第 10 章　基础的现实世界场景

从本章开始，我们将深入到数据包分析的内涵，使用 Wireshark 分析现实世界中的网络问题。在本章第一部分，我们将分析网络工程师、服务台技术人员、应用开发者在日常工作中会遇到的场景——全都来自于我与同事们的实际经验。我们将使用 Wireshark，查看来自 Twitter、Facebook 和 ESPN 的流量，观察这些常用的服务是如何工作的。

本章第二部分将介绍一系列实际问题。针对每一个具体问题，我描述了它们的情况，并把当时可用的信息提供给分析者。在这个基础上，转到分析数据包的过程、描述捕获特定数据包的方法，以及分析过程的每个步骤。分析完成后，我将提供一个完整的问题解决方案，或是指出可能的解决方法，并总结从中汲取的经验教训。

自始至终，要记住分析是一个非常动态的过程，并且，我用来分析每一个场景的方法可能跟你用的不一样。每个人可以用不同的方法来分析。但最重要的是，分析的最终结果能够解决一个问题，或使你获得学习经验。另外，本章讨论的大部分问题，即使不用数据包嗅探器，也可以解决。当我初次学习分析数据包时，发现反常规地使用数据包分析技术来查看典型问题有很多好处，这也是我给你介绍这些场景的原因。