三环与零环IO通讯

零环

1定义控制码

2 定义设备扩展

3 创建设备对象（定义一个设备对象，创建设备名称（RtlInitUnicodeString））

4 设置通讯方式（缓冲区） pDevObj->Flags |= DO_DIRECT_IO

5 获取设备扩展并填充

6 创建符号链接

7定义一般派遣函数

8定义DeviceControl派遣函数

（1）获取irp堆栈，PIO_STACK_LOCATION stack，利用stack点出想要的参数

（2）得到MDL在内核下的映射 MmGetSystemAddressForMdlSafe（pIrp->MdlAddress, NormalPagePriority）

（3）其中根据控制码执行对应流程

（4）将通讯内容放到MDL内，设置pIrp字节，完成状态等

9 设置派遣函数

DriverObject->MajorFunction[IRP_MJ_DEVICE_CONTROL] = DeviceControl派遣函数

三环

1. 定义控制码
2. 打开符号链接
3. 获取DeviceControl的缓冲区