

DCS中以太网故障分析

江苏射阳港发电有限责任公司（224346）刘华山 刘维锋 朱志强

摘要：文章针对DCS系统中操作站所在的以太网发生的几种常见故障，从设备构造及数据通信的原理着手，分别提出以太网广播风暴产生原因、交换机学习功能、堆叠交换机作用等几方面的依据，找出相应故障的原因，提出了解决问题的方法，为DCS系统维护提供参考。

关键词：DCS 以太网 故障 分析

0 引言

进入二十一世纪，计算机及其通信技术飞速发展，在电厂DCS系统中的应用也在日益成熟，传统观念上，电厂维护人员大部分依赖设备制造单位的技术支持，然而，电力体制改革的今天，作为电厂，必须加强自主维护的能力，因此，对于电厂热工人员，DCS系统维护方面的压力显而易见，一旦处理不及时或有所失误，都有可能直接造成停机的危险，这就需要不断学习，汲取新的知识，积累经验。

1 前言

我公司DCS系统主要任务是单元机组热力过程的生产和控制，使用的是NETWORK-6000系统，其网络结构如图1所示，分两层网络，下层为双层环网结构，使用令牌方式传输数据，主要任务是完成服务器同DPU（数据处理单元）进行数据通信。上层网络为千兆以太网结构，使用的网桥为3COM交换机，主要任务是完成服务器同6台操作站进行数据通信，以太网为双冗余配置，正常情况下操作站同主服务器进行数据通信。

天津翔悦

天津翔悦密封材料有限公司



弗莱希波·泰格
金属波纹管有限公司



温州环球阀门制造有限公司



北新集团建材股份有限公司

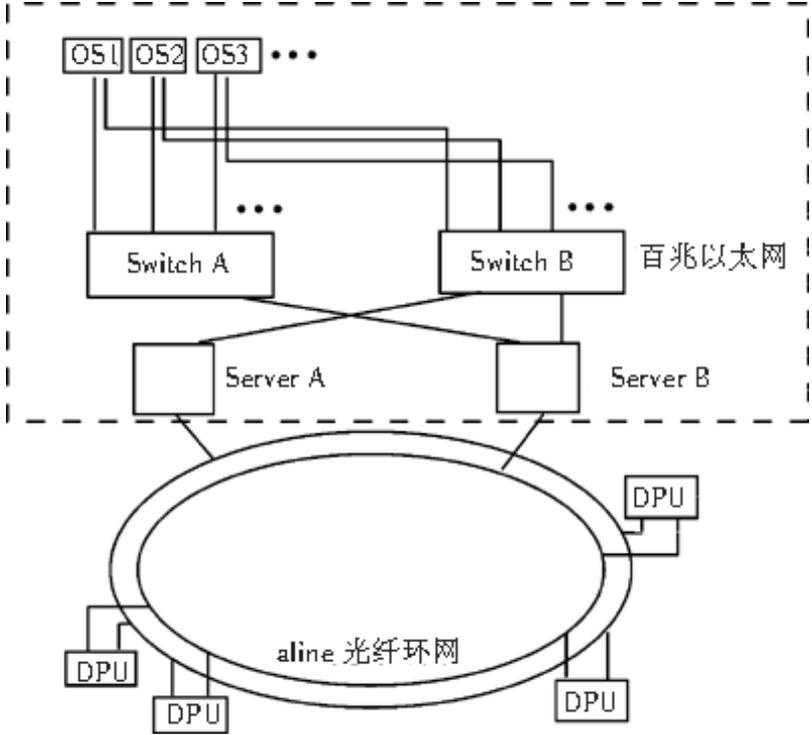


图1 DCS系统数据通信网络示意图

2 故障一：操作站经常切至备用服务器

在DCS系统正常运行时，其os操作站同serverA进行数据通信，经常发生所有操作站全部切为同serverB进行数据通信。

DCS系统os操作站和server服务器使用的fix6.1软件系统，该软件系统功能强大，一般情况下确定os直接与serverA进行通信，在os操作站fix软件的TCP/IP中，对timer进行设置，分别设置send=5秒，receive=5秒，keep active=10秒，也就是根据数据通信的大致流量，将ops操作站向serverA发送时间和接收时间规定在5秒内，如果超过此时间，TCP/IP直接指向备用服务器serverB，因此，操作站经常切至备用服务是由于同主服务器的通信超时引起的。

