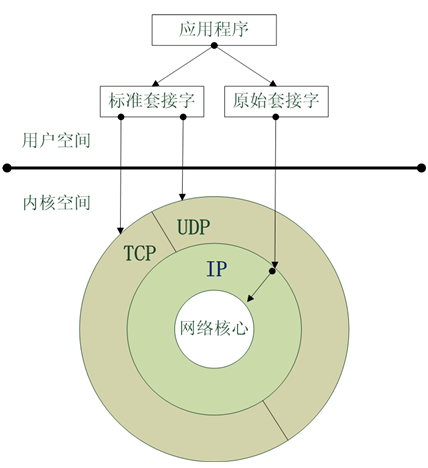
**一、知识回顾：**

通常情况下程序员接所接触到的套接字（Socket）为两类：

1. 流式套接字（SOCK\_STREAM）：一种面向连接的 Socket

（2）数据报式套接字（SOCK\_DGRAM）：一种无连接的 Socket

**二、原始套接字概述**

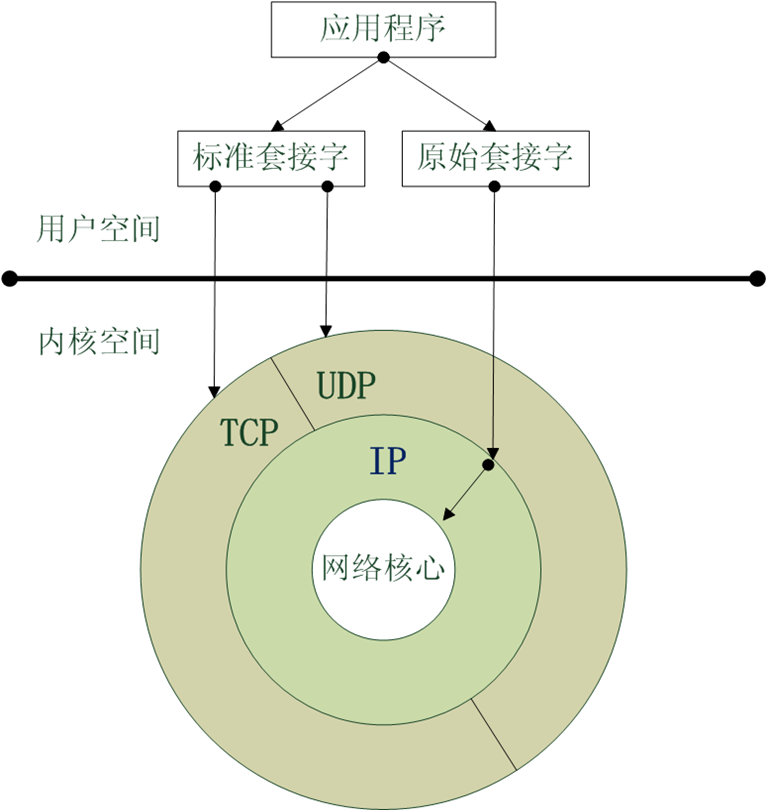


原始套接字广泛应用于高级网络编程，也是一种广泛的黑客手段。著名的网络sniffer（一种基于被动侦听原理的网络分析方式）、拒绝服务攻击（DOS）、IP 欺骗等都可以通过原始套接字实现。

原始套接字（SOCK\_RAW）可以用来自行组装数据包，可以接收本机网卡上所有的数据帧（数据包），对于监听网络流量和分析网络数据很有作用。

原始套接字是基于 IP 数据包的编程（SOCK\_PACKET 是基于数据链路层的编程）。另外，必须在管理员权限下才能使用原始套接字。

原始套接字（SOCK\_RAW）与标准套接字（SOCK\_STREAM、SOCK\_DGRAM）的区别在于原始套接字直接置“根”于操作系统网络核心（Network Core），而  SOCK\_STREAM、SOCK\_DGRAM 则“悬浮”于 TCP 和 UDP 协议的外围。



流式套接字只能收发 TCP 协议的数据，数据报套接字只能收发 UDP 协议的数据，原始套接字可以收发内核没有处理的数据包。