

## 第 7 章 网络层协议

---



无论是处理延迟问题，还是甄别存在错误的应用，抑或是对安全威胁进行聚焦检查以发现异常流量，你都必须首先了解正常流量。在下面的几章中，我们按照 OSI 模型由底层到高层进行介绍，你将会学到正常网络流量在数据包级别是如何工作的。在每个协议的相关部分，都会至少有一个捕获文件供你下载，并可以让你直接上手分析。

在这一章节里，我们会着重关注网络通信的「搬瓦工」—网络层的协议：ARP、IPv4、IPv6、ICMP 和 ICMP6。

接下来的 3 个章节可能是全书的重点。如果你跳过了它们，就好比在感恩节晚餐上不使用烤箱一样。即使你已经对每个协议如何工作有了一定的了解，把这几章快速略读一遍也是对数据包结构进行复习的过程。