2.1 通信超时的原因分析

本公司交换式以太网中，其网桥设备为3com公司的4400E交换机，在以太网组建成功后，交换机即记录下该网络中所有设备的地址，而不需记录其IP地址，其数据交换是一种直通方式，即交换机只要检查到帧头中所包含的目的地址就立即转发该帧，而无需等待帧全部的被接收，也不进行错误校验。由于以太网帧头的长度总是固定的，因此帧通过交换机的转发时延也保持不变。

交换机提供给每个用户专用的信息通道，除非两个源端口企图同时将信息发往同一个目的端口，否则多个源端口与目的端口之间可同时进行通信而不会发生冲突，在操作站设置中，都明确设置了通信的主从结构，因此，不可能由于两台服务器同时向操作站通讯而导致冲突的事件。

那么是什么原因产生广播风暴而引起通信超时的呢？有以下几种可能

第一种可能是网络设备原因，如果网络设备出现问题，网络交换机原有的点对点转发功能失去，这样，在网络稍微繁忙时，就会产生广播风暴。

第二种可能是网卡损坏，如果网络机器的网卡损坏，损坏的网卡不停向交换机发送大量的数据包，这些大量的无用数据包占据交换机的处理时间，导致产生广播风暴。

第三种可能是产生了病毒或受到黑客软件攻击，目前，一些比较流行的网络病毒，Funlove、震荡波、RPC等

病毒，一旦有机器中毒后，会立即通过网络进行传播。网络病毒的传播，就会损耗大量的网络带宽，引起网络堵塞，引起广播风暴。但是，DCS系统以太网属于内部局域网，在现有的软件使用管理制度下，不可能受到病毒感染或黑客软件攻击的。

2.2 数据通信情况的检查

局域网数据通信无法用手工进行测量，只有依靠先进的软件工具进行诊断，我们通过手中的sniffer局域网管理软件，查看网络中数据流量，对局域网设备及数据通信进行专家诊断。

运行sniffer软件，5分钟后，系统提示局域网数据包发送情况监测已经全部连接，未出现任何异常，各个操作站按正常情况向交换机发数据包，再由交换机转发给服务器，同样，服务器将数据包发给交换机后，交换机又直接转发给各个操作站，发出的请求和接收到的基本相等，几个操作站与交换机之间的通讯量基本一致。

转过半个小时后，突然发现192.168.1.1（汽机站）发出的请求数增多，同时它与交换机间的通讯量也急剧增加，达到数百兆后，发现其它所有操作站均出现了切换，也就说明了其产生以太网广播风暴，引起所有操作站均在规定时间内收不到服务器来的数据，自动切换至备用服务器，当然，它是双网卡冗余的，切换后另一块网卡实现数据的正常通讯。

更换了该工控机的网卡后，DCS操作站没有再发生向备用服务器切换事件

3 故障二：操作站更换工控机后连接不上

去年10月份，电气操作站运行中死机，经检查，系工控机主板故障，更换工控机主板，重新安装主板的各种驱动程序，机器恢复后，在连网过程中发现经常连不上以太网，从而导致该操作站无法从服务器中取得生产过程数据。

维护人员检查了交换机各个端口和网线，均正常，也尝试着将连接网线换个端口试验，也无法正常连入，更换主板前系统运行一直正常，而更换主板后即无法联网呢？

以太网交换机是一种“网桥”设备。传统的网桥是这样工作的，一开始它接收以太网帧，然后，把它们发送到除接收端口之外的全部其它端口。以太网交换器具允许允许双绞线连接的能力。在以太网中，IP地址是根据现在的IPv4标准指定的，不受硬件限制比较容易记忆的地址，长度4个字节。而MAC地址却是用网卡的物理地址，保存在网卡的EPROM里面，与硬件有关系，虽然在TCP/IP网络中，计算机往往需要设置IP地址后才能通讯，然而，实际上计算机之间的通讯并不是通过IP地址，而是借助于网卡的MAC地址。IP地址只是被用于查询欲通讯的目的计算机的MAC地址。

