

1.4 小结

章 监听网络线路

2.1 混杂模式

2.2 在集线器连接网络中嗅探

2.3 在交换式网络中进行嗅探

2.3.1 端口镜像

2.3.2 集线器输出

2.3.3 使用网络分流器

2.3.4 ARP 缓存污染

2.4 在路由网络环境中进行嗅探

2.5 部署嗅探器的实践指南

章 Wireshark 入门

3.1 Wireshark 简史

3.2 Wireshark 的优点

3.3 安装 Wireshark

3.3.1 在微软 Windows 系统…

3.3.2 在 Linux 系统中安装

3.3.3 在 Mac OS X 系统中安装

3.4 Wireshark 初步入门

3.4.1 第一次捕获数据包

3.4.2 Wireshark 主窗口

3.4.3 Wireshark 首选项

3.4.4 数据包彩色高亮

3.4.5 配置文件

3.1 Wireshark 简史

Wireshark 的历史相当久远丰富，其最初的版本叫作 Ethereal，由毕业于密苏里大学堪萨斯城分校计算机科学专业的 Gerald Combs 出于项目需而开发，并于 1998 年以 GNU Public Licence（GPL）开源许可证发布。

在 Ethereal 发布八年之后，Combs 辞职并另谋高就，但是在那个时他的雇主公司掌握着 Ethereal 的商标权，而 Combs 也没能和其雇主就取 Ethereal 商标达成协议。于是 Combs 和整个开发团队在 2006 年年中的时候将这个项目重新命名为 Wireshark。

Wireshark 随后迅速地取得了大众的青睐，而其合作开发团队也壮大 500 人以上，然而 Ethereal 项目却再没有前进过一步。