新疆电力通信数据网规划方案初探

李亚平　　新疆电力公司电力调度中心

摘要：随着数据通信技术的发展，电力系统数据传输量需求的日益增大，建立统一的通信数据传输管理平台已成为数据通信发展的需要。文章根据新疆电力系统实际对新疆电力通信数据网规划方案进行初步探讨。

第 1 章 概述

新疆电力通信数据网建设基于新疆电力的现状和发展的需求，以电力企业数字化经营为核心、以通信、网络、数字化技术、软件技术为基础的电力企业数字化建设，使电力企业实现电力运营的现代化，按照建设“一强三优”现代公司的目标，为用户提供了方便、快捷的个性化服务。通信数据网络系统是其中一项基础工作，主要目的是建立基础网络平台。

第 2 章 建设原则

2.1 网络建设目标

电力通信数据网的建设目标为：在认真分析网络的当前需求，通过对网络的建设，构筑一个安全、可靠、先进、稳定的能够承载数据、语音、视频会议业务三网合一的多业务网络平台。

电力通信数据网网络建设完成后，满足开展下列业务的需要：

1、网络实现“电力调度业务”应用的承载。

2、广域网办公系统：在建立内部办公系统的基础上，文件传递、信息传递、多媒体信息交换、值班应急系统等机关办公功能。

3、视频会议系统：实现信息网内多点对多点的桌面视频会议系统。

4、IP 语音系统：实现信息网内的 IP 语音电话系统。

5、电子邮件系统：建设电子邮件消息传递系统。通过该系统实现全系统范围内的电子邮件邮递功能，便于信息传递和人员的沟通与交流。

6、信息发布：通过 WWW 服务器将公共信息发布到网上，实现信息共享，提高信息的利用率。

7、数据共享中心：将各部门可以共享的数据放在网络内部公共平台上，实现最大限度的数据共享；

8、安全体系：提供整个网络的安全手段，包括登录控制、身份认证、授权管理、安全审计、传输加密、数字签名、防范病毒、过程控制、文件保护、

安全岛技术、防火墙技术、桌面保护、物理隔离、定期漏洞检测、受攻击

报警、防辐射干扰等功能。

网络设计原则

为达到电力通信数据网建设的目标要求，在网络设计构建中，遵守以下原则：

高可靠性与安全性--网络系统的稳定可靠是应用系统正常运行的关键保证，在网络设计中选用高可靠性网络产品，合理设计网络架构，制订可靠的网络备份策略，保证网络具有故障自愈的能力，最大限度地支持网络各业务系统的正常运行。安全性：通过 VPN 网络、内外网物理隔离、加密、防火墙等技术，并制订统一的骨干网安全策略，整体考虑网络平台的安全性。

技术先进性和实用性--保证满足应用系统业务的同时，又要体现出网络系统的先进性。在网络设计中要把先进的技术与现有的成熟技术和标准结合起来，充分考虑到网络应用的现状和未来发展趋势。

高性能--骨干网络性能是整个网络良好运行的基础,设计中须保障网络及设备的高吞吐能力，保证各种信息（数据、语音、图象）的高质量传输，才能使网络不成为网络业务开展的瓶颈。

标准开放性--支持国际上通用标准的网络协议、国际标准的大型的动态路由协议等开放协议，有利于保证与其它网络(如公共数据网)之间的平滑连接互通，以及将来网络的扩展。

灵活性及可扩展性--根据未来业务的增长和变化，网络可以平滑地扩容和升级，并在扩容和升级过程中最大程度的减少对网络架构和现有设备的调整。

可管理性--对网络实行集中监测、分权管理，并统一分配带宽资源。选用先进的网络管理平台，具有对设备、端口等的管理、流量统计分析，及可提供故障自动报警。

经济性－－采用先进、合理、实用的技术规划，配置性能价格比最佳的设备，并利用现有的资源，保护已有投资。

为切实达到以上的网络设计原则，使网络系统具有良好的扩展性和灵活的接入能力，并易于管理，易于维护，在网络设计及构建中始终应遵循如下方面技术策略及原则。

统一标准、统一平台

网络的互联及互通关键是对相同标准的遵循，要实现网络业务能融合到一起，实现数据、语音、视频业务的融合，就必须统一标准。从开放性、发展性、成熟性等方面来看，只有 IP 技术才能成为统一平台网络构建的标准。而在具体实施中,必须统一规划 IP 地址及各种应用，采用开放的技术及国际标准，如路由协议、安全标准、接入标准和网络管理平台等，才能保证实现网络的统一，并确保网络的可扩展性。

