

自动化远程维护实践

变电站的形式一直在改进，自动化调试人员的工作方式也应该进行革新，远程维护的目的就是要补充传统的进站工作方式，调试人员在总部机房就可以总览全部变电站的各种数据参数，根据工作性质进行预判与优化处理，达到合理利用有限资源和快速处理紧急情况的目的。

韩旭/北京京电电网维护集团有限公司继电保护自动化公司



韩旭/助理工程师

关键词/Keywords

- 远程维护 ·
- 故障处理 ·
- 稳定性 ·

0 引言

随着北京城市建设的飞速发展，越来越多的商场、写字楼、居民楼拔地而起，变电站的数量也随之猛增，北京现有220 kV变电站81座，110 kV变电站379座，从市中心到最远的站距离大约有100 km，距离十分遥远，调试人员进站的工作效率将大打折扣，紧急故障处理的实效性也将大大降低。如果可以改进一下工作方式，将一部分单纯修改配置和软件层面的处缺工作进行远程操作，这将使进站维护的效率倍增。当然如果进行更换硬件和改线等工作还是必须要调试人员亲自到达现场的。诸如修改服务器数据、远动组态、管理机配置、图形及备份数据等对监控系统修改的工作以及自动装置的重置、重启和故障报文截取分析等工作，完全可以在远端进行。这样一来，远程维护的稳定性和安全性将成为重点考虑的因素。

1 变电站测试

1.1 网络搭建

(1) 物理连接

220 kV台湖站为常规综自变电站，

只有站控层与间隔层，主交换机将两层连接进行数据交换，调度通过专用2Mbit/s通道与远动机相连接，网络结构相对智能来说比较简单。远程维护的目的就是查看和修改站端相应设备，所以远程终端需要连接站端交换网络方能工作。但是台湖站没有到公司本部的自动化远程维护专用通道，因此只能借助现有的已经停运了的集控站五防通道进行测试。集控站五防通道的路由器设置的IP地址与厂站端间隔层地址不在一个网段，集控站五防通道IP为10.0.0.0/30的A类IP地址，而站端交换网络为172.120.0.0/16的B类地址。为了解决此问题，工作人员在站端增加了一个Cisco2621XM路由器作为NAT（网络地址转换协议）路由，安装在保护室网络通信屏内，屏内提供逆变电源，放置一根从调度数据网屏到网络通信屏的直通网线，此网线连接在Cisco2621XM路由器Fa0/0接口；放置另一根网线至本屏主交换机，连接在Cisco2621XM路由Fa0/1接口。物理连接示意图如图1所示。

(2) 相关协议

1) NAT技术。NAT（Network Address Translator）是一种将IP地址从一个编址域映射到另一个编址域的方法，典型的应用是把RFC1918定义的内网IP地址映射到Internet所使用的公网IP地址。NAT的最初目的是弥补IPv4地址数量不足这个先天缺陷，通过映射以减缓可用公网IP地址的消耗，而且还能有效地避免网络外部的攻击，隐藏并保护内网计算机，NAT之内的PC联机到Internet上时，它所显示的IP是NAT主机的公网IP，在外界进行端口扫描时（Port Scan），

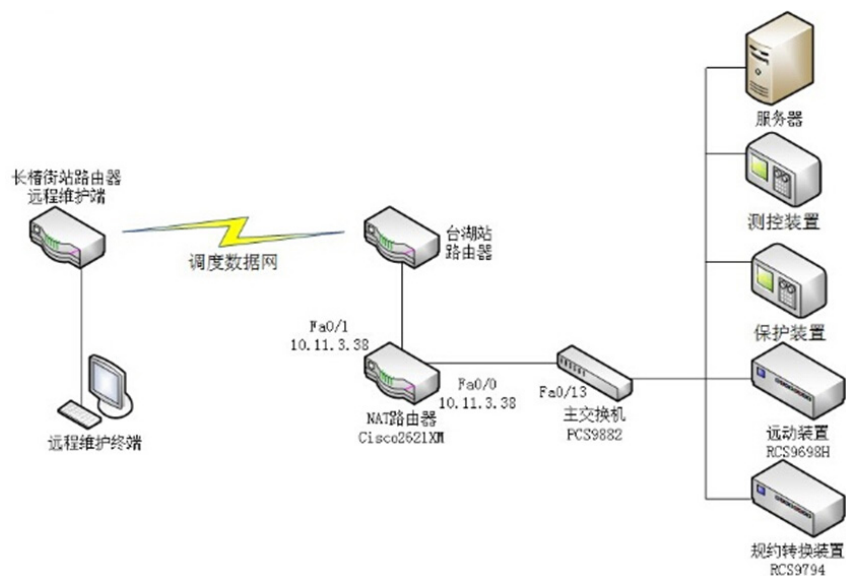


图1 物理连接示意图

client端的主机端口状态是隐藏的，这就使黑客无法进行端口扫描。这次试验采用NAT技术就是需要它的转换映射功能，将10.0.0.0/30的网段映射成198.120.0.0/16的网段，实现网络的互通。另外一种方法是在两个站端路由器上修改配置，各加入一条静态路由条目，使两端路由器的路由表中有到达彼此的网络路径，用这种方法相对NAT来说可以减少路由器的CPU负荷，同时减少网络延时，因为NAT会使路由器对其传送的每个数据包的IP包头进行拆包分析，而这一过程无法进行高速缓存。虽然NAT技术有它的局限性，但由于没有站内路由器的调试权限，只能考虑加装一台新路由器进行NAT映射，这样就可以很方便地使用现有的网络环境。

