网络详细设计及实施方案

目　　录

1. 网络总体方案设计

1.1. 概述

数据网已经完成了福建电力调度数据网络（三级网）（以下简称三级网）的建设。核心节点为省调通中心，配置了两台 Cisco 7513 路由器，其中一台 Cisco 7513 用于直调电厂的接入，一台用于与地调的接入，调通中心和地调间以 4*2M SDH 光纤通道形成环网，部分地调与中调还有 2M 备用通道连接，形成环形＋星形的网络拓扑结构。配置了两台 Cisco Catalyst3550-24 交换机，分别作为两个 VPN 的接入交换机。

骨干节点由福州、厦门、泉州、漳州、南平、三明、龙岩、宁德、莆田等 9 个地调中心节点组成，各节点分别配置一台 Cisco 7206 路由器，2 台 Cisco Catalyst3550-24 交换机,两台交换机分别作为两个 VPN 的接入交换机。

接入层节点由各地的 220KV 变电站组成,这些节点就近接入所属的地调中心，每个节点配置一台 Cisco 2650 路由器，同时在 Cisco 2650 路由器上配置 1 块 16 端口局域网模块作为内置网络交换机，将 16 端口局域网模块分为两个 VLAN，分别用于本地两个 VPN 业务的接入。

福建电力调度专用数据网在结构上分为四层：

核心层：核心节点由调通中心和备份节点组成本次项目，本次项目对原有两台 cisco7513 路由器上增加 E1 卡；在三级数据网已建成的网络管理系统基础上增加 MPLS VPN 管理模块。

骨干层：骨干层节点由福州、莆田、泉州、厦门、漳州、龙岩、三明、南平和宁德 9 个地调组成，本次项目对骨干节点增加一台备份设备和网管工作站。

汇聚层：汇聚层由集控站和各地的县调组成。本次对已接入网络的集控站进行改造，将县调接入到网络。本期主要实施 45 个集控站、4 个二级局、4 个二级局下属的集控站和 18 个县调。每个汇聚点配置 2 套设备.

接入层:接入层由各地的 110KV 变电站组成。本期新上接入层节点共 118 个，每个接入点配置 2 套设备。

本工程网络采用 IP 路由交换设备组网，采用 IP over SDH 的技术体制。

本网络中传输的业务按安全等级进行分类，在全网实现 MPLS/VPN。网络中所有路由设备（包括接入路由器）均具有 MPLS PE 的功能。

1.2. 设计原则

在网络的拓扑设计中，我们遵守了如下原则。

- **拓扑可靠性：**

1) 在各网络的拓扑设计中应遵循 N-1 的电路可靠性和 N-1 的节点可靠性原则。
2) N-1 的电路可靠性：拓扑中去掉任何 1 条连线（电路），不影响节点的连通性。这就要求每个节点至少有两条不相关的电路与其他节点相连。
3) N-1 的节点可靠性：拓扑中去掉任何 1 个节点，不影响其他节点的连通性。如福州骨干节点中的一台发生故障不影响其他节点的连通。

- **双出口：**

每个节点到上一级节点有两个出口，两个出口尽可能应位于不同的地理位置（至少不在一个机房内），防止因外部原因（如停电）造成两出口同时失效。两出口的外联电路中，至少有两条没有相关性（两条链路不在同一条光缆上传输）。

- **局域网两点接入：**

福建电力调度数据网为了确保调度生产业务的可靠性，在所有节点的局域网通过两台设备分别连接到本地的路由器设备上。通过多台设备接入保证了业务不会因一个节点故障而失去和网络的连通。

- **流量（traffic）优化**

根据网络的流量和流向合理配置电路及其带宽。网络流量分布均匀，各电路带宽得到较充分的利用，不存在网络带宽瓶颈。应适度考虑在”N-1”的情况下网络的流量。

- **经济性**

在保证可靠和畅通的前提下，网络电路的数量、总里程和带宽应尽可能减小，以降低网络的运行费用。

- **扩展性**

网络电路和节点的增加、减少以及修改应不影响网络的总体拓扑。

1.3. 拓扑设计

电力能源是国家经济发展的基础，而电力调度数据网的可靠运行则是电力安全生产的保障。特别是随着经济发展、社会信息化的发展，整个社会对电力的依赖越来越重，一旦能源中断，将会使整个经济环境陷于瘫痪，引起巨大的经济损失和严重的后果。因此在电力调度数据网的设计实施中必须对网络的可靠性进行详尽的考虑和设计。