第 3 章 网络规划

3.1 网络结构

新疆电力通信数据网建设规划的总体设计思想是以新疆电力系统的应用需求为指导，力求提供一个安全、先进、灵活，高带宽、高可靠性的多业务网络平台。使得用户能够基于这个平台，实现新疆电力系统应用的平稳承载和不同部门之间安全高速的数据共享，尽可能的简化办公流程，提高办公效率；并为今后新的业务发展，迅速推出相应的新业务打好良好的基础。

新疆电力通信数据网络采用层次化设计，从整体架构上来说，网络总体上可分为三层：核心层、汇聚层和接入层。

核心层负责整个网络的数据交换，设在省公司（核心节点），核心节点采用主备双高端核心路由器，接入核心节点用户业务的交换机采用三层高端核心交换机。

汇聚层负责整个网络的数据汇聚，包括乌鲁木齐、昌吉、吐鲁番、奎屯、准东、哈密、巴州、伊犁、和田、喀什、阿克苏、博州、塔城、阿勒泰等 14 地州地调中心，设备采用高性能的核心路由器，星型双归属结构连接至核心节点。地调接入用户业务的交换机采用三层交换机。

接入层负责整个网络的数据接入，包括各二级局点及变电所,设备采用高性能路由器，星型双归属结构连接至地调中心节点。二级局点及变电所接入用户业务的交换机采用高性能的智能交换机。

本网络的建设相对独立，也可与国家电力数据网络设在各省的骨干节点设备背靠背连接接入国家电力通信数据网络中。设备网管软件，选用集中网管的方式，建设 1 个全网网管中心（省电力公司）,全网采用 MPLS VPN 技术组网，为了方便业务管理，除了普通的 IP 设备网管软件外，还选用 MPLS VPN Manager 网管，负责各个 VPN 业务的管理。

整体网络连接覆盖中心、各个分中心、各个数据采集点的信息点，信息网络通过出口路由器、防火墙连接互联网设备。

3.2 线路及带宽选择

接入层：各个接入层交换机使用超五类 UTP 双绞线 100M 连接到各个办公用 PC 机；接入层交换机使用光纤 100M/1000M 上联到核心/汇聚层交换机,根据业务量的实际情况选择。

核心/汇接层： 各个核心/汇聚层交换机使用光纤 100M/1000M 下联到接入层交换机；使用双绞线 100M/1000M 连接各数据服务器、路由器。

广域网：广域网主用线路的 SDH 2M 数字线路，备用线路采用运营商 2M 及 PSTN 拨号。

3.3 IP 地址规划

新疆电力通信数据网 IP 地址的分配，应遵循电力上级部门关于电力数据网 IP 地址规划的相关规定。在项目的技术实施规划 IP 地址规划中，初步按 5 个 B 类地址进行分配。

1、按照地域规划，每个地市一个独立的网段；这种规划适合业务种类单一的情况，管理方便。

2、按照业务规划，每种业务一个网段，全疆所有的地市同一业务使用同一网段；这种规划适合业务之间互访的控制。

在新疆电力通信数据网项目中，选用按照业务和地域混合编址的方法，整网采用 5 个 B 类地址，VPN1－VPN4 各占用一个 B 类地址，各个地市下的每个 VPN 占用此 VPN 的若干个 C 类地址。

3.4 路由协议

对于骨干层 MPLS 域，需要某种 IGP 协议与 MBGP 结合应用，其中 MBGP 主要完成私网路由标签分配、各私网路由在“公网”传递等作用，没有其他的协议可以替代。各地市 CE 之间的 VPN 路由的传递、VPN 路由标签的分发，都是通过骨干区域 MP-BGP 协议的扩展属性实现的。

对于 IGP 协议，采用 OSPF，因为 OSPF 的适应性好，功能完善，当核心层设备在 20 台以内的时候，只运行一个骨干域“0”，这样网络规划简单、维护方便，并且有利于今后骨干层网络的扩展。

