DOI：10. 16516/j. gedi. issn2095-8676. 2015. 03. 009

电力综合数据网 VPN 划分方案探讨

林志达[1]，魏畅[2]，程小蓉[2]
（1. 中国南方电网有限责任公司，广州 510623；2. 中国能源建设集团广东省电力设计研究院有限公司，广州 510663）

摘要：对电力系统综合数据网网络现状及南方五省 VPN 划分进行了简要介绍，并针对现状提出问题。对现有 VPN 技术进行分析比对，选择适合电网综合数据网特征及需求的技术。根据问题及技术现状，对未来电网 VPN 建设模型进行研究分析，提出三种建设模型，选择最适合电网特性的 VPN 建设模型，以便实现在复杂的网络运维管理环境下，对业务隔离性和安全性的充分保障。

关键词：VPN 应用模型；MPLS VPN；QOS
中图分类号：TP393. 08 **文献标志码**：A **文章编号**：2095-8676(2015)03-0047-04

VPN Research Application Model of Power Systems

LIN Zhida[1], WEI Chang[2], CHENG Xiaorong[2]
(1. China Southern Power Grid Co., Ltd., Guangzhou 510623, China;
2. China Energy Engineering Group Guangdong Electric Power Design Institute Co., Ltd., Guangzhou 510663, China)

Abstract: This paper gives a brief introduction of the integrated power system data network status and the VPN division of the five southern provinces, and proposes the question in view of the present situation. By analysizing the existing VPN technology, we can choose suitable for the characteristics and demands of network integrated data grid technology. According to the problems and technical present situation, this paper researches the future power grid VPN construction model, and puts forward three kinds of development model. And selection model VPN is most suitable for the characteristics of power grid construction, network operation and maintenance management of the environment in order to complex, to fully guarantee the service isolation and safety.

Key words: VPN application model; MPLS VPN; QOS

随着电力系统管理信息类业务对数据通信方式的应用不断深化，各类信息化业务等越来越依赖于数据通信网络承载，且对于数据通信网络的功能和性能提出了更高的要求，网络需要满足业务系统的隔离性、可靠性、QOS 和安全管理等多方面的需求。

本文将针对电力系统数据网络在 VPN 技术选择和 VPN 划分方面的技术路线，开展有针对性的理论研究。

1 网络现状及问题分析

为方便展开研究，下面以某电力系统综合数据网为例建立模型。

收稿日期：2015-06-01

作者简介：林志达(1983)，男，广东梅州人，工程师，学士，主要从事信息网络和系统建设工作(e-mail)linzd@csg. cn。

该电力系统综合数据网架构分为网省地三层，各省之间综合数据网不直接互联，而是分别与网综合数据网互联。网省两级综合数据网的 VPN 划分情况完全不一致，网省根据自身实际情况，为满足各自业务需求，分别进行了 VPN 划分。其中网综合数据网现划分为两个 VPN：综合 VPN 和预留 VPN。各类需要实现网省互通的业务均汇集到网省综合数据网之间的防火墙终结，再通过网省综合数据网互联通道与网综合数据网的综合 VPN 互通，实现网省 VPN 之间的互联[1-2]。具体现状模型图如图 1 所示。

该网络模型存在一个很严重的问题：VPN 划分没有统一规划，网省 VPN 划分各自为政，没有统一的技术思路或者政策手段，造成在各级网络边缘需要采用 VPN 路由互导、路由过滤及接口合并等多种复杂的技术措施，使用不便。同时各类业务系