网络结构的可靠性，主要是对网络互联通道的备份考虑和设计，通过备份线路及设备的备份，保证任何时刻、任何节点之间都有可达的路由。

拓扑设计分为原有三级网拓扑设计和四级网拓扑设计。

1.3.1. 三级网结构和现状分析

目前福建电力调度数据网中每个地调骨干节点已用一台 Cisco 7206 路由器，与省电力调通中心的 Cisco 7513 路由器之间主要通过 4×2Mbps 广域网链路形成骨干层环网。同时，为提高可靠性，省电力调通中心又与部分地调之间又通过 2Mbps 广域网链路形成准网状骨干，对骨干层环网起到链路备份和负载均衡的作用。福建电力骨干网组网图如图 2.3.1 所示：

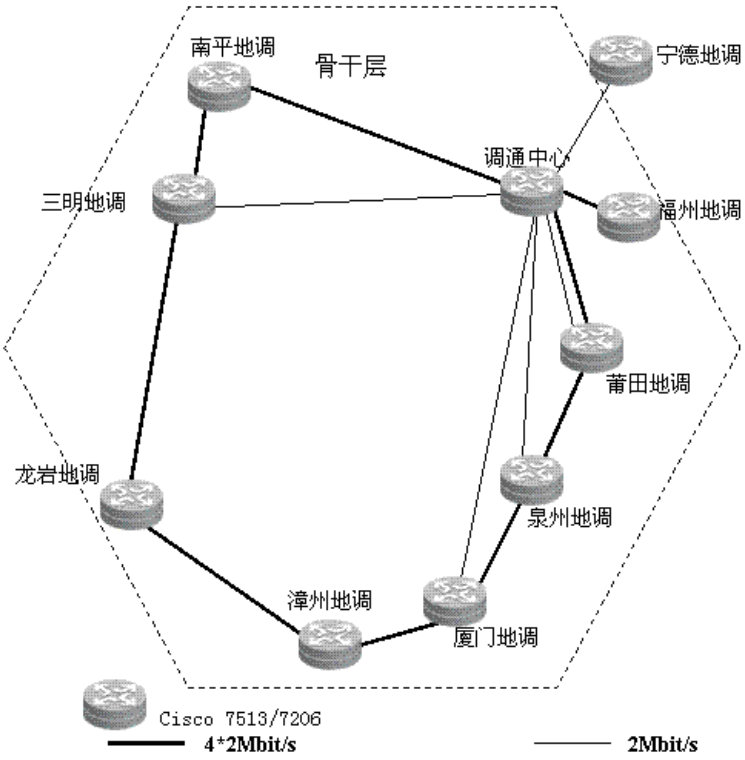


图 2.3.1 福建省电力调度数据网骨干网络拓扑结构图

从上图中可以看出，虽然福建电力调度网骨干网采用环形、星形组网，构成了一个准网状的网络，可靠性比较高，但这个主干网络仍然存在单点故障，省调和任何一台地调节点路由器的故障将导致调度数据发生中断。

龙岩、漳州没有直接到达省调的链路，需要经过其他地调周转，导致路由跳数增加不利于实时数据的转发。同时备用出口带宽太低，在主用链路发生故障时同样不利与实时数据的转发。

以上问题在本次方案设计中必须解决这个问题。

1.3.2. 三级网结构优化设计

原来省调配置了两台 7513，其中一台 Cisco 7513 用于直调电厂的接入，一台用于与地调的接入，省调做为整个调度数据网的核心可靠性必须得到保证，因此本次方案中将用于接入电厂的 7513 也接入到骨干网之中与原有 7513 形成双机，同时在每个地调节点增加一台路由器，这样在省调、地调都形成了双机，使调度数据网的可靠性得到增加。

骨干网的节点数量将大幅度增加，骨干网节点数量将由现在的 11 个节点增加到 20 个，而福建电力调度网可以利用的基础网传输资源却是有限的；

网络结构必须适应网络的业务流量分布情况，根据我们的了解，福建电力调度网骨干网的业务流量分布模型是一种集中汇聚式的模型，网上主要的业务流量分布如下图所示：

110KV、220KV 变电所《－》集控站《－》地调中心《－》省调中心；

相邻变电所节点之间、相邻地调中心之间的业务量很小，所以网络结构的优化也应该适应这种集中汇聚的业务流量模型；

根据上述分析，我们认为福建电力调度网骨干网应加强省调中心节点与各地调节点间直练链路的可靠性并提高这部分链路的带宽；在基础传输网资源有限的条件下，相应地减少各相邻地调节点间的带宽或者保持不变；通过这种方式减少骨干网业务传输的时延，提高骨干网的业务可靠性和实时性；

