计算机网络管理中的故障责任取证

Responsibility Forensics In Computer Network Management

徐鹏民 王 海 （山东莱阳农学院网络中心 266109）

摘要：本文分析了网络管理过程中故障纠纷的成因，并结合实践，对网络管理过程中，故障取证的方法、步骤和存在问题做了探索。

关键词：网络管理 责任取证

随着 INTERNET 的普及，计算机网络在社会生活中的作用日益重要，因而，计算机网络故障所造成的影响也越来越大，尤其是网络故障所引起的责任和经济损失，更引人注目，因此，尽快确定故障原因，明确故障责任，就成为亟待解决的问题。但是，由于网络故障的复杂性和时效性，导致故障责任难以明确，因而，许多因网络故障引起的经济损失和案件无法确定责任，引起大量纠纷。

本文结合工作实践，对这一问题加以探讨。

1 计算机网络故障的类型、成因及责任分析

从故障分析的角度，按照计算机网络的构成和功能，可将其分为四部分：

用户端、局域网（LAN）部分、内容服务部分和广域网（WAN）接入线路。

实际的网络运行中，每一部分都有可能发生故障，但局域网部分最为复杂，是各种网络故障汇聚的焦点，网络故障的责任纠纷也主要在局域网管理者与其他部分之间，因此，本文主要站在局域网管理者的角度。

1.1 用户端

用户入网设备的硬、软件故障，计算机病毒或黑客攻击，用户入网设备与局域网之间的接口故障都可能引起网络故障。

用户入网设备的硬、软件故障，一般症状明显，规律性强，易于取证，很小引起纠纷。

计算机病毒或黑客攻击引起的网络故障，有时有较大的隐蔽性。例如，最近的冲击波和震荡波网络病毒，往往是用户机一上网就出故障，而断网后，则一切正常，因此，普通用户误认为是网络部分故障引起的问题。对待此类问题的取证方法是：

用干净、健康的入网设备，取代用户设备，入网测试，证明故障原因的来源，并对用户设备进行病毒检测，查出致病因素。

用户入网设备与局域网之间的接口故障引起的网络故障，不易明确责任，需要从技术和其他手段，认真搜集证据。首先通过技术测试，确定故障部位，然后按照原施工合同或说明断定责任。如，一局域网用户由于经常插拔 RJ45 接口，加上原布线施工质量不过关，导致接口接触不良，上网时，时断时续，此类责任应由布线部门和用户共同承担。

1.2 局域网（LAN）部分

（1）布线系统。由于布线系统质量问题或布线标准不满足要求而引起的网络故障。例如，在一网络系统中，部分千兆线路用户反映网络速度与理想值差距较大，为此，我们首先对线路两端的网络设备进行性能测试，结果均正常，然后，对布线系统做测试，发现不符合合同要求的六类布线标准，因此，责任应由布线公司承担。

（2）网络设备。网络设备的硬、软件故障，配置错误，环境影响，会引起网络故障。

网络设备的硬、软件故障，配置错误引起的故障，一般具有规律性，较易确定，可采用设备替换或插拔法检测。

环境影响，是无线网络故障的重要故障来源。

（3）网络病毒与黑客攻击。这是近期网络故障的重要来源，而且有愈来愈烈的趋势。网络病毒可引起网络堵塞，性能下降，严重时可导致网络瘫痪。黑客行为可引起信息泄露，也可导致网络瘫痪，这涉及网络安全问题，属于另处一个范畴－计算机犯罪取证，在此不多讨论。

（4）局域网与用户之间的接口。一般是由于用户设备配置不当引起，不易引起纠纷。

（5）局域网与广域网之间的接口。涉及硬件、软件和配置三方面因素，是目前出现故障责任纠纷较多的部位。由于接口处必然存在一方设备安装在另一方机房的情况，因而，还会引起设备管理的问题，如因供电或人为损坏导致存放在本地机房的对方设备故障等。