统没有一致规定的 VPN 承载方式，造成业务间通信存在较大问题。

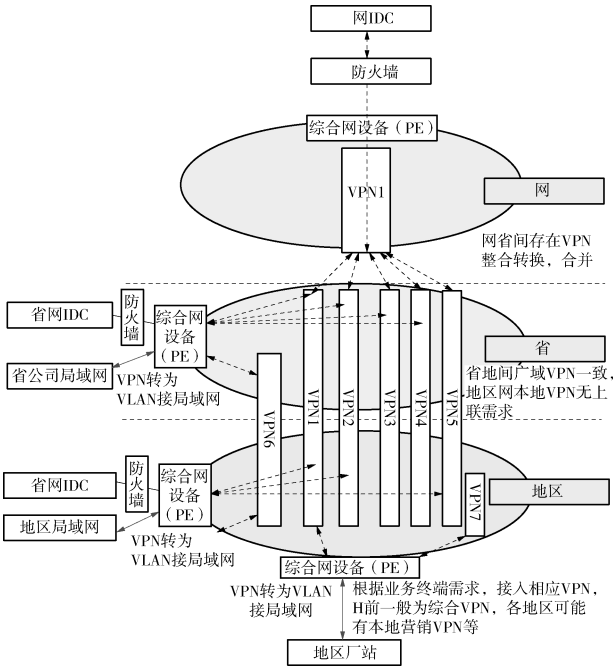

图 1 综合数据网 VPN 现状模型图

Fig. 1 Integrated Data Network Status of VPN Model Diagram

2 VPN 技术分析

目前在数据网络中为充分利用物理网络资源，提高设备使用效率，同时又实现业务隔离传输和安全保障，一般采用 VPN 技术实现在同一个物理数据网络中构建多个逻辑虚拟的数据网络即 VPN（虚拟专用网络）[3]，当前可以采用的各种 VPN 技术分析如表 1 所示。

MPLS VPN 技术是电力通信 IP 数据网的主流技术，MPLS VPN 是一种基于 MPLS 技术的 IP-VPN，是在网络路由和交换设备上应用 MPLS 技术，简化核心路由器的路由选择方式，利用结合传统路由技术的标记交换实现的 IP 虚拟专用网络（IP VPN），可用来构造宽带的 Intranet、Extranet，满足多种灵活的业务需求[4]。采用 MPLS VPN 技术可以把现有的 IP 网络分解成逻辑上隔离的网络，这种逻辑上隔离的网络的应用可以是千变万化的：可以为各种业务提供不同性能的 VPN 业务[5-6]。目前主流厂商全系列的路由器都支持端到端 MPLS 技术。

综上所述，采用 MPLS 3 层 VPN 技术比较适合电力系统综合数据网需求。

表 1 VPN 技术分析对比表

Table 1 Analysis of the Contrast of VPN Technology

技术对比	技术实现	隔离性	灵活性
MPLS 三层 VPN	利用标签技术，对数据包进行标记	二层及三层间的标签（LABLE）隔离，逻辑隔离，相对其它 VPN 技术，隔离性较强	目前的三层 MPLS VPN 可通过 RT 及 Community 实现多种逻辑拓扑，灵活度最高
MPLS 二层 VPN	利用标签技术，标记二层信息，端口号，ATM PVC 等	二层及三层间的标签（LABLE）隔离，逻辑隔离，相对其它 VPN 技术，隔离性较强	可通过 RT 及 Community 实现多种逻辑拓扑，灵活度较高，但受到二层技术本生的生成树等方面限制
QinQ VLAN	多层 802.1Q 标签嵌套，将本地 VLAN 封装进广域网 VLAN	二层隔离，在逻辑通道隔离技术层面，隔离性最强	仅能实现点对点、点对多点，灵活度受限
IP SEC VPN	通过两端加密解密，修改三层 IP 包头，对数据包进行封装	与普通数据包一起传输，仅通过加密实现隔离，相对隔离性一般	仅能实现点对点、点对多点，灵活度受限
SSL VPN	基于应用层的安全套接层协议（Security Socket Layer-SSL），在用户终端和服务器间建立链接，形成应用层隧道，逻辑上的 VPN	与普通数据包一起传输，仅通过加密实现隔离，相对隔离性一般	仅能实现点对点、点对多点，灵活度受限
L2TP 隧道	基于拨号技术的隧道协议，可建立点对多点隧道，形成 VPN，技术相对较老，一般用于运营商的远程拨号用户接入。	与普通数据包一起传输，仅通过加密实现隔离，相对隔离性一般	仅能实现点对点、点对多点，灵活度受限