经过上述分析，我们以龙岩地调中心节点的组网示意图为例说明这种结构优化后的网络结构的变化，龙岩地调的广域网组网示意图如下图所示：

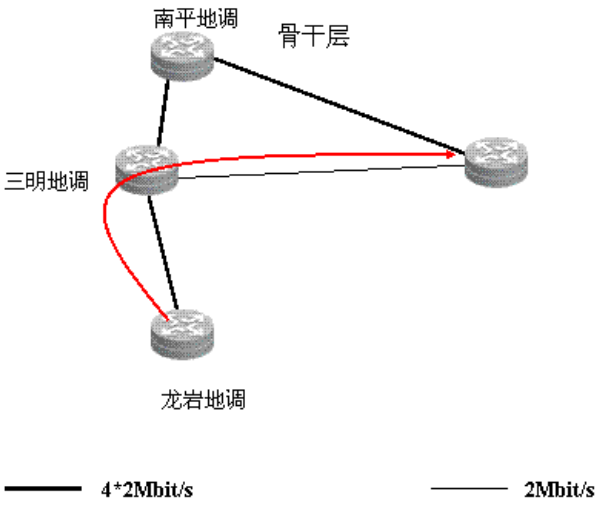


图 2.3.2 龙岩地调广域网组网结构示意图

龙岩地调没有直接到省调的链路，根据 OSPF 对链路 COST 值计算后达到省调要选择龙岩－三明这条链路，三明达到省调的链路才只有 2M，而龙岩与三明的链路却有 4*2M。再通过增加设备以及拓扑结构优化后的龙岩地调广域网组网示意图如下图所示：

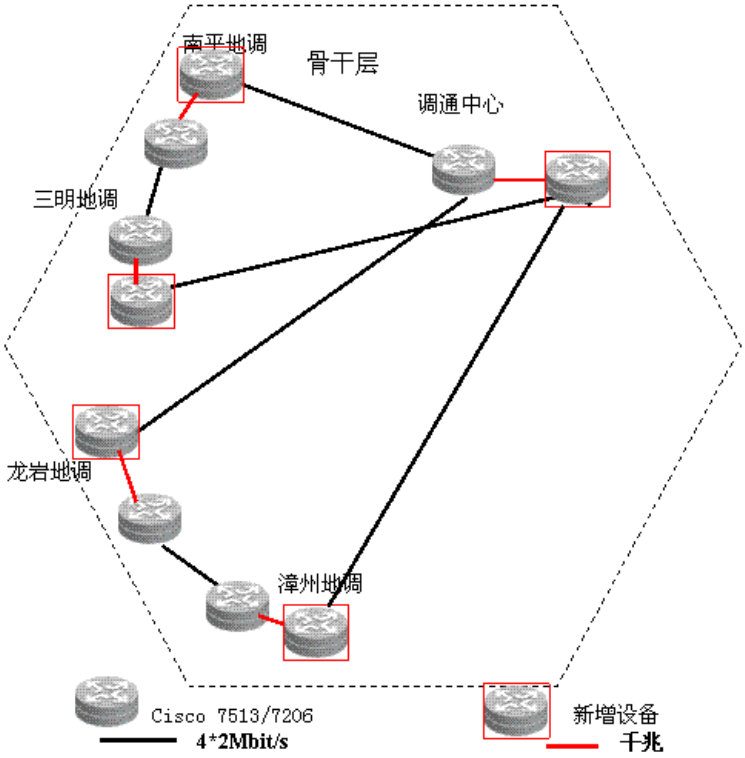


图 2.3.2 结构优化后的龙岩地调广域网组网结构示意图

在上述设计中，我们并没有将各个地调中心的两台路由器与省调通中心的两台路由器之间建立全网状的联系，而是让地调中心的每台路由器只与两台核心路由器中的一台建立联系；

采用这种组网方式，一方面不影响地调中心节点的可靠性（任何一台路由器的故障和任何一条链路的故障下都能保证该地调中心与核心节点间仍一条通路存在）；另一方面，采用这种组网方式，避免将骨干网结构过于复杂化，提高了骨干网的路由收敛速度，也更容易通过策略路由的方式实现两台地调节点路由器之间的负载分担。

