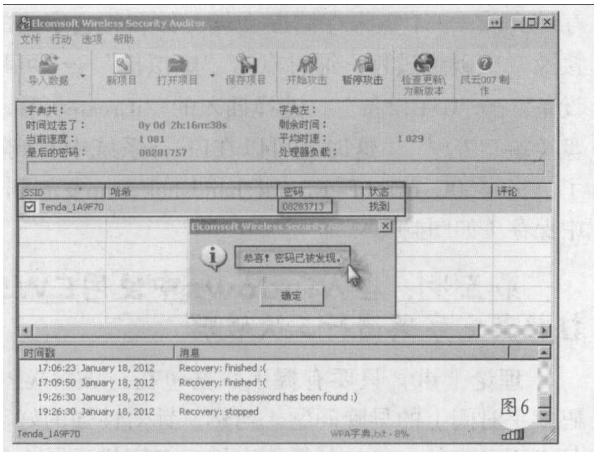


图6

怎么样，貌似极为安全的WPA/WPA2密码在经过被抓取握手数据包、挂接字典暴破等操作之后就灰飞烟灭，是不是很可怕呢？的确，只要你的WPA密码在字典文件中就难逃被破解的厄运！那么，我们就真的束手无策了吗？其实对策也很简单，只要设置一个长度够长、字母数字及特殊字符都包含的足够复杂的WPA密码就安全了。

●文/图 方永辉

# TCP/IP网络故障，分层排查之道

为了方便进行网络共享与通信交流，不少单位往往会以多种形式来组建适当规模的局域网。在尽情享受局域网带给单位员工便利的同时，长时间运行的网络也容易出现各式各样的奇怪故障，这些故障如果不能被快速排查，就会给单位的高效办公带来不小的麻烦。为此，本文现在就以TCP/IP协议类型网络为操作蓝本，向大家介绍如何分层排查网络故障，提高故障排查效率！

## 认识TCP/IP协议模型

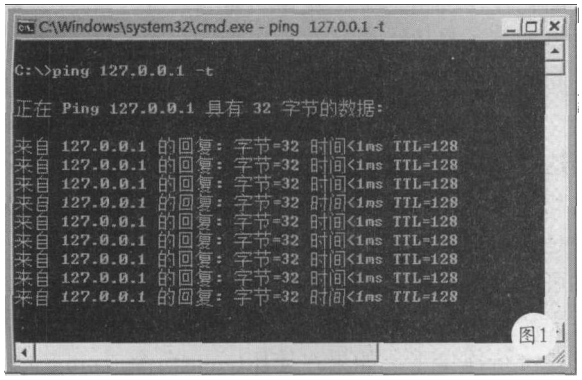
凭借实用、简洁等特点，TCP/IP协议被许多单位广泛使用，该协议实际上是由几个不同的通信协议组合在一起形成的协议栈，它主要包括网络传输控制协议、因特网协议等，使用该协议栈组建而成的局域网，能够将不同的操作系统，不同的硬件设备，不同的内网系统互相连接起来，而且不同的局域网之间也能互相连接，形成全球范围内的因特网。按照从上到下的顺序，TCP/IP协议模型可以分为应用层、传输层、互联网络层、网络接口层；对应类型的网络发生故障时，完全可以按照分层结构进行逐步排查。

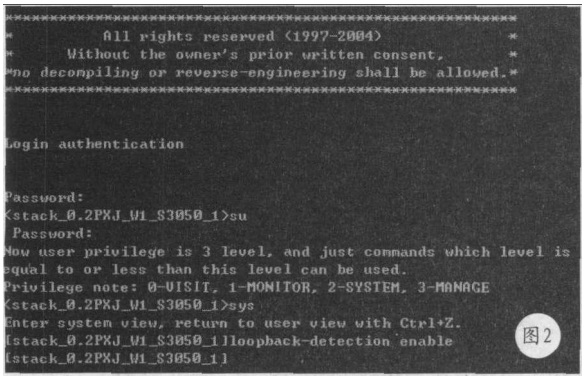
## 排查网络接口层

尽管TCP/IP协议模型对网络接口层没有进行明确定义，不过在实际管理网络的时候，网络接口层其实与OSI参照模型中的数据链路层与物理层存在着对应关系。数据链路层在实际网络分层结构中，主要是对在物理层中传输的数据按照正确的规程进行封装，确保数据信号以标准的网络数据帧在传输介质中正常传输；由于这一层次主要涉及到网卡设备或常规适配卡以及它们的驱动程序，出现在这一层次的网络故障，多半也与这些因素有关，所以在网络客户端系统中，网管员应该依照不同型号的网卡设备或适配卡，来正确安装对应的设备驱动程序，确保设备以及驱动程序工作状态都正常。