对于 PE 与 CE 互联，采用的路由协议有静态路由、直连路由、RIP 和 BGP 等多种路由协议。具体使用那种路由协议要根据情况而定。

综上，建议的路由协议类型就是：骨干层 MBGP＋OSPF、PE 与 CE 互联采用静态、直连路由。这样对整个网络中的设备要求不是太高，并且很好的实现了 MPLS-VPN。

3.4.1 BGP 协议规划

1、AS 号

采用私有的 AS 号，按照省公司的统一规划。

路由反射器

骨干的路由器运行在同一个 BGP 的 AS 中，按照 BGP 协议的要求，所有这些路由器必须保证是全连通的，即：任意两台路由器之间都必须配置邻居关系。这样会导致 N 平方问题，为了解决这个问题，必须使用 BGP 反射器技术。

由于网络规模较大，所以使用二级路由反射。

第一级路由反射：

路由反射器 RR	客户机
省中心主路由器	各地州路由器
省中心备份路由器	各地州路由器

其中：两台 RR 之间配置普通邻居关系，配置中的 cluster ID 使用两台 RR 中主用的路由器的 router id。

第二级路由反射：

各地州核心路由器，都作为本市路由器的路由反射器。

3、路由的引入

在各地市的 PE 设备上，BGP 的 vpnv4 地址族中，不需要引入其他路由协议；BGP 的 IPV4 地址族中，通过 redistribute 命令引入本 VPN 的直连和静态路由。

3.4.2 IGP 协议规划

在 MPLS 骨干区域内的 IGP 采用动态的、基于链路状态的 OSPF 协议。由于整个新疆电力通信数据网设备数量较多，为了保证整网的性能，考虑 OSPF 的分域规划，可以按地市把几个地调分到一个子域中，也可以按照每个地市单独分配一个区域，考虑到新疆电力通信数据网的实际情况和未来扩容的需要，采用每个地调分配一个子域的原则。由于网络拓扑结构设计的原因，每台设备都有双归属链路，因此这样导致了每个 OSPF 子区域都有多个 ABR，在有多个 ABR 的子域上采用路由汇聚要保证这些子域上 ABR 的路由汇聚配置相同，不然会由于错误配置的原因导致网络故障。

区域的划分

OSPF 的区域概念是基于路由器接口的，因此将新疆电力通信数据网中心两台核心路由器和各地州核心路由器划分到一个 AREA 0。

各地州核心路由器与下带的市县分别划分到非 0 区域，按各地州的区号来划分：

如果有新的地调节点加入，则按新的子区域号来规划。如果有新的变电站需要加入，则按照新加入节点上连到具体的 2 个地州区域号来规划。为避免路由环路，在 PE 上不通过 OSPF 发布缺省路由。

路由的引入

在各地的 PE 设备上，通过 Network 命令将 PE 设备的 loopback 地址和互连端口地址引入到 OSPF 协议中去。为了便于控制路由的规模，不采用 redistribute 命令引入静态或其他协议的路由。

对于双链路设备的两条上行链路采用如下原则：汇聚层到核心层的两条链路采用负载分担的方式；接入层到汇聚层的链路使用主备切换的方式。对于具体采用哪种方式可以通过在路由器接口模式下通过 ospf cost 命令来控制,对于汇聚层到核心层的接口,设置相同的 Cost 值，采用负载均衡的方式，对于汇聚层到接入层的接口，设置不同的 Cost（一大一小，cost 小的为主链路，cost 大的为备用链路），采用负载分担的方式。

3.4.3 静态、直连路由规划

部分的 CE（接入层）采用二层交换机，这样直接在在 PE 上配置各业务的直连网段。

部分的 CE 采用三层交换机（核心层和汇聚层），这样就在 PE 和 CE 之间运行静态路由。在 PE 上配置网段为本地，下一跳指向 CE 的静态路由，然后引入到 MP-BGP 中，发布到其他地市；同时，在 CE 上配置目的网段为其他地市，下一跳为 PE 的静态路由。

