网络技术:DNS故障引发子网流量异常计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/555/2021_2022__E7_BD_91_E7_BB_9C_E6_8A_80_E6_c98_555799.htm 这是笔者最近亲历的一起网络故障，故障比较典型，排错思路比较可取。我把这个过程写下来和大家分享，希望能够帮助到你。 1、症状描述 客户来电报告中心主网络则基本正常，而一个子网突然变慢。这是本地铁通网络服务公司，该公司为普通用户提供Web服务和Internet接入服务。前几天其服务的一个片区的用户反映网络速度很慢，发Email也需要等待超过60秒以上的时间才能联通。这个片区被划分为一个子网，从主机房的网管系统上观察发现除了该片区(子网)路由器流量很高以外(测试为97%)，中心网络的路由器与其它子网的交互流量均为40%以下。此外，没有其它特别现象。 2、诊断过程 铁通的维护人员自行进行了网络排错可惜没有找到故障所在，由于不能断开网络停止用户服务来进行检查，于是求助于我们，本人被派出诊。应该说，从症状上看这个故障比较简单，只要查出子网的路由流量来源就可以很快确定故障方向，进一步则立即可以查出流量源。 从网络拓扑图上看，故障子网与中心网络为E1链路。故障子网下面有一个营业厅，一般只与中心网络交互一些业务数据应该不会有太大的流量。此外，该子网下的Web服务器数量为45台，中心的网管系统报告97%的流量肯定是过高的。 笔者考虑只有一种情况可以比较多地占用E1通道的有效流量，那就是故障子网下的网站与中心网络的网站或服务器之间有多媒体文档的传输或者下载业务才会造成这种情况。不过询问管理人员得知中心网络并不提供

诸如多媒体视频的播放和下载服务，那只能借助工具进行检测了。 由于故障网络规模比较小，中心网络的网管系统只支持到路由器一级的管理，交换机和服务器等采用的是廉价的桌面交换机，所以无法支持网络管理。将网络测试仪接入交换机进行测试，启动便携网管功能，可以看到路由器的流量和网管系统观测的到的流量是相同的，均为97%左右。 查看中心网络处与此相连的路由器流量，也是997%左右，这说明路由器通道链路性能基本正常。不过这样高的通道流量必然导致路由器拥塞和丢包，所以从流量的角度看又是不正常的。现在需要了解的是，如此高的路由流量是从哪里来的，以及数据包到达路由器以后的去向等。这样就可以很快定位导致如此之高的通道流量的数据源和拥塞源。 将网络流量分析仪接入网络的路由器通道进行监测和分析，结果显示95%流量流向了业务数据服务器，且多数为HTTP和Email方面应用。其中，Internet访问流量占88%，本地流量占7%。查看流量分析仪指示的流量来源分布图，没有发现集中的流量应用，IP地址分布比较均衡，最高的流量只占0.5%。这些数据表明，用户的应用比例均衡，故障原因应该在应用过程中而不是某个集中的用户“ 轰击 ”比如黑客等。也就是说，应该是应用的过程和通道出了问题。其原因是这些流量按通道设计不应该到达营业厅网络的业务服务器，而是应该直接从中心网络的Internet主路由器进入互联网。那么，这些流量是如何被引导到营业厅服务器方向上来的呢? 下面我们进行进一步的分析，大家知道IP数据包在传输过程中会在路由器中作地址解析(ARP)，或是在本地DNS中进行域名分析。如果这些分析路径出问题，则IP数据包的传输和交换就会出问题。根据流