NAT的实现方式有三种，即静态转换Static NAT、动态转换Dynamic NAT和端口多路复用PAT。第一，静态NAT是指将内网IP地址映射为公网IP地址，地址是一一对应且固定的。第二，动态NAT是将内网IP地址映射到一个指定的公网IP地址池，地址池是一个合法公网IP地址的集合，可以是一个连续IP地址，也可是不连续的几个独立的IP地址，映射也是一一对应的；当地址池中的公网IP地址全部被占用后，后续的NAT申请将会失败，NAT具有一个计数器当连接超时，自动解除映射。第三，PAT将n个内网IP地址映射为一个公网IP地址的不同端口，这也是实际应用最为广泛的一种模式。本站使用静态的方式，路由主

要配置如下所示。

```
Hostname Router
Interface fastethernet0/1
IP address 198.120.0.254 255.255.0.0
IP nat inside
Interface fastethernet 0/0
IP address 10.11.3.38/30
IP nat outside
IP nat inside source static 198.120.0.254
10.11.3.38
IP route 0.0.0.0 0.0.0.0 10.11.3.37
```

2) 端口镜像。端口镜像（Port Mirroring）功能通过在交换机或路由器上，将一个或多个源端口的数据流量转发到某一个指定端口来实现对网络的监听，指定端口称之为“镜像端口”或“目的端口”，在不严重影响源端口正常吞吐流量的情况下，可以通过镜像端口对网络的流量进行监控分析。在智能站中端口镜像是非常重要的功能，可以很好地对变电站内部的网络数据进行监控管理；在网络出故障的时候，可以快速定位故障，网络分析仪所用的数据就是交换机端口镜像转发过来的。在交换机中具体实现端口镜像功能的是交换机端口分析（Switched Port Analyzer）。以太湖站为例，交换机使用的是南瑞继保的PCS-9882交换机，配置如图2所示。

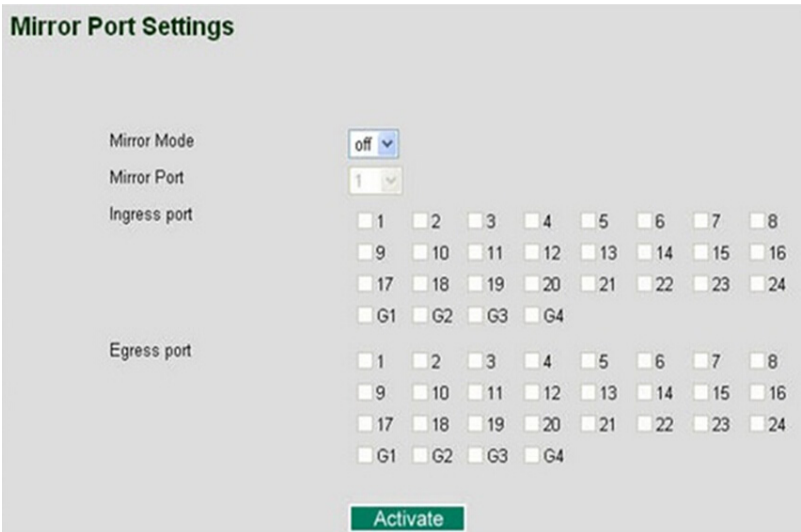


图2 交换机配置

在镜像模式中选择L2开启镜像功能，因为Cisco2621xm与站端交换机连接的端口是13，所以在镜像端口上选择13，在Ingress port上选择全部1~22口（除去镜像口13、23和24口）。因为默认为100 Mbit/s SFP口，在不配置的情况下不能作为二层口使用故不被选择。在Egress port上的选择与Ingress port一样，Ingress port为端口输入流量，Egress port为端口输出流量，端口流入流出选择视实际交换机使用情况而定。

1.2调试工具

(1) 传输工具

比较常用的是flashfxp、cuteftp等，它们都是基于FTP协议（文件传输协议）的。实际测试时，使用工具新建站点分别指向远动主机RCS9698H，目地IP设置为198.120.0.205；远动备机IP为198.120.0.206，进入目录tffs1:中将ccu文件夹中的ccu_工程间隔.cfg和rcs9698.ini两个文件传输至调试终端，完成了对远动装置组态的备份工作。使用效果跟在厂站端一样，可以将程序和组态等数据通过网络传输到终端，也可以将修改后的组态传输至站端远动装置，只是远程传输快慢受通道带宽限制。维护口为串口的装置除外。

(2) 各厂家调试工具

变电站内常用的调试工具有四方的watchbug、CSC1321；南瑞继保的RCS9698、RCS9798、RCS9793和Cfgdebug；南自的PsxView；南瑞科技的Nsctool；长园深瑞的