其他节点的组网方式与此类似，经过上述结构优化后的福建省电力调度数据专网骨干网的组网示意图如下图所示：

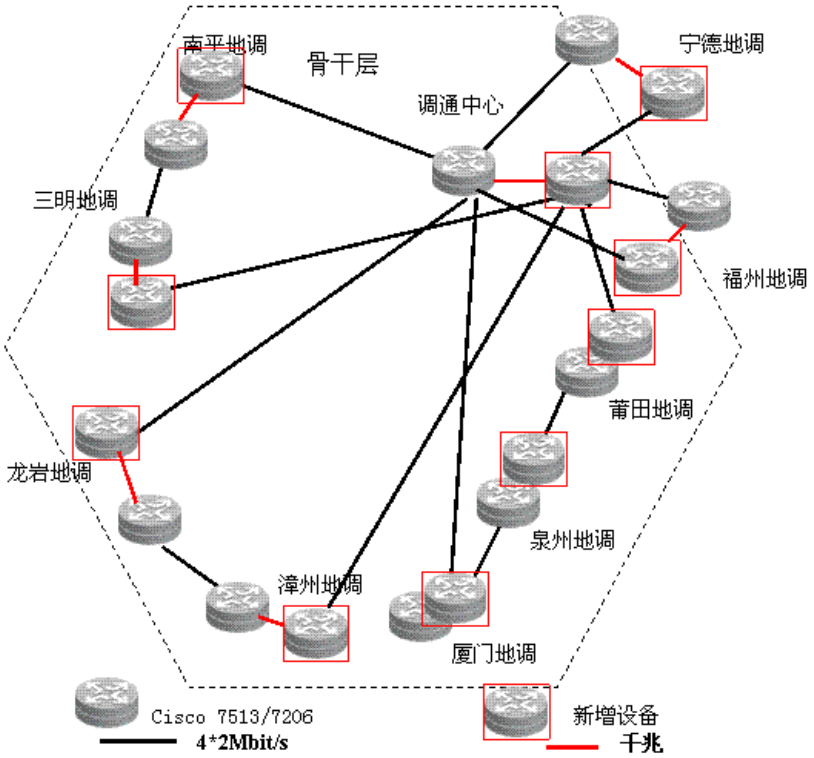
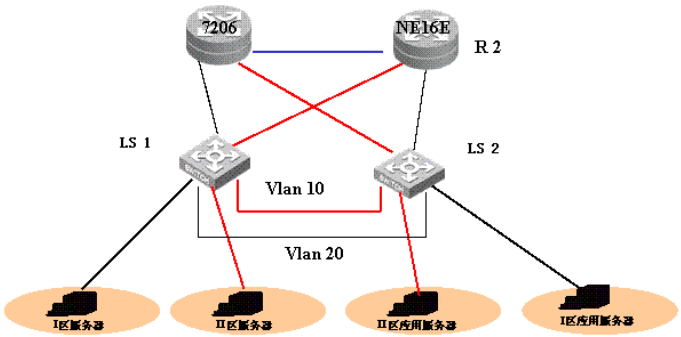


图 2.3.3 结构优化后的福建省电力调度数据专网骨干网结构示意图

1.3.3. 三级网局域网优化设计

福建电力调度数据专网各级地调节点都配置了两台交换机，经过网络优化后，各地调节点将拥有两台路由器，两台路由器可以运行 VRRP 协议，为局域网业务接入提供高可靠性。



改造后的各地调局域网，最大限度地继承了原来地调局域网的拓扑结构，减少了网络改造的工程量和造价，同时增加了调度数据业务接入的可靠性。

1.3.4. 三级网结构优化后的特点

经过上述优化后，福建省电力调度数据专网骨干网将体现如下优势：

拓扑结构和各骨干网节点的高可靠性：拓结构优化后的骨干网，继承了原来骨干网网格状的拓扑结构的可靠性优势，又通过为每个地调节点增加一台备份路由器，进一步增强了骨干节点的可靠性，真正实现了 N-1 的节点可靠和 N-1 的电路可靠性：

- 去掉任何一条连线（电路），不影响该节点的连通性；
- 去掉任何一个节点设备，不影响其他节点的连通性，和该调度中心的连通性；

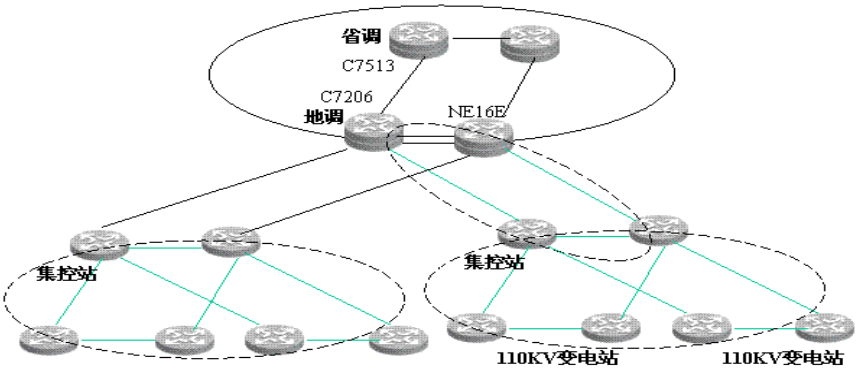
业务的实时性大幅度提高，业务时延大幅度降低：网络拓扑结构与业务模型更匹配，减少了业务迂回，减少了网络时延；

