

综合自动化系统中网络技术的应用及故障分析

网络是现代变电站综合自动化系统的基础，它的结构相对简单合理，根据OSI模型可以清晰地分析和查找问题所在。网络的一些主要协议，如TCP、CDP、STP都是网络中重要的部分。TCP是传输的基础协议，CDP是思科Cisco自有知识产权的专利协议便于管理整个网络中的所有设备，其创建的网络设备拓扑对管理网络非常重要。STP是交换网中负责的冗余备份的协议，防止网络中出现因联络线故障引起的断网情况。OSI是一个通用的模型，厂家都在一个通用的平台上开发自己的通信模块，但是涉及到一些专利协议的兼容性确实有待测试。

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

TCP ·
STP ·
CDP ·

0 引言

在综合自动化变电站取代常规变电站不久，更加先进的数字化变电站的理念也被引入国内，无论是IEC 61850还是IEC 104都是依赖于网络架构，从二层交换到三层路由，从Ethernet到OSPF，网络技术已经渗透到变电站系统的每一行代码中。网络是基础也是推动力，这也促使调试人员更加全面、更加深入地理解和应用网络。网络技术的每次革新必将变电站系统推向又一个高度。新的技术的应用往往可以带来更高效的更稳定的网络环境。

1 综合自动化系统变电站网络组成

1.1 以太网和IEEE 802封装

以太网不是一种具体的网络，而是一种技术规范。以太网是当今现有局域网采用的最广泛的通信标准，具有开放

性好，兼容性好的特点。该标准定义了局域网（LAN）中采用的电缆类型和信号处理方法。以太网在互联设备之间以10 Mbit/s~10 Gbit/s的速率传送数据包，采用IEEE 802.3协议定义了物理层和数据链路层的MAC子层和LLC子层的作用与传输方式，采用CSMA/CD（载波监听多路访问/冲突检测）作为访问方式。综合自动化系统中网络103规约就是运行在这种结构上，在变电站站控层中保护装置、测控装置和其他自动装置都与主交换机相连接，以如图1所示的220 kV北寺站为例，两个主交换机构建两个互为备用的网络A和B，保护装置通过保护管理机与主交换机相连接；服务器、远动和五防装置等与主交换机直接连接；测控装置先与GIS室的交换机连接再通过光纤连接主交换机。

1.2 以太网结构

（1）总线结构

这种结构中所有装置都直接与总线相连接，所有装置都是等同的，无主次只有先后，各节点在接受信息时都进行地址检查，看是否与自己的地址相符，相符则接收网上信息。总线型机构特点：结构简单，所需的电缆较少、价格低，当需要增加节点时只需在总线末端增加装置即可。缺点是传输距离近、易衰减、不易隔离故障点和采用共享的访问机制易造成网络拥塞。北京地区只有南瑞继保RCS9600及RCS9700综合自动化系统是运行在这种架构之上的。

（2）星形结构

这种结构是用集线器或交换机作为

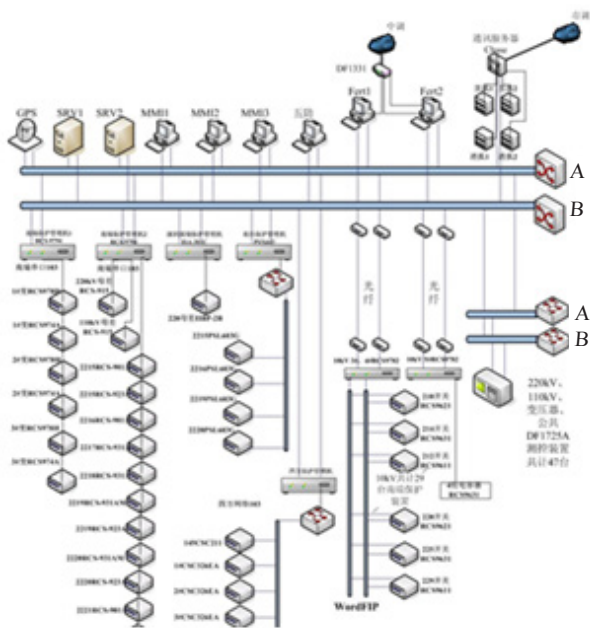


图1 220 kV北寺站网络配置图

网络的中央节点，网络中的每一台计算机都通过网卡连接到中央节点，计算机之间通过中央节点进行信息交换，各节点呈星状分布。其优点是管理方便、容易扩展和易排除故障。缺点是需要专用的网络设备作为网络的核心节点、需要更多的网线、对核心设备的可靠性要求较高。主流监控系统都是运行在星形结构之上的。

1.3 TCP和UDP协议

以太网在OSI模型中的工作范围是物理层和数据链路层，也就是处理数据流的部分，这部分功能具有差错控制功能。之前认为数据链路层只能检测错误不能改正的观点是不确切的，但实际上只能作简单的修改，注意只是简单的，而TCP协议可以完全修正。TCP和UDP协议工作在OSI模型的第四层也就是传输层，传输层的工作是将数据分段并重组成数据流，通过流量控制、面向对象的连接和窗口机制三部分将数据快速传输并检测修正错误。