3 VPN 应用模型分析及建议

3.1 VPN 划分方式研究

1）方案一：根据业务需求划分

根据业务要求，每个重要业务单独一个 VPN。在网省间互联节点的省网侧进行 VPN 归集整合，以适应网层面对 VPN 的划分。具体示意图如图 2 所示。

2）方案二：根据业务性质划分

根据业务性质或需求，同一类安全等级，或类似流量模型的业务划分为一个 VPN[7]。即在网省间

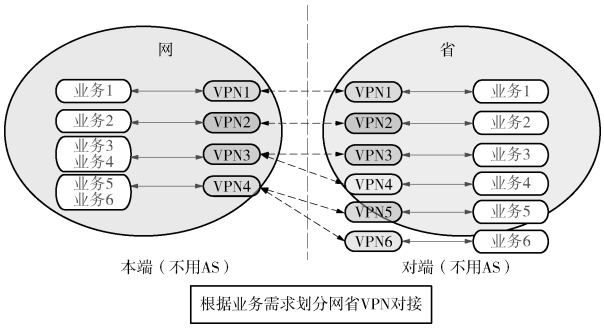

图 2　VPN 划分方式一示意图

Fig. 2　A Schematic Diagram of VPN Division 1

互联节点的上级网络侧进行 VPN 归集整合，以对应网 VPN 的划分。具体示意图如图 3 所示。

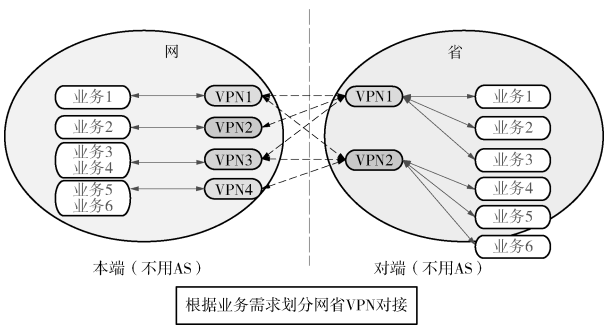

图 3　VPN 划分方式二示意图

Fig. 3　A Schematic Diagram of VPN Division 2

3）方案三：混合传输不划分 VPN

不划分 VPN，在综合数据网上各种业务均通过同一个 VPN 承载。即在网省间互联节点的省网侧进行业务整理，以对应网 VPN 的划分。具体示意图如图 4 所示。

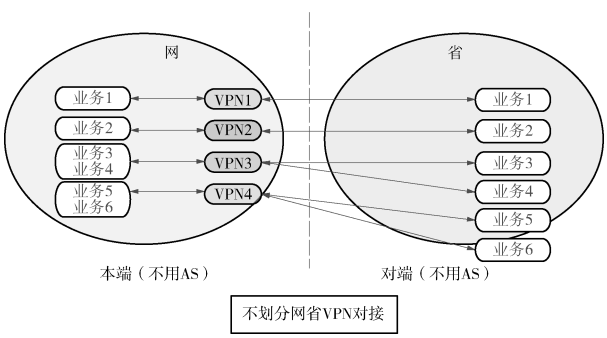

图 4　VPN 划分方式三示意图

Fig. 4　A Schematic Diagram of VPN Division 3

4）比较分析及建议

下面将对以上方案从业务分类、安全隔离保障、后续扩展能力、维护难度。具体如表 2 所示。

表 2　VPN 划分方式方案比较

Table 2　Scheme Comparison of VPN Division

问题	根据业务需求划分 VPN	根据业务性质划分 VPN	混合传输不划分 VPN
业务分类	清晰	相对混合传输清晰	不清晰
安全	在 VPN 使用模式清晰的情况下，可完全实现安全隔离保障	同一性质或者信息安全等级的业务同 VPN，可达到安全隔离保障	无隔离，各类业务在广域网中混合传输，自由互访，仅在两端节点可通过安全设备进行端点控制．安全隔离性低
后续扩展能力	随着业务增加，VPN 数量同步增加，对于电力系统的业务流量模型而言，意味着需要更多跨 VPN 间访问的策略设置，维护和管理难度呈指数增加。	随业务增加，根据业务性质放到不同 VPN 中，由于事先已经进行了 IP 地址分类，其维护管理难度增加不大，扩展能力较优	由于无 VPN 限制，各业务间可以自由互通，相对扩展能力最优
维护难度	VPN 数量的增加提高了维护难度，但上下级网络互联节点的维护难度无增加	VPN 数量较少，且可相对固定，维护难度较按照业务需求划分较低，但在网络内部是难于不划分 VPN 的方式．	1）本网络内部相对简单；2）需要上下级网络跨网互联的业务，维护较为困难，在保障路由可达的同时，还要确保不因为本网络内部的 VPN 混合互通影响上级网络的 VPN 隔离，需要在网络边缘设置防火墙，以大量 ACL 进行控制。

综上比较，采用以业务性质划分 VPN 的方式进行网主干网的 VPN 划分，同时进行对下级省网和地区网的 VPN 划分规范化工作。

3.2　VPN 分类研究

综合前述，以采用以业务性质的分类为前提，从划分操作的管理实现难易程度考虑，根据数据流向并综合等级保护和服务质量要求对 VPN 进行分类，具体分类情况如表 3 所示。

