个workqueue队列，为系统中的每个CPU都创建一个内核线程。输入参数：  @name：workqueue的名称 |
| 2 | create\_singlethread\_workqueue | 用于创建workqueue，只创建一个内核线程。输入参数：  @name：workqueue名称 |
| 3 | destroy\_workqueue | 释放workqueue队列。输入参数：  @ workqueue\_struct：需要释放的workqueue队列指针 |
| 4 | schedule\_work | 调度执行一个具体的任务，执行的任务将会被挂入Linux系统提供的workqueue——keventd\_wq输入参数：  @ work\_struct：具体任务对象指针 |
| 5 | schedule\_delayed\_work | 延迟一定时间去执行一个具体的任务，功能与schedule\_work类似，多了一个延迟时间，输入参数：  @work\_struct：具体任务对象指针  @delay：延迟时间 |
| 6 | queue\_work | 调度执行一个指定workqueue中的任务。输入参数：  @ workqueue\_struct：指定的workqueue指针  @work\_struct：具体任务对象指针 |
| 7 | queue\_delayed\_work | 延迟调度执行一个指定workqueue中的任务，功能与queue\_work类似，输入参数多了一个delay。 |

**Ps：4.5与6.7基本一致，区别在与4.5执行的工作队列是内核提供的system\_wq**

## 参考资料

<http://www.cnblogs.com/sky-heaven/p/5847519.html>

<http://bgutech.blog.163.com/blog/static/18261124320116181119889/>

<http://kernel.meizu.com/linux-workqueue.html>

# [同步/异步与阻塞/非阻塞的区别消息](http://www.cnblogs.com/Ray-chen/archive/2011/12/27/2303115.html)

同步/异步与阻塞/非阻塞的区别.  
  
这两组概念常常让人迷惑,因为它们都是涉及到IO处理,同时又有着一些相类似的地方.  
首先来解释同步和异步的概念,这两个概念与**消息的通知机制**有关.  
举个例子,比如我去银行办理业务,可能选择排队等候,也可能取一个小纸条上面有我的号码,等到排到我这一号时由柜台的人通知我轮到我去办理业务了.  
前者(排队等候)就是同步等待消息,而后者(等待别人通知)就是异步等待消息.在异步消息处理中,等待消息者(在这个例子中就是等待办理业务的人)往往注册一个回调机制,在所等待的事件被触发时由触发机制(在这里是柜台的人)通过某种机制(在这里是写在小纸条上的号码)找到等待该事件的人.  
而在实际的程序中,同步消息处理就好比简单的read/write操作,它们需要等待这两个操作成功才能返回;而异步处理机制就是类似于select/poll之类的多路复用IO操作,当所关注的消息被触发时,由消息触发机制通知触发对消息的处理.  
  
其次再来解释一下阻塞和非阻塞,这两个概念与**程序等待消息(无所谓同步或者异步)时的状态**有关.  
继续上面的那个例子,不论是排队还是使用号码等待通知,如果在这个等待的过程中,等待者除了等待消息之外不能做其它的事情,那么该机制就是阻塞的,表现在程序中,也就是该程序一直阻塞在该函数调用处不能继续往下执行.相反,有的人喜欢在银行办理这些业务的时候一边打打电话发发短信一边等待,这样的状态就是非阻塞的,因为他(等待者)没有阻塞在这个消息通知上,而是一边做自己的事情一边等待.但是需要注意了,第一种同步非阻塞形式实际上是效率低下的,想象一下你一边打着电话一边还需要抬头看到底队伍排到你了没有,如果把打电话和观察排队的位置看成是程序的两个操作的话,这个程序需要在这两种不同的行为之间来回的切换,效率可想而知是低下的;而后者,异步非阻塞形式却没有这样的问题,因为打电话是你(等待者)的事情,而通知你则是柜台(消息触发机制)的事情,程序没有在两种不同的操作中来回切换.  
  
很多人会把同步和阻塞混淆,我想是因为很多时候同步操作会以阻塞的形式表现出来,比如很多人会写阻塞的read/write操作,但是别忘了可以对fd设置O\_NONBLOCK标志位,这样就可以将同步操作变成非阻塞的了;同样的,很多人也会把异步和非阻塞混淆,因为异步操作一般都不会在真正的IO操作处被阻塞,比如如果用select函数,当select返回可读时再去read一般都不会被阻塞,就好比当你的号码排到时一般都是在你之前已经没有人了,所以你再去柜台办理业务就不会被阻塞.  
  
