kgdb最早什么时候可以开始debug kernel？

```
    kgdbwait    [KGDB] Stop kernel execution and enter the
                kernel debugger at the earliest opportunity.
```

用户在kernel的启动参数上添加"kgdbwait"来trigger kgdb。

```
static int __init opt_kgdb_wait(char *str)
{
    kgdb_break_asap = 1;

    kdb_init(KDB_INIT_EARLY);
    if (kgdb_io_module_registered)
        kgdb_initial_breakpoint();

    return 0;
}

early_param("kgdbwait", opt_kgdb_wait);
```

enable kgdb首先kgdb_io_module_registered is true

in kgdb_register_callbacks()

```
    if (!kgdb_io_module_registered) {
        kgdb_io_module_registered = 1;
```

kgdb_register_io_module() –> kgdb_register_callbacks()

即是否由module invoke kgdb_register_io_module().

目前只有 2 个module注册了kgdb的"io module"

1. drivers/tty/serial/kgdboc.c
2. drivers/usb/early/ehci-dbgp.c

对serial而言

```
#ifdef CONFIG_KGDB_SERIAL_CONSOLE
/* This is only available if kgdboc is a built in for early debugging */
static int __init kgdboc_early_init(char *opt)
{
    /* save the first character of the config string because the
     * init routine can destroy it.
     */
    char save_ch;

    kgdboc_option_setup(opt);
    save_ch = config[0];
    init_kgdboc();
    config[0] = save_ch;
    return 0;
}

early_param("ekgdboc", kgdboc_early_init);
#endif /* CONFIG_KGDB_SERIAL_CONSOLE */
```

即使用串口调试kernel，满足 3 个条件

1. enable CONFIG_KGDB_SERIAL_CONSOLE
2. kernel启动参数添加"ekgdboc" (必须在"kgdbwait"参数之前)
3. kernel启动参数添加"kgdbwait"

使用usb(ehci host controller)来调试kernel

```
    kgdbdbgp=   [KGDB,HW] kgdb over EHCI usb debug port.
            Format: <Controller#>[,poll interval]
            The controller # is the number of the ehci usb debug
            port as it is probed via PCI.  The poll interval is
            optional and is the number seconds in between
            each poll cycle to the debug port in case you need
            the functionality for interrupting the kernel with
            gdb or control-c on the dbgp connection.  When
            not using this parameter you use sysrq-g to break into
            the kernel debugger.
```

```
static int kgdbdbgp_wait_time;

static int __init kgdbdbgp_parse_config(char *str)
{
    char *ptr;

    if (!ehci_debug) {
        if (early_dbgp_init(str))
            return -1;
    }
    ptr = strchr(str, ',');
    if (ptr) {
        ptr++;
        kgdbdbgp_wait_time = simple_strtoul(ptr, &ptr, 10);
    }
    kgdb_register_io_module(&kgdbdbgp_io_ops);
    kgdbdbgp_io_ops.is_console = early_dbgp_console.index != -1;

    return 0;
}
early_param("kgdbdbgp", kgdbdbgp_parse_config);
```

kgdb只有在kernel处理完启动参数以后才会有效。

in init/main.c

```
start_kernel(void)
{

    ......

    parse_early_param();

    ......

}
```

parse_early_param()之前的kernel code，kgdb是无法调试的，只有JTAG debugger可以。