硬件故障较易定位，也容易确定责任。

软件和配置故障，一般是由于本地网络设备或其他设备

做了改动,而对方相应设备没有做相匹配的更改所致。

但确定网络设备配置错误,有时是比较复杂的过程,尤其涉及网间路由问题,由于双方技术人员互不了解对方的网络配置,所以经常难以确定故障来源,从而也无法落实责任。

1.3 内容服务部分

内容服务器因设备硬件、软件配置和病毒等因素,可产生用户无法访问的网络故障,但无论那种故障,都容易取证,主要责任一般应由服务器管理者承担。

1.4 广域网(WAN)接入线路

线路中断、端设备硬件故障或容量不足、配置不当是接入线路故障的主要来源。其中,接入商线路容量不足,导致网络阻塞是局域网管理者经常遇到的,限于管理手段,其取证比较困难。如有的线路提供商为很多用户提供接入服务,当接入用户同时在线时,网络产生阻塞,但其他时间则比较通畅。

2 网络故障取证方法

2.1 故障现场录像、录音、照相

这是传统的取证手段,适合硬件故障。如通信设备上都设有各种指示装置,相关设备产生异常时,会出现错误报警,通过对报警指示的录像和录音,记录下故障表现,可做为故障分析和责任确定的有力证据。

2.2 计算机屏幕拷屏

由于很多网络监控是通过计算机进行的,对故障现场的屏幕进行硬拷贝,也是可靠的故障记录手段,这种方法不易伪造,可信度较高,图 1 是一幅网络监控的屏幕拷贝,可清楚显示出交换机各端口的数据流量情况、时间及其他相关故障表现。

图 1

2.3 设备日志

计算机网络的运行情况会在路由器、交换机和服务器上有详细的记载,通过日志分析,可以为故障原因和责任提供证据。

2.4 现场检测

在责任相关各方在场的情况下,采取各方承认的各种工具对网络进行现场检测,并将测试过程和结果交由各方签字确认。

2.5 广泛的用户调查与确认

相同或类似环境用户的共同反映,是网络故障定位的充分有力证据。如果大量来自同一局域网的用户均出现上网问题,则可初步断定网络部分产生故障,否则,大多数用户网络正常,只有个别用户出现问题,则用户本身的故障的可能性更大一些。

3 取证步骤及实例分析

3.1 取证步骤

对于网络管理人员,遇到网络故障,首先要对所辖设备进行认真检查和测试,进行故障定位,包括:

故障点到中心交换机之间的各级网络设备的硬件,可用观察、替换等方法;

故障点到中心交换机之间的网络链路,可用 PING、TRACERT、NSLOOKUP 等网络测试命令;

网络管理与监控工具,如 SNIFFER 和各种网络软件;

病毒和黑客检测工具;

其他设备与工具,如网络布线测试设备等;

故障定位后,需要查清故障原因,然后视情况采取以下措施:

如果条件允许,保护现场,将有关责任人集中到现场,明确责任;

否则,采取相应取证方法,对故障现场做好取证记录后,再排除故障,恢复网络运行,然后,根据证据落实责任。

3.2 实例分析一

某一用户报告无法使用网络,但脱机工作正常。

首先,检查整个网络运行情况,工作正常;

检查用户设备硬件,正常;

了解与该用户位于同一网段的其他用户的网络状况,也正常;

用另一设备替代该用户机上网,正常;

至此可以确定,故障原因在用户机,进一步检查,发现该机感染网络病毒,要求用户清除病毒。但用户反复杀毒后,仍然不能解决问题,便认为故障原因在网络部分。为此,我们使用网络嗅包器 SNIFFER 对用户机的网络数据进行检测,确定用户机感染震荡波病毒,并显示出发包情况和包内内容,使用户承认故障来源。如图 2 所示。