RemoteMon及ConfigTY122。无论什么软件只要支持网络的都可以进行远程维护。具有专用维护网口的CSC1321和Nsctool等调试软件则需要从NAT路由器的fa0/2口放置一根网线至专用维护网口，根据专用网口网段再做一个NAT 指向fa0/2口。实际测试时，在远程终端打开南瑞继保的Cfgdebug工具，可以在对下窗口里查看测控保护装置的遥信、遥测数值并可以置数；在对上窗口里可以查看104报文，并可以将报文保存至远程终端。

(3) 网络抓包工具

Etheral是一款非常强大的网络数据包分析软件。在远程终端打开软件选取网卡后，配合在站端交换机PCS982上做的端口镜像，可以截取站端站控层全部数据包用来分析一些疑难问题，尤其是分析智能站的goose和sv报文。

(4) 远程桌面工具

Xmanager是一款用于Windows平台远程连接UNIX平台的x终端工具，可提供可视化的远端系统界面。配置xmanager连接站端主服务器的IP，地址为198.120.0.180，进入UNIX solaris登录界面，登录后打开终端，输入tar cvf sophic2013.7.2.tar sophic，将RCS9700系统打包备份，然后再进行压缩，compress sophic2013.7.2.tar，通过ftp工具将压缩后的sophic2013.7.2.tar.Z传输至远程终端。监控系统好多缺陷都是只需要重置、重启装置，在终端中进入特权模式输入init 6正常重启服务器，强制重启时使用reboot命令；远动管理机等装置型可

以用telnet工具或者本厂家维护软件进行重启。需要注意的是，因为通道带宽仅为2 Mbit/s，可视化桌面传输需要的更高的带宽，所以远程桌面显示卡顿十分严重，勉强进行操作。ftp传输几百兆的备份也很吃力，日后如果申请专用通道并将带宽提升到100 Mbit/s的话，可有效解决此问题。

2 远程维护可行性

2.1 远程维护特点

远程维护具有快速、高效的特点。

第一，危及缺陷。当遇到危及缺陷时，远程终端可以先行查看监控界面、程序进程、实时数据和历史数据等参数进行初步判断，如果是程序异常或者进程丢失等情况可以进行远程重置，远程处理失败或者历史数据显示硬件告警的情况，根据前期获得的装置情况确定所需板件、定值单等，做到危及缺陷的优化处理。

第二，事故处理。当遇到保护动作时，可以从远程终端调取监控、保护装置、测控装置和录录的信息，确定保护是否正确动作，做到事故处理的快速性。

第三，一般缺陷。与危及缺陷一样可以进行远程预判和处理，当需要长期监视设备时，远程维护更具优势，例如220 kV老君堂站的PSR741测控不定时发出通信中断故障信号，当时进站用笔记本截取报文，可是因为故障时间不确定，导致调试人员在站端一整天都没能截取到故障报文，效率极低。使用远程维护后，可以在远程终端开启调试程序24 h截取报文，根据实时数据信息判断时间点，做到了监视的持续性和高效性。

2.2 远程维护的安全性

远程维护从技术角度来说实现是可行的，影响其实行最大的问题就是安全。工作票制度和许可制度是电力安全生产最重要的制度，这是进站工作的基础，远程维护的工作也必须按制度执行，如何解决远程维护工作与工作票制度中的矛盾成为其是否能够实行的关键问题。传统工

作的工作票是要写出具体工作地点的，工作屏位两侧及前后是要做措施的，这与远程维护是有矛盾的，个人认为只需为远程维护做出相应附加条款，用远动装置+IP地址取代工作地点，从而起到了同做措施一样的作用。这需要台账的内容更加详尽，每台装置的每个网卡的IP地址都需要记录，如果型号和IP地址输入不正确，将影响工作的正确性。

远程维护机房应该是专用的、独立的、有专人管理的且有严格的门禁制度的，不符合条件的、工作票有误的、工作内容不适用远程维护的及IP地址与装置不对应等情况都应拒绝其工作。进入机房工作的，应双人工作起到监护作用，工作前后都要做好备份并归档。机房应装设防火墙或者纵向加密装置，禁止远程终端连接Internet，远程维护终端应安装杀毒软件并且由专人定期更新毒库。维护人应使用专用U盘，远程维护终端只允许安装工作相关软件。每台远程终端应有相应电子日志，包括工作的人员，具体时间日期、修改内容及工作票号等。

3 结束语

其他几个变电站也做过同样的测试，无论是改造工程，还是日常维护，都是根据现场网络的实际情况搭建远程网络，从而实现远程维护的。远程维护的实践效果已经达到预期，毕竟时间是宝贵的而人力是有限的，快速且优化的工作方式也符合公司节约、高效的工作理念，随着技术的不断革新，制度的不断完善，远程维护会在未来的变电站维护工作中占有很大的比重。

作者简介

韩旭（1983-），本科，助理工程师，从事调度系统厂站端调试工作。

（收稿日期：2015-12-10）EA

（编辑：杨得润）