linux 驱动调试

本文主要内容是如何使用两台机器远程调试 Linux 内核,基于 Linux 2.6。

一　补丁

这里使用 quilt 工具(http://savannah.nongnu.org/projects/quilt)来管理 patch。

```
$ tar jxf linux-<base_kernel_version>.tar.bz2
$ cp -a kgdb-2 linux-<base_kernel_version>/patches
$ cd linux-<base_kernel_version>
$ quilt push -a
```

如果不想使用 quilt，则必须手动将所有 patch 打进内核：

```
$ tar jxf linux-<base_kernel_version>.tar.bz2
$ cd linux-<base_kernel_version>
$ for p in $(grep patch ../kgdb-2/series);do patch -p1 -si ../kgdb-2/$p;done
```

二 编译

内核编译：在开发机上准备好内核源码及对应的 KGDB patch 文件（使用的 2.6.18－92.el5）

将下列选择选编入内核

```
Device Drivers --->
    Character devices --->
        Serial drivers --->
            <*> 8250/16550 and compatible serial support
            [*] Console on 8250/16550 and compatible serial port

Kernel hacking --->
    [*] KGDB: kernel debugging with remote gdb
    [*] KGDB: Console messages through gdb
        Method for KGDB communication (KGDB: On generic serial port (8250)) --->
            (X) KGDB: On generic serial port (8250)
    [*] Simple selection of KGDB serial port
    (115200) Debug serial port baud rate
    (0) Serial port number for KGDB
```

make modules

make modules_install （把编译后的模块文件安装到当前系统的/lib/moudles/.....下)

在源码文件存放的一级目录下生成 System.map 文件，在 arch/i386/boot 下生成 bzImage,把这两个文件拷贝到/boot 下并重命名：

cp System.map /boot/System.map-2.6.18-92

cp bzImage /boot/vmlinuz-2.6.18-92

创建 连接： ln -s System.map-2.6.18-92 System.map

ln -s vmlinuz-2.6.18-92 vmlinuz

制作 initrd 文件：mkinitrd initrd-2.6.18-92 ****(****表示 make modules_install 时在/lib/modules 下新创建的文件夹名)

三 启动

将 vmlinuz-2.6.18-92 和 initrd-26.18-92 部署到测试机上,并修改启动项以 KGDB 方式启动.

如果要使用串口来调试内核，那么就在 grub 中，内核的启动参数上加上 kgdbwait，它将会在系统启动内核的时候停下来等待调试。如果要改变串 口的参数，使用 kgdb8250 驱动，那内核启动参数为 kgdb8250=0,115200，0 代表使用串口 0（/dev/ttyS0），波特率是 115200

例 1：使用串口 ttyS0，波特率为 115200 的参数是：

kgdb8250=0,115200 kgdbwait

例 2：要使 KGDB 在启动的时候停下来等待连接，参数是：

kgdbwait

系统内核在启动过程中，有可能没有输出信息，过一段时间就会出现 Login 提示符，这可能视编译内核时的选项所决定。

四 调试

4.1 调试方法

主要尝试过两种方法：打印或单步调试

1.打印：

printk 分很多级别信息，功能类似于 c 语言的 printf, 一般来说信息打印到/var/log/messages，可通过 cat 命令或 tail 命令查看

大多数问题都可以通过 printk 来解决，缺点在于不够直感

2.调试工具：

GDB ,KDB,KGDB 都需要编译 DEBUG 版本内核。KDB 单机汇编级调试,需要单独下载 kernel 对应的 patch，KGDB 在 2.6.*后就已缺省放在内核源码里了，其他的需要单独下载 PATCH，反正我的 2.6.18 内核里没有(在 kernel.org 中,people/ark 下应该能找到 2.6.18 的 patch,注意打 patch 的顺序） 查看是否有 KGDB 的方法是：源码路径下 make menuconfig 后能看到 KGDB 这一项。

3.硬件连接性测试

KGDB 需要两台机器配合，一个开发机，一个测试机，两台机器通过串口线连接

在开发机上 执行 stty -ispeed 115200 -ospeed 115200 -F /dev/ttyS0

在测试机上 执行 stty -ispeed 115200 -ospeed 115200 -F /dev/ttyS0

在开发机上 执行 cat /dev/ttyS0

在测试机上 执行 echo "12345" < /dev/ttyS0

如果在开发机上能看到 12345 表示两台机器连通

4.2 内核调试

被调试内核的机器叫 target machine，使用某一台机器去连接 target machine 的机器叫 development machine。当在 development machine 上调试 target machine 机器上的内核时，在 development machine 上执行：

```
$ cd linux-<base_kernel_version>
    $ gdb ./vmlinux
    (gdb) set remotebaud 115200
    (gdb) target remote /dev/ttyS0
```

如果是通过网络调试内核，那么内核启动参数为：

kgdboe=@10.0.0.6/,@10.0.0.3/ (kgdboe=@LOCAL-IP/,@REMOTE-IP/)

调试命令是：

```
$ gdb ./vmlinux
    (gdb) target remote udp:HOSTNAME:6443
```

4.3 模块调试

使用 gdbmod-2.4 这个二进制的命令来调试内核模块。它是基于带有 KGDB 模块调试补丁的 gdb(6.4)。可以从这里下载：http://kgdb.linsyssoft.com/downloads/gdbmod-2.4.bz2，源代码可以从这里下载：http://kgdb.linsyssoft.com/downloads/gdb-6.4-kgdb-2.4.tar.bz2。

调试命令为：

```
$ gdbmod-2.4 ./vmlinux
```

4.4 通过网络调试内核

如果通过网络调试内核，则 NAPI 特性必须禁止。NAPI 是用于在 1G 和 10G 以太网卡上快速通讯设计的。当一个包到达时，它能开启网卡的以太网驱动模式 (ethernet driven mode) 和切换到查询模式(switch to polling mode)。查询模式是尽快的关闭了到达包的暂停(The polling mode is turned off as soon as incoming packets take a pause.)。KGDB 不能在这种情况下工作，即使是 100M 网卡，NAPI 也要关闭。