路由劫持案例分析思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E8_B7_AF_E7_94_B1_E5_8A_AB_E6_c101_644164.htm 与路由相关的故障，往往会造成大片或者全局性的网络瘫痪，管理员们对此也是避之不及的。笔者做网络支持多年，接触过太多这样的案例。下面和大家分享一个路由劫持案例，进而进行拓展谈谈类似路由故障的排错思路和技巧。 一、案例再现路由器被劫持了! 1、故障描述 某公司的内网是在三层交换处划分的VLAN，最后通过路由器与远程连接，网内有近二百台主机。前段时间网络出现了这样一个故障：公司网络网速缓慢，且出现延迟现象，登录服务器很久都没有响应，时常提示超时。当初判断是网络中有异常数据流，因为网络中的交换机和路由器灯长明、狂闪。 2、定位中毒客户端 最初以为公司网络部署不严密或者在网络中存在ARP欺骗，ARP风暴吞噬了网络带宽，影响了网络速度。鉴于接入网络机器太多，手动全部查找很麻烦，决定借助分析软件来查。将安装软件的笔记本接入到中心交换机端口，经过一个小时，根据软件得到的数据分析，感觉是感染了蠕虫病毒，是些病毒在网络中感染了其他机器，产生了数据风暴，使网络性能下降。 根据软件“ 诊断视图 ”中显示的连接尝试，发现有一台IP为172.16.56.7的主机不正常。进行定位分析后，判断此主机可能感染了蠕虫病毒，且该病毒正在试图感染其他主机。病毒自动通过网络与其他主机的TCP 445端口建立连接，试图感染其他主机，严重消耗了网络资源，造成网络性能下降，严重时会使整个网络瘫痪。于是对此主机进行了隔离，病毒查杀

后，重新接入网络。 3、故障重现 本以为问题得到解决，可第二天又出现了以前的情况，只是没有以前大面积长时间断网或停滞，还是有规律地发生网络拥堵，网速缓慢。再次用分析软件进行抓包分析，通过分析发现大流量的数据是从外网通过路由器转发到一个MAC地址为00-A0-D1-E5-17-05的主机上，这个数据占了外网流入量的80%以上。通过档案资料查到了此主机为一台服务器，主要用来实现内部文件共享的文件服务器。通过对此服务器进行检查，结果发现此服务器配置成了代理服务器，怀疑被人入侵了。 那么为什么配成代理服务器呢?是不是路由器也被入侵了?登录路由器，发现路由器设置了端口转发，许多端口转发都转到了这台文件服务器上。现在原因已经很清楚了，有人入侵了此文件服务器，并将它设置成了代理服务器，然后控制了路由器，在路由器上设置了端口转发，把外网数据转到服务器上，最后在自己的机器上设置代理上网，通过P2P软件大量下载造成网络拥堵。因为公司规定除个别机器可以上网外，绝大部分机器不能接入 Internet网，所以通过路由器进行了限制。由于公司路由器采用的是默认用户名，只是简单地设置了密码，这样路由器就被控制了。 4、故障彻底解决 运行网络分析软件，首先取消了文件服务器的文件共享，设置网络监控软件，很快获得了大量数据。根据几个可疑MAC及所存的档案，很快找到了相应的主机。然后恢复文件服务器共享功能，取消代理服务器设置，重新设置路由器密码。至此问题彻底解决。 二、深入拓展如何解救被劫持的路由? 也许，上面的案例比较特殊。其实，网络运维中类似的案例还是比较多的，其原因也是非常复杂的。下面谈谈造成类似故障的排错思路和排错流程

。1、排错思路 (1).上层交换机或者电信核心交换机出现了故障。如果是这种原因，公司网络内部仍然是畅通的，路由器和交换机设备处于工作正常状态。这种情况也是时有发生的，比如笔者本地的电信路由就曾因遭到攻击而瘫痪。对此，公司管理员是无能为力的，只能等待电信部门尽快恢复了。(2).公司内部用户在使用Emule、BT等下载软件在下载资料。员工使用Emule和BT等下载软件下载资料时，会占用公司大量带宽，公司网络本身就有一定负载，因此极有可能造成其他用户不能访问网络，打开网页出现超时等现象。如果是因为这个原因，则可以在入口处通过技术手段禁用这些下载软件即可。 (3).路由器以及交换机在长期运行后，支持软件对内存的消耗超过了设备本身的临界值而超负荷运行，也会导致网络速度变慢。出现这种现象，分别重启交换机、路由器以及防火墙等设备即可。 (4).带宽满足不了公司要求，建议增加公司带宽。网速与公司所申请的带宽、电路类型、局域网设备性能及参数设置、网络内电脑的数量等诸多因素有关系，而在公司接入电路后，只能是去测试实际带宽是否能够达到所申请的带宽。这里提供一个简单的带宽测试方法：通过在网上下载一些比较大的文件，观察下载的流量是否能达到或接近所申请的速率(为申请速率的75%以上)。 我们可以在接入电路上接一台PC，以便测试的结果更加接近实际效果。下载越大的文件所需的时间也就越长，所反映出来的效果就越准确。下载所显示的速率单位一般为字节，而电路申请的速率为比特，所以在确认测试结果的时候要注意单位的换算。若下载所显示的速率与申请的带宽有较大差距，则有可能是电脑的性能因素造成的，也有可能是接入电路的因素造

成的，此时可向电信公司申告故障。若测试正常，而在局域网内下载又非常慢，那就应该查一下局域网内的配置了。局域网内电脑的数量应与所需申请的带宽成正比。 2、排错流程 针对上述故障点，建议采取以下流程来解决故障问题。 (1).检查网络连通情况。先对公司内部网络进行联通测试，主要对网关、路由器及交换机进行联通测试。然后对上层交换机和外网IP地址进行测试，如果一切正常则转入下一步操作，否则进行设备检查。 (2).如果公司网络出口处使用了防火墙或者监控软件，可以通过防火墙或者监控软件来查看网络连接。网络出现速度缓慢，一般是因为某台或者数台计算机大量占用带宽造成，也有可能是由于网络风暴造成的。防火墙管理软件可以很方便地发现大量发包的计算机IP以及端口等信息。找到这些计算机后，切断故障源头，再查看网络使用情况，如果正常，则解决故障源头计算机则可。 (3).采取补救措施。对存在问题的计算机进行杀毒等安全检查，确保计算机运行正常后才再接入网络。有条件的话，可以对Emule、BT等软件做分时下载限制或者禁用。 最后，百考试题希望本文提供的案例以及排错技巧、思路对大家有所帮助。 编辑特别推荐: 各个方向CCIE认证投资回报分析 思科证书的意义：技术经验的证明 我是主考官：给一位应届毕业生的回信 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com