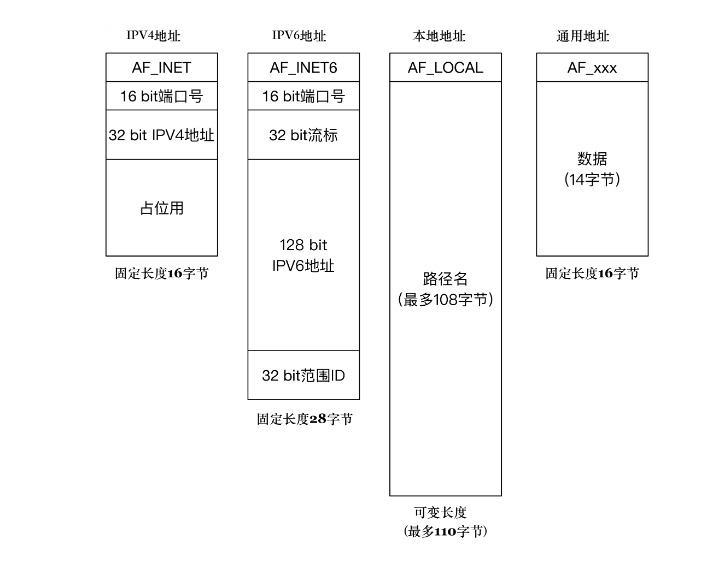
**本地套接字**

1、本地套接字用来本地进程间通信

2、效率比TCP/UDP套接字高不少

常用命令

**netstat -alepn**

**netstat Socket -x -alepn （只对UNIX）套接字进行筛选**

**lsof /var/run/docker.sock （找出谁打开了这个文件）**

**lsof -i :8080 查看端口**

**tcpdump 抓包工具：**

**1、tcpdump -i eth0 指定网卡**

**2、tcpdump src host hostname 指定来源**

**3、tcpdump 'tcp and port 80 and src host 192.168.1.25' 抓的包是TCP，端口是80,IP地址来自 192.168.1.25**

**4、tcpdump 'tcp and port 80 and tcp[13:1]&2 != 0' tcp[13:1]表示打是TCP**

**头部开始偏移13字节，如果值为2,说明设置了SYN分节，当然可以设置成其他的分节。**