可见,同步/异步与阻塞/非阻塞是两组不同的概念,它们可以共存组合,也可以参见这里:  
http://www.ibm.com/developerworks/cn/linux/l-async/  
  
同步和异步:上面提到过,**同步和异步仅仅是关于所关注的消息如何通知的机制,而不是处理消息的机制**.也就是说,**同步的情况下,是由处理消息者自己去等待消息是否被触发,而异步的情况下是由触发机制来通知处理消息者**,所以在异步机制中,处理消息者和触发机制之间就需要一个连接的桥梁,在我们举的例子中这个桥梁就是小纸条上面的号码,而在select/poll等IO多路复用机制中就是fd,当消息被触发时,触发机制通过fd找到处理该fd的处理函数.  
  
请注意理解**消息通知和处理消息**这两个概念,这是理解这个问题的关键所在.还是回到上面的例子,轮到你办理业务这个就是你关注的消息,而去办理业务就是对这个消息的处理,两者是有区别的. 而在真实的IO操作时,所关注的消息就是该fd是否可读写,而对消息的处理就是对这个fd进行读写.同步/异步仅仅关注的是如何通知消息,它们对如何处理消息并不关心,好比说,银行的人仅仅通知你轮到你办理业务了,而如何办理业务他们是不知道的.  
  
而很多人之所以把同步和阻塞混淆,我想也是因为没有区分这两个概念,比如阻塞的read/write操作中,其实是把消息通知和处理消息结合在了一起,在这里所关注的消息就是fd是否可读/写,而处理消息则是对fd读/写.当我们将这个fd设置为非阻塞的时候,read/write操作就不会在等待消息通知这里阻塞,如果fd不可读/写则操作立即返回.  
  
很多人又会问了,异步操作不会是阻塞的吧?已经通知了有消息可以处理了就一定不是阻塞的了吧?  
其实**异步操作是可以被阻塞住的,只不过通常不是在处理消息时阻塞,而是在等待消息被触发时被阻塞**. 比如select函数,假如传入的最后一个timeout参数为NULL,那么如果所关注的事件没有一个被触发,程序就会一直阻塞在这个select调用处.而如果使用异步非阻塞的情况,比如aio\_\*组的操作,当我发起一个aio\_read操作时,函数会马上返回不会被阻塞,当所关注的事件被触发时会调用之前注册的回调函数进行处理,具体可以参见我上面的连接给出的那篇文章.回到上面的例子中,如果在银行等待办理业务的人采用的是异步的方式去等待消息被触发,也就是领了一张小纸条,假如在这段时间里他不能离开银行做其它的事情,那么很显然,这个人被阻塞在了这个等待的操作上面;但是呢,这个人突然发觉自己烟瘾犯了,需要出去抽根烟,于是他告诉大堂经理说,排到我这个号码的时候麻烦到外面通知我一下(注册一个回调函数),那么他就没有被阻塞在这个等待的操作上面,自然这个就是异步+非阻塞的方式了.

Linux aio是Linux下的异步读写模型。Linux 异步 I/O 是 Linux 内核中提供的一个相当新的增强。它是 2.6 版本内核的一个标准特性。对于文件的读写，即使以O\_NONBLOCK方式来打开一个文件，也会处于"阻塞"状态。因为文件时时刻刻处于可读状态。而从磁盘到内存所等待的时间是惊人的。为了充份发挥把数据从磁盘复制到内存的时间，引入了aio模型。AIO 背后的基本思想是允许进程发起很多 I/O 操作，而不用阻塞或等待任何操作完成。稍后或在接收到 I/O 操作完成的通知时，进程就可以检索 I/O 操作的结果。

## I/O 模型

在深入介绍 AIO API 之前，让我们先来探索一下 Linux 上可以使用的不同 I/O 模型。这并不是一个详尽的介绍，但是我们将试图介绍最常用的一些模型来解释它们与异步 I/O 之间的区别。图 1 给出了同步和异步模型，以及阻塞和非阻塞的模型。  
  