省通调中心与地调的高速直通链路，大幅度减少了骨干网时延；经结构优化后的骨干网，绝大部分地调都直接与省通调中心建立了高速的直接连接。只有在严重故障的特殊情况下，地调中心到省通调中心的两条链路全部中断，即便在这时，地调中心与省调度中心之间也最多经过一个迂回节点；

在现有的网络结构中，大部分地调节点与省地调中心直连链路的带宽很低，大部分的地调节点到省通调中心都需经过多个地调节点进行迂回，网络的时延大；

1.3.5. 四级网拓扑设计

三级网在地调通过增加设备节点实现了双机备份使网络的可靠性大大增加，为了充分发挥地调双机的作用以及保证四级网的可靠性，在四级网中的汇聚层和接入层也全部采用双机配置。



四级网采用全部双机的设计就完全具备与三级网一样的优点：

- 实现了 N-1 的节点可靠和 N-1 的电路可靠性；
- 网络拓扑结构与业务模型更匹配，减少了业务迂回，减少了网络时延

1.4. 传输链路通道

根据福建电网提供的通信接入条件，本工程广域网系统的提供的 WAN 通信接口为 N*2Mbps / G.703 接口，介质为 75Ω 非平衡式同轴电缆。核心层、骨干层、汇聚层、接入层之间的链路带宽需求为:骨干层与核心层之间带宽为 4*2M；汇聚层节点与骨干层节点之间链路带宽为 2*2M 链路；接入节点与汇聚节点之间链路带宽为 2*2M。以上链路全部采用双路由冗余备份通道。

1.5. 节点设计

路由器设备的命名方案：

为了保证以后的管理方便，设备命名需有一定的规范性。

设备采用以下命名方法： AA- YY-X。

- AA：表示该设备所属的级别和名称，通常的规则是取汉字拼音的首字母缩写。

省调-SD	福州-FZ	莆田-PT	泉州-QZ	厦门-XM
漳州-ZZ	南平-NP	三明-SM	龙岩-LY	宁德-ND

- YY：设备型号。如 NE16E、NE08、AR4640、AR2831、S3928TP-SI。
- X：表示如果前三项相同的设备，用数字编号 1、2 标识。如果没有备份的设备则无此项标识，例如地调的设备。
- 厂站设备命名规则：AA-『厂站名称的拼音缩写的小写字母』-设备类型。设备类型中以 R 代表路由器 S2 代表二层交换机.（实际命名时可以以具体路由器或交换机的型号代替，如 AR46、S3900）。所有 110KV 变电站都在变电站名称字母前加 1。