TCP和UDP的应用对远动规约有很重要的意义，以前北京远动规约主要采用的是SC 1801规约和IEC 101规约，两者都是属于串口规约的范畴。SC 1801规约是按照RTU装置硬件的规格编写的，如一个逻辑RTU里只能定义16个槽，每个槽定义的类型可以是遥信或者是遥测、遥控，对于遥信

来说每个槽最多定义24个，遥测是12个，遥控是8个，而且传输遥测的准确度不高，无法显示小数点，主站需要在设置系数上乘以10的倍数才能显示。SC 1801的询问帧结构如表1所示。

表1 询问帧结构

RTU地址	DRF	字节数	字节数	LPC
-------	-----	-----	-----	-----

其中LPC是数据的校验位。IEC 101规约帧结构分为固定长度帧和可变长度帧，短帧的结构如表2所示。

表2 IEC 101规约短帧结构

启动字符 (10H)
控制域 (C)
链路地址域 (A)
帧校验和 (CS)
结束字符 (16H)

两种串口规约有一个特点就是最后一个字节都是校验位，校验的作用是对一帧里每个字节数值进行加运算，正确的有效，错误则数据无效。对于数据帧来说，校验是必须进行的步骤，因为通道误码或者丢帧造成的错误会对电力系统的正常运行造成影响，尤其是进行遥控时可能导致误控或者拒控。误上遥信信息也对系统运行有很大影响。但是规约带有校验，远动机CPU的负担就要大很多，占用必要的系统资源，随着网络技术的发展IEC 104已经取代前两种规约并广泛的应用于北京地区，智能站厂站端规约虽为IEC 61850，但与主站通信仍然采用IEC 104规约。IEC 104应用层与IEC 101完全一样，也就是规约里定义的ASDU和APCI，是IEC 101的网络版，而比起IEC 101扩展了类型标识，且传输介质改为网络，端口号默认2404，但采用东方电子DF1800系统的厂站在配置主站通道时主备通道端口号不能重复，主通道是标准的2404，备通道的端口号就要设置成2405。IEC 101有校验位，IEC 104校验则由OSI模型的传输层进行校验，101是非平衡式，104为平衡式。101的帧结构有2种，而104为1种，但有

3种格式U、S、I。IEC 104的帧结构中没有校验步骤，原因是TCP协议本身具有错误纠正功能，传输初始时利用三次握手机制保证信道的完整及可靠，然后应用层向TCP层发送用于网间传输的、用8位字节表示的数据流，然后TCP把数据流分割成适当长度的报文段（通常受该计算机连接的网路的数据链路层的最大传送单元（MTU）的限制）。之后TCP把结果包传给IP层，由它来通过网络将包传送给接收端实体的TCP层。TCP为了保证不发生丢包，就给每个字节一个序号，同时序号也保证了传送到接收端实体的包的按序接收。然后接收端实体对已成功收到的字节发回一个相应的确认（ACK）；如果发送端实体在合理的往返时延（RTT）内未收到确认，那么对应的数据（假设丢失了）将会被重传。TCP用一个校验和函数来检验数据是否有错误；在发送和接收时都要计算和校验，这样利用网络本身机制起到简化规约数据帧结构，也就简化了远动机与服务器的有限资源。

2 网络故障分析

110 kV肖庄站于2011年4月投运，投运几天后频繁出现厂站通道中断RTU停止的现象，重启远动后不久又出现中断现象。简单介绍肖庄站情况：肖庄站使用国电南京自动化股份有限公司的监控系统PS6000+，远动装置为该公司的PSX600U，厂站端站控层及间隔层使用网络IEC 103规约，与主站通信使用IEC 104规约，为标准的综合自动化站。主站端使用东方电子的DF8002系统，交换网使用思科（Cisco）6500系列交换机，通道为SDH 2M通道。

肖庄远动为主备模式，分别接调度数据A网B网，但PSX600U实现主备机功能要具有遥控回路，因为曾经出现过由于下装配置时出错导致远动切机时误掉负荷的严重后果，所以本站并没有设计此回路，也就是远动无法区分主备机。东方主站默认向活动的所有通道都发送报文，所以国电南京自动化股份有限公司两台远动都同时向主站发送变化数据及全数据，如果主站故障无法区分通道报文将导致数据异常，试用两个不同数据

源同时通过两台远动发送不同数据，主站正确显示，说明主站通道判别正确。试将其中一台远动关闭数时后问题依旧。通道中断时用PsxView软件通过主交换连接远动机均能登陆两台远动并查看数据，检查通信状态显示对上通道异常，ping对上网口显示超时，重启远动后网口正常。CPU板、对下网口均正常，问题应该出现在对上网卡上。用笔记本连通道交换机上截取网络数据帧，收到汇总数据如图2所示。