  
图 1. 基本 Linux I/O 模型的简单矩阵  
   
每个 I/O 模型都有自己的使用模式，它们对于特定的应用程序都有自己的优点。本节将简要对其一一进行介绍。

## 同步阻塞 I/O

最常用的一个模型是同步阻塞 I/O 模型。在这个模型中，用户空间的应用程序执行一个系统调用，这会导致应用程序阻塞。这意味着应用程序会一直阻塞，直到系统调用完成为止（数据传输完成或发生错误）。调用应用程序处于一种不再消费 CPU 而只是简单等待响应的状态，因此从处理的角度来看，这是非常有效的。

图 2 给出了传统的阻塞 I/O 模型，这也是目前应用程序中最为常用的一种模型。其行为非常容易理解，其用法对于典型的应用程序来说都非常有效。在调用 read 系统调用时，应用程序会阻塞并对内核进行上下文切换。然后会触发读操作，当响应返回时（从我们正在从中读取的设备中返回），数据就被移动到用户空间的缓冲区中。然后应用程序就会解除阻塞（read 调用返回）。

  
  
图 2. 同步阻塞 I/O 模型的典型流程  
   
从应用程序的角度来说，read 调用会延续很长时间。实际上，在内核执行读操作和其他工作时，应用程序的确会被阻塞。

## 同步非阻塞 I/O

同步阻塞 I/O 的一种效率稍低的变种是同步非阻塞 I/O。在这种模型中，设备是以非阻塞的形式打开的。这意味着 I/O 操作不会立即完成，read 操作可能会返回一个错误代码，说明这个命令不能立即满足（EAGAIN 或 EWOULDBLOCK），如图 3 所示。  
  
  
图 3. 同步非阻塞 I/O 模型的典型流程  
   
非阻塞的实现是 I/O 命令可能并不会立即满足，需要应用程序调用许多次来等待操作完成。这可能效率不高，因为在很多情况下，当内核执行这个命令时，应用程序必须要进行忙碌等待，直到数据可用为止，或者试图执行其他工作。正如图 3 所示的一样，这个方法可以引入 I/O 操作的延时，因为数据在内核中变为可用到用户调用 read 返回数据之间存在一定的间隔，这会导致整体数据吞吐量的降低。

## 异步阻塞 I/O

另外一个阻塞解决方案是带有阻塞通知的非阻塞 I/O。在这种模型中，配置的是非阻塞 I/O，然后使用阻塞 select 系统调用来确定一个 I/O 描述符何时有操作。使 select 调用非常有趣的是它可以用来为多个描述符提供通知，而不仅仅为一个描述符提供通知。对于每个提示符来说，我们可以请求这个描述符可以写数据、有读数据可用以及是否发生错误的通知。  
  
  
图 4. 异步阻塞 I/O 模型的典型流程 (select)  
   
select 调用的主要问题是它的效率不是非常高。尽管这是异步通知使用的一种方便模型，但是对于高性能的 I/O 操作来说不建议使用。

## 异步非阻塞 I/O（AIO）

最后，异步非阻塞 I/O 模型是一种处理与 I/O 重叠进行的模型。读请求会立即返回，说明 read 请求已经成功发起了。在后台完成读操作时，应用程序然后会执行其他处理操作。当 read 的响应到达时，就会产生一个信号或执行一个基于线程的回调函数来完成这次 I/O 处理过程。  
  
  
图 5. 异步非阻塞 I/O 模型的典型流程  
 

在一个进程中为了执行多个 I/O 请求而对计算操作和 I/O 处理进行重叠处理的能力利用了处理速度与 I/O 速度之间的差异。当一个或多个 I/O 请求挂起时，CPU 可以执行其他任务；或者更为常见的是，在发起其他 I/O 的同时对已经完成的 I/O 进行操作。

从前面 I/O 模型的分类中，我们可以看出 AIO 的动机。这种阻塞模型需要在 I/O 操作开始时阻塞应用程序。这意味着不可能同时重叠进行处理和 I/O 操作。同步非阻塞模型允许处理和 I/O 操作重叠进行，但是这需要应用程序根据重现的规则来检查 I/O 操作的状态。这样就剩下异步非阻塞 I/O 了，它允许处理和 I/O 操作重叠进行，包括 I/O 操作完成的通知。除了需要阻塞之外，select 函数所提供的功能（异步阻塞 I/O）与 AIO 类似。不过，它是对通知事件进行阻塞，而不是对 I/O 调用进行阻塞。

## 参考资料

<http://www.cnblogs.com/Ray-chen/archive/2011/12/27/2303115.html>

http://www.ibm.com/developerworks/cn/linux/l-async/