端口的域名命名规则：

[端口类型]—[接口板号]—[端口号]，其中端口类型包括：

(1) FE：百兆以太网接口；

(2) GE：千兆以太网接口；

(3) POS：155M SDH 接口；

(4) P04：622M SDH 接口；

(5) P16：2.5G SDH 接口；

(6) ATM：155M ATM 接口；

(7) E1：2M E1 接口；

(8) ……；……。

具体名称由接口所在的槽位及排列顺序决定。

如：FE-0-0

MP 命名规则

multilink 接口统一命名为：mp－group A/B/C，其中：

A 表示所捆绑的 EI 口所在的槽位

B 表示所捆绑的 E1 口所在的卡位

C 表示对端的设备所属的设备编码（主用路由器为：1；备用路由器为：2；地调路由器为：ospf 区域号*10）

端口描述的命名规则：

网络设备接口描述编码方式为：to 对方网络设备名称 带宽

各字段具体含义如下所示：

对方网络设备名称：见上一节对网络设备名称的详细说明。

带宽：2M 或 100M 等等

例子 1：description to FZ-NE16 2M

表示：该端口对端设备中心福州 NE16E 路由器，带宽为 2M 。

对于 ethernet 子接口的情况，将 description 写在主接口下。

2. 各节点设备配置

2.1. 骨干节点

设备为 NE16E、共计 9 台，每台设备基本配置为冗余路由引擎、冗余系统控制单元、告警单元、冗余电源、风扇

2.1.1. 福州地区

路由设备 E1 接口 75Ω G.703 端口 82 个，千兆光纤接口 6 个，路由设备 10/100Mb/s 局域网电口 8 个。

2.1.2. 莆田地区

路由设备 E1 接口 75Ω G.703 端口 11 个，千兆光纤接口 3 个，路由设备 10/100Mb/s 局域网电口 4 个。

2.1.3. 泉州地区

路由设备 E1 接口 75Ω G.703 端口 35 个，千兆光纤接口 3 个，路由设备 10/100Mb/s 局域网电口 4 个。

2.1.4. 厦门地区

路由设备 E1 接口 75Ω G.703 端口 25 个，千兆光纤接口 3 个，路由设备

10/100Mb/s 局域网电口 4 个。

2.1.5. 漳州地区

路由设备 E1 接口 75Ω G.703 端口 21 个，千兆光纤接口 3 个，路由设备 10/100Mb/s 局域网电口 4 个。

2.1.6. 龙岩地区

路由设备 E1 接口 75Ω G.703 端口 17 个，千兆光纤接口 3 个，路由设备 10/100Mb/s 局域网电口 4 个。

2.1.7. 三明地区

路由设备 E1 接口 75Ω G.703 端口 19 个，千兆光纤接口 3 个，路由设备 10/100Mb/s 局域网电口 4 个。

2.1.8. 南平地区

路由设备 E1 接口 75Ω G.703 端口 19 个，千兆光纤接口 3 个，路由设备 10/100Mb/s 局域网电口 4 个。

2.2. 汇聚节点

设备为 AR4640，共计 142 台，每台基本配置为路由引擎（1M 转发性能）、内置冗余电源、风扇

2.2.1. 福州地区

单台接口配置为：

12 个 E1 端口（接口为 75Ω G.703），4 个 10/100BASE-T LAN 端口

本地区 AR4640 数量为 28 台

2.2.2. 莆田地区

单台接口配置为：

12 个 E1 端口（接口为 75Ω G.703），4 个 10/100BASE-T LAN 端口

本地区 AR4640 数量为 8 台

2.2.3. 泉州地区

单台接口配置为：

12 个 E1 端口（接口为 75Ω G.703），4 个 10/100BASE-T LAN 端口

本地区 AR4640 数量为 24 台

2.2.4. 厦门地区

单台接口配置为：

12 个 E1 端口（接口为 75Ω G.703），4 个 10/100BASE-T LAN 端口

本地区 AR4640 数量为 24 台

2.2.5. 漳州地区

单台接口配置为：

12 个 E1 端口（接口为 75Ω G.703），4 个 10/100BASE-T LAN 端口

本地区 AR4640 数量为 6 台

2.2.6. 龙岩地区

单台接口配置为：

12 个 E1 端口（接口为 75Ω G.703），4 个 10/100BASE-T LAN 端口

本地区 AR4640 数量为 16 台

2.2.7. 三明地区

单台接口配置为：

12 个 E1 端口（接口为 75Ω G.703），4 个 10/100BASE-T LAN 端口

本地区 AR4640 数量为 14 台

2.2.8. 南平地区

单台接口配置为：

12 个 E1 端口（接口为 75Ω G.703），4 个 10/100BASE-T LAN 端口

本地区 AR4640 数量为 10 台

2.2.9. 宁德地区

单台接口配置为：

12 个 E1 端口（接口为 75Ω G.703），4 个 10/100BASE-T LAN 端口

本地区 AR4640 数量为 12 台

2.3. 接入节点

设备为 AR2831，共计 236 台。单台配置为：

4 个 10/100BASE-T LAN 端口

2 个 E1 端口（接口为 75Ω G.703）

2.4. 业务交换机

设备为 S3928TP-SI，共计 378 台。

3. 路由协议规划

在本期工程中，采用 OSPF 作为骨干层、汇聚层和接入层网络的内部 IGP 路由协议。

3.1. OSPF router id 规划

每台设备的 router id 设置为与该设备的 loopback 地址相同。

3.2. OSPF 子区（AREA）规划

采用 OSPF 作为 IGP，构建骨干路由。OSPF 是一种收敛迅速、消耗系统资源较少的高效的链路状态路由协议，在很多大型的骨干网的环境中得到了成功的应用。

OSPF 里最重要的概念之一是存在层次和区域。OSPF 允许把连续网络汇集起来，以进行分组。这样的组，和路由器一起维护到内含网络的接口，称为区域(area) 。每个区域独立运行基本链路状态路由算法的一个副本。

与把整个自治系统当作单个链路状态域相比，区域的拓扑结构更优越一些，它能隐藏起来，使之从区域外面不可见。同样地，其它区域里的路由器不知道其区域外的拓扑结构，这样明显地减少路由选择流量。

在网络里可以创建多个区域，不需要自治系统里的全部路由器都去维持整个链路状态数据库。只有同一区域里的路由器要有相同的数据库。

由于创建了区域，自治系统里的路由分成两种：区域内(连接到区域内的目标)和区域间(连接到本地区域外的目标)。

通过设计，OSPF 协议可把网络强制分层。对于能实施 OSPF 的网络，必须存在或能创建层次结构。区域的概念促使管理员在网络里创建层次。

随着区域间路由选择的引入，出现了主干区域(backbone area)的概念。区域之间的所有流量必须流经主干区域。OSPF 主干区域是专用 OSPF 区域 0。OSPF 主干始终包含全部的 ABR，并负责在非主干区域之间发布路由选择信息。主干区域必须连续。如果不连续的话，必须创建虚拟链路使之连续，以保证流量不被中断。