3.6 MPLS VPN 规划

划分为 4 类 VPN：（规划按照数字越小，优先级越高）

VPN1：

实时监控系统（EMS、变电站计算机监控系统、水电厂计算机监控系统、火电厂计算机监控系统等）或具有实时监控功能的系统其监控功能部分（AGC 等），数据实时性为秒级，网络系统外部边界的通信均经由电力调度数据网的实时虚拟专用网（VPN）。功角测量、安全自动装置控制系统等。（通信对象是电厂、地调和变电站，数据交换频繁，数据实时要求高，数据量不大，优先级为 1）。

VPN2：

水调自动化系统（通信对象是数量不多的水电厂，数据交换频繁，数据实时要求不是太高，数据量小，优先级为 2）及未来的电力市场技术支持系统（通信对象是变电站、地调和电厂，数据交换不频繁，数据实时性要求不高，数据量大，优先级为 2）。

VPN3：

继电保护故障录波远传与信息管理系统、DTS（调度员培训仿真）系统，电能量计量系统（优先级为 3）

VPN4：

同步时钟系统、通信监控系统（通信对象变电站、地调和电厂，数据交换频繁，数据实时性要求高，数据量小，优先级为 4）

3.6.1 VRF 规则

VRF 对应一个 VPN，

3.6.2 RD 规则

使用 16 bits：32 bits 格式，分配规则为 『AS 号：VPN 类别』。

3.6.3 Route-Target 规则

通过配置 VRF（路由转发实例）的 target 属性，可以实现不同业务的 VPN。不同路由器通过 target 相关联而组成可以互相访问的集合， VPN 的成员关系是通过路由所携带的 route target 属性来获得的。不同 CE 通过 PE 配置的 VRF 里的 Target 实现互访与隔离，从而组成不同的 VPN。

使用 16 bits：32 bits 格式。其中 AS 号统一使用骨干 AS 的 64600，如果各业务间没有互访的需求，就将 route-target 的 export 和 import 设为一致。

3.6.4 VPN 的互通和隔离

接入层本地 VPN 接入 CE 设备采用的是 2 层交换机，因此不同 VPN 可以通过 2 层 VLAN 进行本地隔离，在 MPLS PE 设备上为每个 VPN 维护一张单独的路由表，防止了不同 VPN 路由的相互泄漏，同一 VPN 的各个 site 可以互通，不同 VPN site 之间相互隔离。但汇聚和核心层 VPN 介入 CE 设备采用的是三层交换机，在三层交换机上配置 VLAN 虚接口后，各个 VLAN 是互通的，为了使得各个 VPN 在本地隔离，因此在汇聚层和骨干层的本地接入交换机上需要启用 ACL（访问控制列表），禁止几个本地 VLAN(VPN)之间的互访。

对于个别级别高的主机（信息点、业务系统），需要访问任何一个 VPN，可以通过设置一个 Super VPN 来解决，通过控制 Route-Target 属性，使其全部接受和发布全部 VPN 的路由，这样使其可以访问全部的 VPN（业务系统）。

3.6.5 不同 VPN 之间互通的配置规划

不同的 VPN 之间是严禁互相访问的，但考虑到网络和业务的扩展性，会存在不同的 VPN 之间互相访问的需求。由于 MPLS/VPN 的互访是通过 RT 来控制的，只需要在现在配置的 RT 基础上进行简单的修改即可。

3.7 网络的备份和流量分担

3.7.1 网络的备份

网络备份可以同时通过两种方式实现：

1、通过合理的网络规划设计，实现物理链路与物理设备的备份。中心的两台汇聚节点是主备和负荷分担的，在正常工作的情况下，共同分担整个网络的流量，当其中一个失效后，另外一台设备能够承担起所有的流量，保证业务的正常运行；各地市到中心节点的两条广域网链路也是主备的，在主用链路中断的情况下，业务可以通过备用链路传输。

2、应用动态路由协议，做到网络的自动备份。OSPF 和 BGP 协议，均可以自动地发现两个网络节点之间的迂回路由，并在主用路由不可用时而自动使用备份链路。并且可以通过在路由器上加入策略，控制数据的流向。

3.7.2 流量的分担

每个地市到中心节点都由两条主备链路，可以通过设置不同的 Cost 值，实现部分节点的主链路汇聚到 NE16-1，而另外的节点的主链路汇聚到 NE16-2，从而达到负荷分担的目的，避免网络流量不均衡。

