用户故事 | 王未：网络排查能力是一名合格运维工程师的必备技能

2022-04-04 王未

《网络排查案例课》 课程介绍 >

讲述：王惠

时长 08:34 大小 7.86M

你好，我是王未，目前在上海一家互联网公司从事运维工作，有 7 年左右的工作经验。

运维是一项非常杂乱、技术支持性要求比较高的工作，分类也非常多，比如有应用运维、网络运维、系统运维、安全运维、监控运维、运维开发等等。就以应用运维为例，我们需要对各个运维中间件、监控系统了解精通，同时也要对排查故障做到得心应手。

那么，**作为一个运维工程师，维护系统稳定是天职，而这就需要我们能够在出现问题的时候，迅速解决故障，把损失降低到最小。**至于如何排障，运维的基本功——网络排查，就是一名合格运维工程师的必备技能了。但往往，很多人在这方面掌握得并不是很好。

为什么要学习这门课程？

日常排查工作中遇到的问题，我们大多是通过日志给出来的报错，来顺藤摸瓜式地排查定位，可一旦遇到网络问题，我们可能就找不到方向了。网络世界太复杂，七层协议，每一层都有很多概念和原理需要理解精通，就比如：

网络层，有 TTL、RTT、MTU、hops、Router 等。

传输层，包括 TCP Sequence Number、AckNumber、MSS、Receive Window、Congestion Window，latency、DupAck、SACK、Retransmission、Packet loss 等。

应用层，有 HTTP 协议的 header、body 等。

而除了这些之外，我们还需要结合 Linux 的操作性，来设置合理的 TCP 层的内核参数等等，这样就使得我们对 TCP 协议的理解和掌握非常混乱，很难系统性地去学习。

我在刚入行时看过一本书，是机械工业出版社的《TCP/IP 详解 卷 1：协议》，来来回回看了几次，书里的理论知识比较多，但当时道行比较浅，工作实践比较少，另外也没有结合实战，所以理解起来比较费劲。

可以说，网络排查一直是我一知半解的领域，每次遇到类似的问题，我都很难灵活地去排查问题，对 Wireshark 的使用也非常不熟悉，那些数据包抓出来后在 Wireshark 里的展示，对我来说基本上就是“天书”了。

所以，胜辉老师的《网络排查案例课》在极客时间推出后，一下子就吸引了我，终于有个全面讲解 TCP/IP 协议、使用 Wireshark 的课程上线了。

我们知道，TCP/IP 协议是运维知识体系的基石，就像房子的地基一样，必须要牢固。所以基于这个普遍认知，也让我对自己的网络排查能力有了一定的要求。就我个人而言，我想要通过这门课程，达成以下三个学习目标：

学习并理解二、三、四层的工作原理；

系统地实战学习故障排查方法，积累经验；

拓展自己的技术思维。

学习课程的心得体会

因为之前我对 TCP/IP 协议并不熟悉，没有全面、系统性地学习过，所以在解决问题方面并不灵通，对各种概念也是一知半解的。不过，胜辉老师的运维经验非常丰富，并且老师生动的讲解方式，也非常易于我们理解。随着课程的推进和学习，也让我对之前工作中遇到的一些网络排查问题的思路渐渐清晰了。

举个例子，Nginx 499 的问题我之前在工作中也遇到过。我在公有云工作的时候，在某个区域的客户请求有一定比例的 499，当时因为只是极个别的客户，也没去抓包，觉得反正是客户主动断开的，大概率就是网络不稳定导致客户端超时断开了，而且客户没有报障，也就不管了，最起码不是我们服务端的问题。不过，具体为什么会断开、为什么 reset，其实并不了解。

现在想想，之前的工作态度其实会比较草率，没有做到刨根问底地去分析、解决问题，或许我当时深入去研究一下，早就能够提升自己的网络排查能力了。HTTP 400 也是一样，也只是知道客户端请求格式不正确，具体 HTTP 的请求格式也并没有了然于胸，还只是非常肤浅地理解一些概念而已，知其然而不知其所以然。

还有第 19 讲的案例中，关于 TLS 握手失败的问题，我在实际工作中也遇到过，但是很难解决。当时是不同服务器上的 curl 客户端，有些 TLS 失败，有些成功。那时候，我们的处理是将 curl 升级到最新版本才解决，但最后也并不了解问题根因在哪、为什么这样做就 OK 了，直到学习了课程才明白，原来这种故障大概率是因为 Cipher Suite 问题导致的。

我的高效学习方法

我想，能来这里学习的人，大多数都是希望提升自己的小伙伴，我也一样。所以这里，我也想分享一下我的学习方法，希望能给你带来一些参考。其实这些方法也很简单。

温故而知新

我一般会在课程更新的第一时间，先打开电脑学习一遍，用正常的倍速去听讲，遇到没理解的地方暂停，重复学习，同时拿着抓包文件对着 Wireshark 同步操作。

然后，我也会利用上班时的地铁通勤时间，或者晚上睡觉前的时间，用手机 App 学习。用手机主要是为了复习，因为这个时间很难高度集中注意力，比较适合复习刚刚学完的知识，尤其是像这种碎片化的知识，需要不停地复习加强记忆。

做好笔记

通过整理笔记，能帮我们做到高度归纳、快速梳理知识点，也非常有利于我们后期温习。

其实，做笔记这个方法对于我们在几个月甚至更长的时间后去复习内容非常有帮助，这样我们一般就不需要重新学习一次课程了。

重视思考题，以及留言区其他小伙伴的提问

毕竟，带着问题去学习会事半功倍。而且，留言也是输出的一种，而输出是学习的最佳路径。

在学到一些概念的时候，自己其实会有不清楚的地方，或者是一些看似自己已经明白的概念，如果用自己的话再说一次，也会发现其中的很多细节我其实根本没搞懂，我要不停地查资料，把不懂的地方搞明白，那么这时候的留言，当然就很有存在价值了，这样在充分搞清楚这些概念的前提下，再去学习课程也会更容易理解。理解，才能更好地掌握知识点。

另外，通过留言，我们还可以根据其他小伙伴的提问以及交流讨论，再次巩固所学知识，让不同的思想碰撞，从而更接近学习的本质。

总结

目前课程已经基本接近尾声，我也想再回过头来，总结一下自己的学习过程。

首先，很明显，整个课程学起来还是比较轻松的，因为之前对 TCP/IP 的了解比较模糊，而通过学习课程，我的网络排查能力有了很大的提升，以后遇到抓包问题不会怵了，基本上能够熟练使用 Wireshark 去分析了。

其次，课程里非常全面地介绍了各种情况下的网络问题，在后面的工作过程中再遇到网络问题，我想也不会超出课程里的案例情况。并且，老师介绍的各种排查方法和抓包技巧，也能让我在工作中及时、灵活地排障。

最后，我想说的是，无论是学习网络排查还是其他的运维知识，我们都必须要把基本功夯实好，**多学多练**才能提升自己的能力，坚持久了自然而然就水到渠成了，我们的技术能力

就会像武侠的内功一样深不可测。

上一篇 用户故事 | 小S：学习是人生路上生生不息的活泉

下一篇 25 | 抓包分析的回顾、拾遗，和提高

精选留言

写留言

由作者筛选后的优质留言将会公开显示，欢迎踊跃留言。