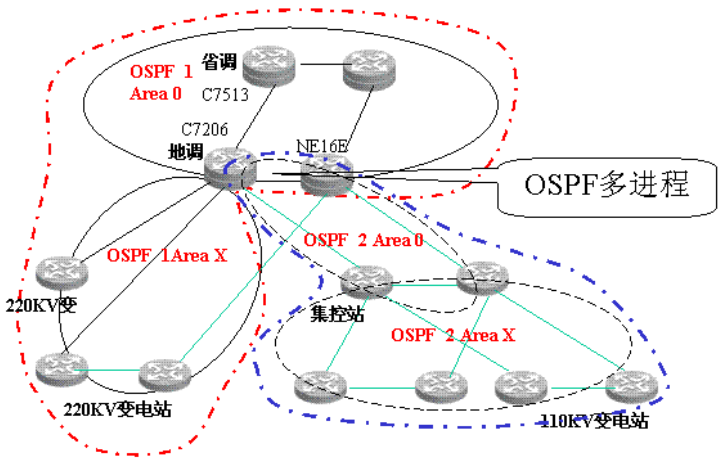
流量不能不流经主干区域。但是，若整个网络只有一个区域，那区域 ID 就

不重要了，因为不需要主干区域。若单个区域设置成非主干区域，引入第二个区域时，把第二个区域当作主干区域来建立，因为所有区域间的流量必须流经过它。

OSPF 层次的主要优点在于隐含了其它区域的拓扑结构，这样能明显地减少路由选择协议流量。区域可能是一个或多个网络、一个或多个子网、或是网络或子网的任意组合。若需要进一步减少路由更新，可能需要总结网络或子网。总结使用连续的地址块。

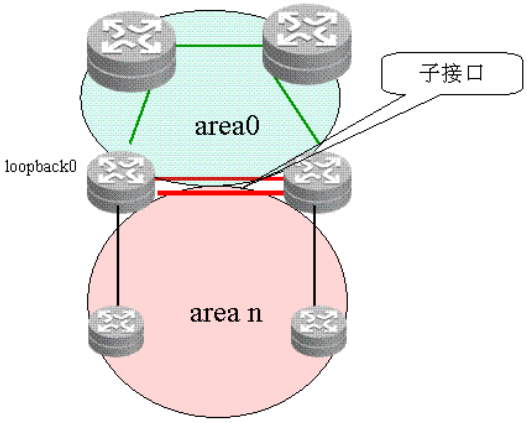
福建电力调度三级网采用 OSPF 做为 IGP 路由协议，省调与所有地调设备做为 OSPF 的主干区域（Area0），地调与各自所属的接入设备做为非主干区域（Area1－9）。本次工程要在地调新增一台设备与原有设备形成互备，负责四级网的设备接入，与原有 7206 同属于主干区域（Area0）。由于 7206 和 NE16E 还要接入四级网的汇聚层和接入层设备而且设备数量众多如果加入到原来的非主干区域（Area1－9）不利四级网中路由的收敛和聚合，同时会对原有网络造成影响，为了解决这个问题建议 7206 和 NE16E 上启用 OSPF 多进程（OSPF 2），在 OSPF 2 中，地调 C7206 和 NE16E 设备与集控站 AR46 划为 OSPF2 的主干区域 Area0，每个集控站的 AR46 和下属 110KV 变电站划为 AreaX，变电站可以学习到集控站和地调的路由；如果集控站和变电站需要访问省调，可以在地调的 C7206 和 NE16E 上配置路由相互引入即可。

本工程区域划分图如下：



骨干层和汇聚层都为双机配置，由于运行了 OSPF 多进程骨干层和汇聚层都处于不同进程的主干区域（Area0），因为要对非骨干区域内的路由进行地址聚合操作，所以需要确保非骨干区域的连通性，建议在双机互联的接口起子接口，一个子接口（子接口 1）属于主干区域（Areo0），一个子接口（子接口 2）属于非主干区域（Area1－9）。

划分方法见下图：



注：本图为一个地区的 OSPF 规划示意图，其他地区 OSPF 规划采用相同方法。

节点	Area 划分细则
每个地调原有的 7206	和三级核心、三级网骨干层节点的接口以及与地调新增设备互联的子接口 1 属于 OSPF1 的 Area 0，与地调新增设备互联的子接口 2 属于 OSPF2 的 Area 0
每个地调新增 NE16E	和三级核心、三级网骨干层节点的接口以及与 7206 互联的子接口 1 属于 OSPF1 的 Area 0，与地调 7206 的子接口 2 属于 OSPF2 的 Area 0
每个集控站设备	和 7206、NE16E 互联的接口以及集控站两台互