3.8 网络安全

网络安全技术包括：防火墙，身份认证，入侵检测和漏洞扫描，VPN 安全通道，安全策略管理和防病毒。

1、**防火墙技术：**一般用于内部网络和外部网络交界处的安全，主要包括因特网出口处以及内部单位之间的安全，Internet 出口处的安全措施一般采取加防火墙的方法，实施地址转换，

隐藏内部网络结构，限制外部用户访问内部网络的权限和可到达的区域等防火墙目前包括硬件防火墙和软件防火墙。

2、**身份认证**：包括用户身份鉴别、用户访问权限授权、用户访问资源计帐。

3、**漏洞扫描**：检查安全基础设施的有效性，包括新系统安装检查，发现恶意入侵行为的措施等。安全扫描工具主要用于主动的发现内部网络上所有设备存在的安全漏洞，可以提示用户进行相应的措施加以解决。

4、**安全通道**：指数据的保密性，涉及数据在传输过程特别是在公网信道上不被窃取，保证数据的目标用户可以容易解读加密的数据。包括有硬件信道加密以及二层 VPN、三层 VPN 等技术。

5、**防病毒**：建立网络病毒检测、预防和治理相结合的完善防病毒体系。

6、**安全策略**：主要由用户根据网络内部不同部分的重要性的差别，以及功能差别等因素，定制处不同的安全策略,包括 Internet 网络用户对内部网络的访问以及内部用户的不同的访问权限等，安全策略的制定将直接影响到网络的安全性能。

3.9 系统网管需求

新疆电力通信数据网将在新疆电网调度中心建立一套全省网管中心系统（对这个网络的设备进行设备管理），全省网管中心全面负责全省骨干网的管理，能采集全省骨干网上的全部信息，并能对全省骨干网中的所有设备进行监视和控制，包括网络中 P、PE 设备的管理。根据网络规模的要求，采用华为 Quidview 网管系统进行网络管理。由于调度数据网络本身的调度数据流量和网管数据流量较少，所以采用带内网管方式。网管要管理到包括接入层 2 层交换机在内的 CE 设备，在建立设备网管的同时建立一套 VPN 网管。设备网管按照实际需求的 license 配置，VPN 网管按照按照实际需求的 license 配置。

3.9.1 对 PE 与 CE 设备统一网管

要求设备网管不仅能够管理所有的 PE 设备，而且还能够同时管理 VPN 中的 CE 设备，为了安全考虑，要求网管工作站仅对 P、PE、CE 设备可见，对 VPN 内的用户设备是不可见的。

由于 CE 与 PE 之间的 link 链路地址属于 VPN 内部的地址，无法发布到公网（这里的公网是指 PE 和 P 设备使用的地址空间），所以为了实现上述需求，必须为每一台 CE 设备增加一条与 PE 设备之间的公网 LINK 链路（出于节约物理链路的考虑，可以在路由器上使用子接口功能，在 L2 或 L3 上使用 VLAN Trunk 功能）。每台 CE 设备的 loopback 地址（如果是 L2 则是管理地址）也配置为公网地址。

网管工作站同样采用公网的地址空间，直接连接在核心路由器的 FE 接口上。规划为了便于统一管理，设备网管系统采用统一的规划的 IP 地址段。

3.9.2 路由器相关参数设置

SNMP 相关版本设置

SNMP 协议的相应版本，统一使用 SNMP V1 版本。

Trap 报文相关属性设置

允许被管理设备主动向网管工作站发送 Trap 报文。

设置 Trap 目标工作站的地址为网管工作站的地址。

设置被管理设备发送 Trap 的源地址为该设备的 loopback 地址。

4.结束语

电力通信数据网络是一个集数据、话音、多媒体和视频图象于一体的综合数据网络。该网络配置了包括省电力公司及所辖地市供电局在内的骨干交换节点和省内主要发电厂和所有变电站的边缘交换节点。当前，电力通信业务正在由以话音通信为主逐步向以数据通信为主转变。在各种数据业务中，IP 协议占据了主导地位，随着电力市场化的进一步发展，基于 Internet 的具有开放性和安全可靠性的信息传输平台将成为电力数据网络发展的必然趋势。