判断数据链路层工作状态是否正常，可以在客户端系统依次单击“开始”、“运行”命令，在弹出的系统运行对话框中，输入字符串命令“ping 127.0.0.1 -t”，按回车键后，要是系统返回如图1所示的结果信息，那就意味着数据链路层工作状态是正常的，具体地说就是网卡以及驱动程序都是正常的；如果ping命令测试操作失败，例如出现响应时间比较长，无法达到目的地等，那就需要检查网卡设备的工作状态以及对应驱动程序是否正常，在查看网卡设备工作是否正常时，可以先打开系统的设备管理器窗口，展开网络适配器分支，检查目标网卡设备图标上是否有红色叉号标志或黄色感叹号标志，黄色感叹号标志表示网卡

地址可能与其他客户端系统的地址发生了冲突，需要重新调整IP地址，如果出现红色叉号标志，就说明网络传输介质与网卡设备接触不良等。




物理层主要是用来规定信道传输的介质、电气或机械的接口，这一层次的网络主要包括网络硬件设备以及它们的连接方式，比方说常见的路由器、交换机、集线器、ADSL MODEM等设备和它们的电气连接方式。在排查物理层的网络故障时，可以借助专业的线缆测试工具，来测试物理链路的连通性是否正常，之后通过查看设备信号灯状态来判断网络设备的工作状态是否正常。一般来说，网络设备上的link信号灯状态应该处于长亮状态，action信号灯应该处于闪烁状态，如果发现信号灯状态明显不正常时，那必须认真检查网络设备的接口与传输介质之间的接触是否牢靠，在设备接触牢靠的情况下，信号灯状态仍然还不正常的话，不妨尝试重新启动设备，再依照网络设备的操作手册对其进行正确操作。

## 排查互联网络层

这一层网络结构中主要涉及到的设备包括三层交换机、路由器以及普通计算机终端设备等。一般来说，在对已有网络进行升级扩容，或者调整原有网络的拓扑结构时，互联网络层就特别容易出现一些网络故障，当然，如果对相关的网络协议配置不正确的话，也容易在这一层发生网络故障，所以在怀疑互联网络层出现故障现象时，必须要依照实际情况以及具体的故障现象进行逐一排查。

在普通客户端系统中，如果网管员没有正确配置好上网参数，具体包括DNS服务器地址、默认网关地址、子网掩码地址、IP地址等参数，那么互联网络层就会出现网络访问失败的故障。对于局域网中的三层交换机以及路由器等重要网络设备来说，网管员应该在熟悉组网拓扑结构的情况下才能进行正确配置。正常情况下，网管员使用ping命令分别对本地系统IP地址、本地网关地址、远端IP地址进行分别测试，基本就能分辨出究竟在互联网络层的哪个位置出现故障了。倘若网络配置正常，而且物理层检查也没有发现问题时，那就需要对下面几个细节因素进行认真检查了：

### 1、检查病毒因素

现在，网络病毒疯狂肆虐，稍有不慎网络就可能遭遇大面积攻击的现象，这种现象会直接造成有效的出口带宽资源被许多无效的数据信息长期“霸占”，最终会导致用户访问网络不通。此时，网管员可以在局域网的核心交换机中，扫描每个交换端口，查看它们的接受数据包和发送数据包的状态信息，如果某个交换端口的数据流量比较大时，那就意味着该端口连接的子网络可能存在病毒攻击现象。这时，从网络中下载安装sniffer工具，对网络中传输的数据进行抓包分析，要是显示来自某个IP地址的数据包不正常时，那就能判断出指定IP地址的计算机系统感染了网络病毒；之后，将连接该计算机系统的网络线缆从局域网中断开，使用最新版本的杀毒软件对目标计算机系统进行病毒查杀操作，待病毒查杀干净后，恢复对应系统的网络连接状态。