表 3　VPN 分类

Table 3　VPN Classification

VPN 序号	综合 QOS 及等保要求划分	推荐业务	MPLS EXP 位	802.1P
VPN 1	综合承载 VPN	各类管理信息业务等	4	4
VPN 2	IDC VPN	IDC 服务器之间互相访问	5	5
VPN 3	QOS 优先保障 VPN	语音视频等	7	7
VPN 4	容灾备份 VPN	容灾备份等大颗粒业务	2	2
VPN 5	互联网统一出口 VPN	承载互联网统一出口业务	3	3

3.3 VPN 应用模型结论

根据以上分析，得出如图5所示模型。

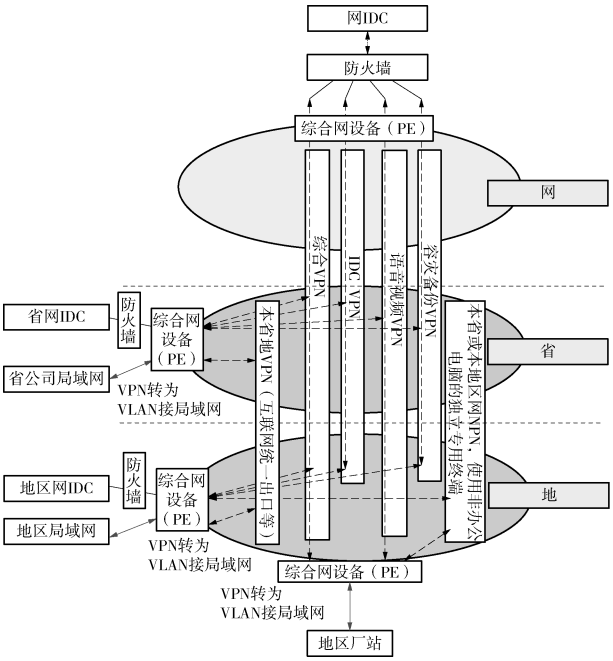

图5 VPN 应用模型示意图

Fig. 5 Shematic Diagram of the VPN Application Model

如图所示，综合 VPN 和语音视频 VPN 的最终末梢至地区厂站，IDC VPN 和容灾备份 VPN 末梢至地区供电局。

本省或者本地区内无需全网贯通的业务可以各自网络分别存在。

4 结论

本文建议在电力系统综合数据网采用 MPLS VPN 技术进行业务分类隔离和传输，在电力综合数据网中的 VPN 应用模型应采用以业务性质划分 VPN 的方式，并具有网省地三级一致联通、仅省地区网内部联通两种 VPN。综合数据网 VPN 划分方式应综合考虑业务安全等级保护要求和 QOS 保障要求进行划分和设置，在控制网络运维管理复杂度的情况下，充分保障承载业务的隔离性和安全性。

参考文献：

[1] 王占京，张丽诺，雷波．VPN 网络技术与业务应用[M]．北京：国防工业出版社，2012.
WANG Zhanjing，ZHANG Linuo，LEI Bo. VPN Technology and Application[M]. Beijing：National Defence Industry Press，2012.

[2] 李进印．MP-BGP 协议在 MPLS-VPN 中的应用浅析[J]．科技资讯，2009(1)：18.
LI Jinyin. The MP-BGP Protocol in MPLS-VPN Application Brief Analysis[J]. Science & Technology Information，2009，(1)：24-25.

[3] 韩海雯，张潇元．BGP/MPLS VPN 工作机制剖析[J]．现代计算机，2007(9)：58-61.
HAN Haiwen，ZHANG Xiaoyuan. Analysis of the Mechanism on BGP/MPLS VPN[J]. Modern Computer，2007(9)：58-61.

[4] 洪必海．电力调度数据网改造方法[J]．科技创新与应用，2014(33)：199.
HONG BiHai. The Transform Method for Electric Dispatching Networks[J]. Technology Innovation and Application，2014(33)：199.

[5] 张学林．MPLS VPN 技术在大客户组网业务中的应用[J]．中国新通信，2014(22)：82-83.
ZHANG Xuelin. The Application of MPLS VPN Technology in Major Customer Networking Service[J]. China New Telecommunications. 2014(22)：82-83.

[6] 贺文华，刘慧，贺劲松．IPSec VPN 与 SSL VPN 的比较研究．电子商务[J]．2014(11)：70-71.
HE Wenhua，LIU Hui，He Jinsong. The Comparison of IPSec VPN and SSL VPN. E-Business Journal[J]. 2014(11)：70-71.

[7] 孟繁华．VPN 技术在计算机网络中的应用[J]．电子技术与软件工程，2014(22)：50.
MENG Fanhua. The Application of VPN in Computational Networks[J]. Electric Technology and Software Engineering，2014(22)：50.

（责任编辑 黄肇和）