量分析仪的指示，笔者任意选择了10个IP地址做路由追踪测试，用网络测试仪追踪的结果是，他们都要经过一个DNS服务器。而模仿营业厅网络成员分别对已知的本地和外地用户做ICMP监测和路由追踪测试，结果发现ICMP监测中重定向数据包占82%，目标不可达数据包数量占13%。这表明，只有约2%的用户能一次性出入正常路由到达目标站点，其余95%的IP数据包都要经过路由竞争或重新发送才能有部分机会到达目的地。 由此，可以重点检查主路由器的路由表和DNS的转换表。由于多数Internet访问流量被引导到了营业厅业务服务器，所以可以重点检查DNS服务器。用网络测试仪对DNS服务器做查询，观察查询结果，发现DNS转换表有相当大的比例指向了营业厅子网中的业务服务器。笔者怀疑是DNS服务器出了问题! 于是通知中心网络的网管人员将DNS服务器重新启动并快速设置一次，稍后网络管理人员报告网络业务恢复正常。用网络测试仪的Internet工具包查询DNS服务器，可以看到指向营业厅业务服务器的数据已经全部消失，这表明网络已经完全恢复了正常工作。但好景不长，约3分钟后，故障重新出现，仍有97%的通道流量被指向了子网。 由于DNS服务器只设置了一台，没有备份或备用服务器，于是不得不立即来到中心网络机房，对DNS服务器及其周围设备进行检查。测试服务器网卡和与路由器的电缆正常。为了不中断服务，笔者让网管人员在另一台备用服务器上临时安装设置了DNS服务器。经过短暂的业务中断后，更换上的新DNS服务器开始投入适用。只见子网路由器的流量立刻降低到了1.5%。经过30分钟的稳定工作后，所有用户均恢复到正常工作状态，故障消除。 3、故障原因 大家知道，DNS服务器

用于将用户域名转换为IP地址，一般来说不会出现什么问题。但由于某些原因，造成了类似本例的中转换地址统统指向了营业厅子网的业务服务器。业务服务器不具备路由处理功能，对发送来的IP数据包要么拒收并置之不理，要么返回目标不可达或需要重定向的报告数据包。这就是我们在ICMP监测时经常观察到的现象。 本地铁通的用户数量并不多，而且与上级网络的链路带宽为155M的ATM链路，大有富余，所以上Internet的用户其上网速度主要受子网带宽的影响。因为许多的用户要经过拥挤的无效E1链路，造成路由重定向和严重的时延。大量的IP数据包拥向只有2M带宽的子网路由器，流量达到了97%，造成子网工作速度突然变慢，路由器出现严重拥塞等现象。 4、两点建议 (1).DNS服务器要定期“ 体检 ”基为了防止DNS服务不稳定造成业务中断或出错，不少网管人员在设置DNS服务器时都安装了备用DNS服务器，亦即安装不只一台DNS服务器。但这样做也会带来一个潜在的危险，即主DNS服务器出问题，备用自动服务器投入运行，这样会牺牲一定的网络带宽，使得系统总体性能有所下降。危险在于，性能的下降常常是在不知不觉中来到的。所以，为了保证网络经常处于良好的工作状态，网络管理人员需要定期检查DNS服务器的转换表。 本故障中的DNS指向错误导致用户的IP数据包对准了子网服务器，但如果对准的不是服务器而是中心网络本地网段中的某台机器，则故障强度会减弱，用户不会感到非常明显的速度变慢。这样可能不会感到明显的“ 身体不适 ”从而使得网络长期带病运行。就象人一样，定期的体检对及时发现疾病及其隐患是非常必要的。而如何及时发现路由优化方面的问题，也是网络定期项目测试中的

内容之一，对大型网络则更有必要，必须坚持定期维护和测试。 (2).网络状况的实时监控 许多网络设备如路由器、交换机、只能集线器等都支持SNMP网管功能，但为了全面监测网络通道功能，还需要网络设备支持全面的RMON和RMON2。用这样的设备组建起来的网络其管理和故障诊断功能是很不错的。但现实的问题是，这样的网络设备价格是普通网络设备的6～10倍左右，用户难以接受。因此，为了随时监测网络的服务应用流量及其比例、来源，工作记录以及必要时进行解包分析，建议用户在重要的服务器通道或路由通道上安装监测接口。以便必要时可以随时将流量分析仪、网络测试仪接入通道进行监测和分析。这样，本故障的查找时间可以缩短到20分钟左右。当然，如果资金允许，也可以将流量分析仪长期接入通道对多个重要的网络设备进行全速率透明流量监测，这样可以把故障定位时间缩短到1分钟以内。 这次“ 出诊 ”总的来说还算顺利，其实每次出诊就是一次学习和提高的机会。也许上述案例只是个案，你可能不会遇到，但排错思路还是值得大家借鉴的。另外，最后的两点建议我希望能够引起大家的重视。 2009年上半年全国计算机等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总 2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 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