### 2、检查环路因素

要是局域网中出现了环路现象，那么互联网络层的工作状态就会不正常。环路现象具体地表现为两种类型，一种是路由环路现象，另外一种是网络环路现象，其中路由环路现象主要是由于两个不同子网之间发生了环路故障，这类问题我们可以从一个实践案例中来进行认识。比方说，某单位局域网的核心交换机中划分设置了若干个VLAN，为了保证每个VLAN之间可以相互访问，网管员在不同VLAN之间配置启用了访问路由，不同VLAN通过宽带光纤线路连接到不同的办公楼层。要是将不同的VLAN借助交换机互相连接起来，这样就容易发生路由环路现象，从而造成VLAN连接端口被许多无效的数据包堵塞，最终造成网络传输通道被中断。由于路由环路影响的范围比较广泛，在排查这类网络故障时，尽量要使用分段排查

的方法，来定位故障位置，每一段的排查方法几乎与网络环路的排查方法相同。

要是某个工作子网中由于连接不当因素，发生了网络环路现象时，那就会造成每一帧数据包都在网络中重复广播，从而会引起广播风暴，最终会阻塞网络传输通道。正常情况下，当局域网中发生网络环路现象时，那么该子网上联交换机所有端口的信号灯都会处于不停闪烁状态；所以，当网管员看到某台交换机中的信号灯出现相同的现象时，就需要依次拔出连接到交换端口上的每一根网络线缆，当断开某根线缆的连通状态后，交换机上所有信号灯的显示状态全部恢复为正常时，那就能判断出对应交换端口下面存在网络环路现象，之后查看目标交换端口下面的网络连接，直到排除网络环路现象为止。

当然，现在排查网络环路现象比较方便了，因为很多智能交换机都支持环路监测功能以及环路监测受控功能，通过这些功能交换机可以自动定时对所有端口进行扫描监测，以便判断交换端口下面是否存在网络环路现象，如果监测到某个交换端口被网络环回时，该交换端口就会自动处于环回监测状态，依照交换端口参数设置以及端口类型的不同，交换机可以自动将指定交换端口关闭掉或者自动上报对应端口的日志信息，日后网管员只要查看日志信息或根据端口的启用状态，就能快速判断出局域网中是否存在网络环路现象了。

例如，在H3C系列交换机中，可以进入交换机后台管理界面，执行“system-view”命令，切换到系统全局视图状态，输入“loopback-detection enable”命令，将交换机的全局端口环回监测功能启用成功，如图2所示；之后继续执行“interface G1/0/16”之类的命令，进入特定交换端口视图状态，同时在该命令行提示符下再执行“loopback-detection enable”命令，启用特定交换端口的环回监测功能，执行“loopback-detection control enable”命令启用环路监测受控功能，这样交换机日后就能自动检查发现网络环路现象了。

### 3、检查负载因素

当局域网中某台交换机工作时间一长后，它的自身性能在不断老化，同时它所连接的负载可能在不断增加，在这种情形下，交换机常常会由于负载太多而不堪重负，最终造成频繁死机现象。在排查这类因素引起的网络故障时，可以先使用telnet命令尝试远程登录交换机，来查看它的CPU和内存资源的占用状态，当这些资源的消耗率在70%以上时，那就意味着交换机此时已处于超负荷运行状态，频繁发生的网络故障就是由于交换机性能老化、运行负载太重引起的，此时可以重新启动交换机系统来尝试解决网络故障，实在无法解决时，只有更换性能更高的交换机来替代旧设备进行连接了。如果在使用telent命令或ping命令登录或测试交换机时，交换机无法响应，那就能确认交换机已处于死机状态，此时唯一解决的办法就是更换新的交换机设备。当然，交换机如果自身的硬件或软件出现问题时，也容易导致互联网络层出现网络故障，由这种因素引起的网络故障，一般也只能通过更换交换机来解决。

## 排查传输应用层

传输层主要涉及到用户数据报协议和传输控制层协议，依靠用户数据报协议提供的非连接、不可靠服务，将数据包传输到网络中，通过传输控制层协议为上层应用提供面向连接的、可靠的服务。这一层引起的网络故障，往往都是由于操作系统网络连接组件工作状态不正常或防火墙设置不当引起的，只要查看防火墙是否进行了网络连接限制，或查看操作系统是否存在动态连接库文件受损等现象，如果存在的话，只要将它们消除就能解决网络故障了。

而应用层主要涉及到用户的实际网络应用，比方说WWW服务、DNS服务等，在排查这一层网络故障时，重点是检查一些核心的网络服务是否启动正常，应用程序的网络设置是否正确等。