图2 网络数据帧汇总

截取时间为1 h53 min；数据包2 521个，如图3所示。抓包分析将近2 h，数据量2 000多个包，与网络动辄几十万的数据包相比，数据量可以忽略。根据图3证明，Cisco交换机开启了STP生成树协议，STP能有效解决交换网络中环网所导致的广播风暴问题。图3所示数据量很小，所以环网导致广播风暴的说法也不正确。从截获的数据来看，数据包主要包括三类，CDP、STP和104数据。问题应该出在CDP数据包上，在图3中标蓝的协议全称为思科发现协议（Cisco Discovery Protocol，

Protocol	% Packets	Packets	Bytes	Mbit/s
Frame	100.00%	2521	188878	0.000
Ethernet	100.00%	2521	188878	0.000
Logical-Link Control	51.21%	1291	91536	0.000
Spanning Tree Protocol	48.81%	1233	73980	0.000
Cisco Discovery Protocol	1.59%	40	15360	0.000
Internetwork Packet exchange	0.71%	18	2196	0.000
NetBIOS over IPX	0.60%	15	1470	0.000
Name Management Protocol over IPX	0.12%	3	726	0.000
SMB (Server Message Block Protocol)	0.12%	3	726	0.000
SMB MailSlot Protocol	0.12%	3	726	0.000
Microsoft Windows Browser Protocol	0.12%	3	726	0.000
Address Resolution Protocol	37.37%	942	58100	0.000
Data	5.88%	128	18482	0.000
Internet Protocol	6.35%	160	19950	0.000
User Datagram Protocol	6.35%	160	19950	0.000
NetBIOS Datagram Service	1.59%	40	8910	0.000
SMB (Server Message Block Protocol)	1.59%	40	8910	0.000
SMB MailSlot Protocol	1.59%	40	8910	0.000
Microsoft Windows Browser Protocol	1.59%	40	8910	0.000
NetBIOS Name Service	4.76%	120	11040	0.000

图3 某时段截取的数据帧

CDP)，CDP是Cisco的独有协议，作用是监视维护全网Cisco设备的状态的，收集网络中Cisco设备的软硬件信息，默认定时向全网发送组播。所以开始怀疑CDP与远动机存在不兼容问题，随后根

据CDP特性测试，将A通道与A远动机之间加入一个Dlink的8口交换机，然后截取数据包，并未发现CDP协议，在非Cisco的交换机上CDP协议不转发。监视一段时间，远动通道未中断。

3 结束语

正确理解变电站网络结构和掌握网络协议的工作原理是非常重要的，日常维护和基建改造工程中会遇到各式各样的问题，只有善于发现、总结才能使使自己的经验技术不断提高。

作者简介

韩旭（1983-），男，助理工程师，主要从事调度系统厂站端调试工作。

（收稿日期：2015-12-10）EA

（编辑：鞠佳）

（上接第596页）

上传，实现工作过程录制、两票现场编制、远程技术支持、现场信息数据采集各环节一体化控制与管理，不仅保证现场工作质量，也确保工作执行效率。

3）建立多样化数据采集与展示平台，无线智能终端对现场信息的采集，通过通信网络将采集到的文字、声音、图像和视频等信息实时上传到管理后台，通过后台管理系统将任务的各种现场信息以报告的方式进行汇总、整合，并将报告推送给相关业务系统和工作人员，使远端管理人员能够直观、清晰地掌握现场实际情况。

4）建立实时互动体系，现场人员可通过无线智能设备以文字、图片和声音等方式向非现场工作人员实时发送现场工作场景和执行任务过程中的问题，非现场人员也可通过后台管理系统或其他无线智能终端向现场工作人员发送作业任务指导和要求，实现工作现场与非现场实时交互信息，确保电力现场作业的安全性和规范性，确保实时监控管理现场作业。

5）建立数据共享，实现通用现场信息采集、任务管控一体化，项目通过数据接口方式与生产管理系统（即PMS）、营销SG186、应急指挥系统等管理系统数据共享，各相关系统可将计划作业任务或临时任务传送到项目，智能作业终端现场

采集的信息及任务执行情况可传送到相关系统，实现通用的信息采集及现场任务管理。

6 结束语

随着网络通信与信息技术的迅猛发展，更为先进的通信与信息技术将应用于无线智能终端设备，无线智能终端上交互的数据更为安全，认证更为完善和严密。

随着无线通信技术和智能终端技术的快速发展，以及电力企业信息化建设的不断发展，对移动智能应用的需求就会越来越迫切。通过移动应用将电网内部的业务信息化应用延伸至无线智能终端上，突破时间与空间的壁垒，只要是无线网络覆盖，企业内部所有人员在任何时间、任何地点都能掌握数据信息，以便于做出快速反应与决策，从而提升电力企业的运营管理能力。

作者简介

尹康（1981-），女，副教授级高级工程师，主要从事信息通信管理。

郭轶（1981-），女，高级项目经理，主要从事信息项目管理。

（收稿日期：2015-12-10）EA

（编辑：鞠佳）