以太网交换机具有学习功能，它渐学习哪一个端口连接了哪些MAC地址。这时候，网桥就变成了一台学习设备，能够存储在一个端口上看到的全部的MAC地址表。当一个帧需要发出时，网桥将查看在网桥表中的目标MAC地址，并且知道应该在哪一个端口发送这个帧。这种仅向正确的主机发送数据的能力是交换技术中的一个巨大的进步，因为这可能显著减少通信冲突。如果在网桥表中没有目标MAC地址，交换机就简单地把数据发送到全部端口。

因此，在电气操作站主板损坏前，交换机记住其网卡的MAC地址，每次发送数据至电气站时，都按照直接发送至其MAC地址的方法。由于操作站使用的是主板集成网卡，在更换主板后，相当于更换了MAC地址，同交换机中原端口对应的MAC地址表冲突，导致通讯不上。同时，其它几个端口也是由于以前的调试和他用，导致其形成了地址表而不能接受新地址表。

根据设备制造说明书，交换机学习的MAC地址表在断开一定时间后，即可以自动清空，但由于交换机长时间未断电，其MAC地址表自动清空功能未起到作用。在运行的机组不允许对交换机断电的情况下，维护人员通过仔细查找，终于找到一个未定义地址表的端口，将操作站恢复使用。

机组停运后，检修人员打开交换机，进行停电和内部清扫灰尘，系统恢复至原始状态运行。

4 故障三：所有操作站数据均丢失

去年12月份，#2机组正在运行中，DCS系统所有操作站突然数据全部丢失，但两台服务器数据正常，公司立即进入事故预案的预警阶段，热工维护人员进行现场抢修。

从上述图1中可以看出，如果单个操作站网卡故障，会造成一般情况下的广播风暴，导致操作站自动切为备用服务器运行，操作站仍能够看到数据并维持运行。因此，可以排除是由于单个操作站原因引起所有操作站无数据的故障。

那么，问题集中在以太网交换机上，我们可以从目前使用的两只堆叠的以太网交换机工作原理来进行分析。

所谓可堆叠交换机，就是指一个交换机中一般同时具有“UP”和“DOWN”堆叠端口。当多个交换机连接在一起时，其作用就像一个模块化交换机一样，堆叠在一起交换机可以当作一个单元设备来进行管理。一般情况下，当有多个交换机堆叠时，其中存在一个可管理交换机，利用可管理交换机可对此可堆叠式交换机中的其他“独立型交换机”进行管理。可堆叠式交换机可非常方便地实现对网络的扩充，是新建网络时最为理想的选择。这样做的好处是，一方面增加了用户端口，能够在交换机之间建立一条较宽的宽带链路，这样每个实际使用的用户带宽就有可能更宽（只有在并不是所有端口都在使用情况下）。另一方面多个交换机能够作为一个大的交换机，便于统一管理。

由此分析，出现所有操作站数据丢失的原因是推叠交换中的管理交换机出现故障，导致交换机功能失去，数据不能正常通信。

检修人员更换了这对交换机后，系统恢复正常使用。

5 结论

通过对DCS系统中的以太网故障的分析，解决了数据通信方面的问题，并且为以后的检修提供了一些指导性的理论。当然，DCS中以太网存在其它类型故障的机会还有可能发生，只要了解系统设备原理，一样可以顺当地解决问题。

6 参考文献

[1] 王廷尧等. 以太网的技术与应用[M]. 北京：人民邮电出版社，2005.

文章作者： 刘华山

发表时间： 2006-07-24 00:00:00

[\[关闭窗口\]](#) [\[打印文章\]](#) [\[回到顶端\]](#)