3.3 实例分析二

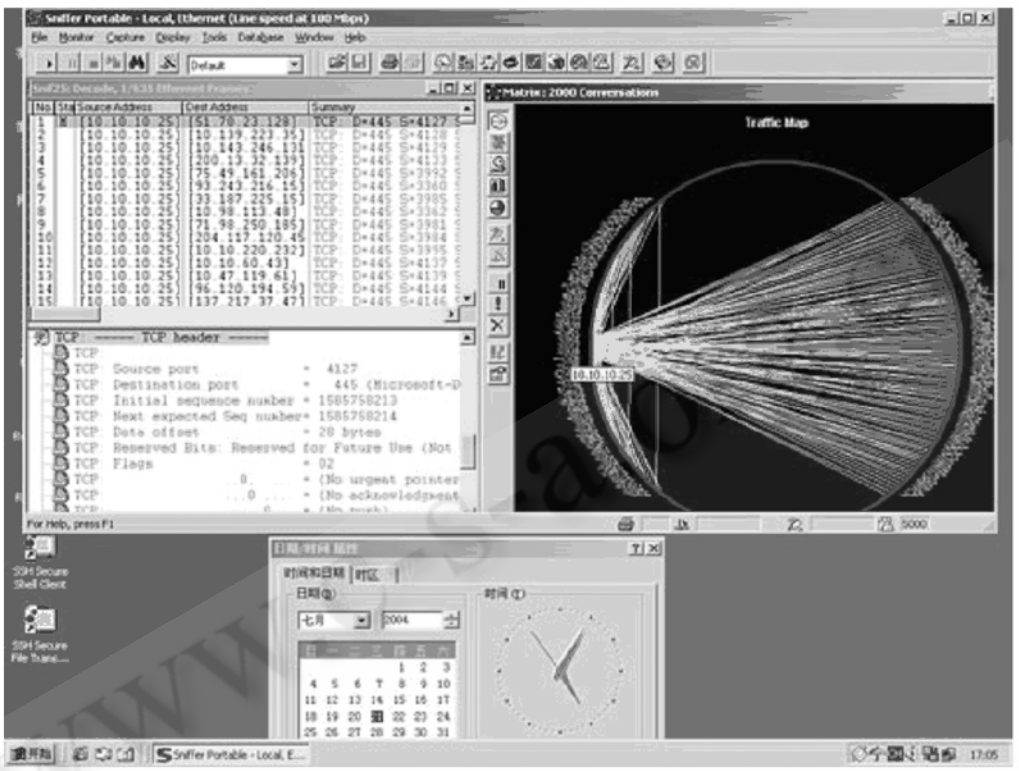

图 2

网络租用线路的各种通信设备表现正常,但网络数据传输时断时续,且无规律性,当线路提供商技术人员到现场时,线路正常,未取得异常证据,因此,线路提供商认为故障原因在局域网内,拒绝承担责任。为此,我们将局域网与租用线路隔离,在线路两端使用单机做不同长度的发包测试,故障出现时,将测试结果做硬拷屏,清楚显示出故障表现,当数据包长度超过 40 字节时,数据通信中断,从而使线路提供商确认线路存在问题。

4 网络故障取证中存在的问题及注意事项

网络故障取证与其他计算机取证一样,处于初始阶段,因而,实践中还存在很多问题,有待进一步解决:

(1) 方法与工具的不足,加上数字设备极易做假而又不易留下痕迹的问题,使得数字化证据的可信度不高,容易引起争执,法律上也难以得到认可;

(2) 网络故障往往具有突发性和无规律性,而且,一般不能为保存证据而使网络长时间处于故障状态;

(3) 相关法律法规的缺乏,使用追究责任变得困难。

为此,在具体工作中,需要尽可能做好如下工作:

① 做好并长期保存好各种网络信息记录,如用户上网信息、设备配置信息、服务日志以及网络历史流量等,以便出现故障和确定责任时参考。

② 故障定位和取证的用户确认。各种测试过程和结果应该得到用户的确认,才能成为有力的证据。

③ 证据的时效性。有些网络故障原因有较强的时效性,必须及时得到责任有关者的确认,否则,将失去可信度。如网络病毒引起的故障,往往在短时间给用户造成损失,但很快消失,如果不能在病毒发作期间,让用户确信病毒存在并影响网络,事后则很难为用户接受故障原因。 (全文完)