	联的子接口 1 属于 OSPF2 的 Area 0，集控站两台互联的子接口 2 和接入设备互联接口属于 OSPF2 的 Area X
接入层设备	属于各自地调的相应 Area X

以上为基本 OSPF 规划原则，各个地区的 OSPF 划分方案都以此原则为准，下面以福州地区个节点（以 14 个集控站举例）OSPF 划分进行举例说明：

节点	Area 划分细则
福州 1	连接三级核心的接口以及与福州 2 互联的子接口 1 属于 OSPF1 的 Area 0，与福州 2 互联的子接口 2 属于 OSPF2 的 Area 0
福州 2	连接三级核心的接口以及与福州 1 互联的子接口 1 属于 OSPF1 的 Area 0，与福州 1 互联的子接口 2 属于 OSPF2 的 Area 0
集控 1-1	连接两台骨干设备的接口以及与集控 1-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 1-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 1
集控 1-2	连接两台骨干设备的接口以及与北郊集控 1 互联的子接口 1 属于 OSPF2 的 Area 0，连接北郊集控 1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 1
集控 2-1	连接两台骨干设备的接口以及与集控 2-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 2-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 2
集控 2-2	连接两台骨干设备的接口以及与集控 2-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 2-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 2
集控 3-1	连接两台骨干设备的接口以及与集控 3-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 3-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 3

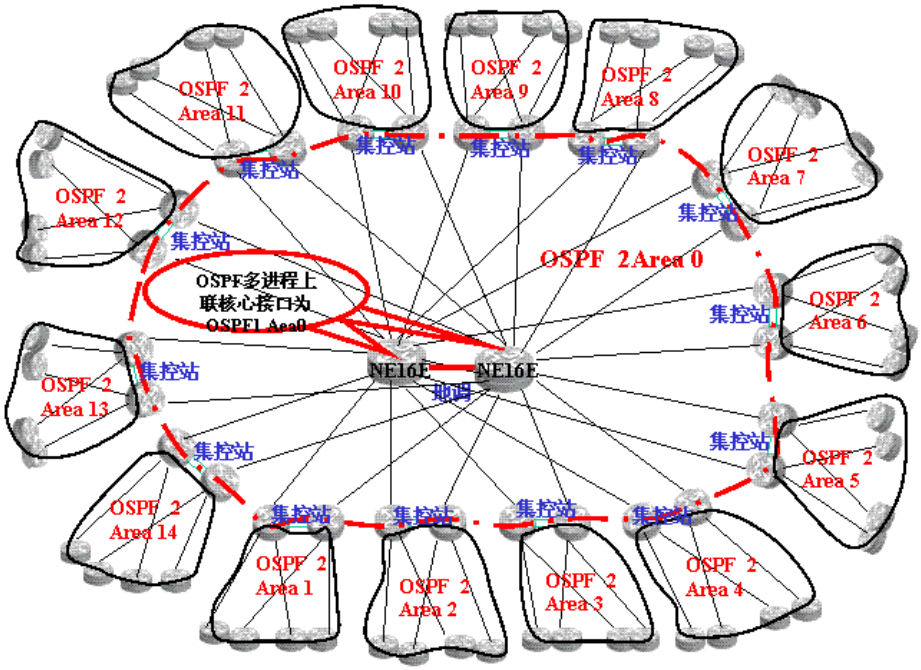
集控 3-2	连接两台骨干设备的接口以及与集控 3-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 3-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 3
集控 4-1	连接两台骨干设备的接口以及与集控 4-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 4-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 4
集控 4-2	连接两台骨干设备的接口以及与集控 4-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 4-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 4
集控 5-1	连接两台骨干设备的接口以及与集控 5-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 5-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 5
集控 5-2	连接两台骨干设备的接口以及与集控 5-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 5-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 5
集控 6-1	连接两台骨干设备的接口以及与集控 6-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 6-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 6
集控 6-2	连接两台骨干设备的接口以及与集控 6-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 6-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 6
集控 7-1	连接两台骨干设备的接口以及与集控 7-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 7-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 7
集控 7-2	连接两台骨干设备的接口以及与集控 7-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 7-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 7
集控 8-1	连接两台骨干设备的接口以及与集控 8-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 8-2 的子接

	口 2 和所属接入设备互联接口属于 OSPF2 的 Area 8
集控 8-2	连接两台骨干设备的接口以及与集控 8-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 8-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 8
集控 9-1	连接两台骨干设备的接口以及与集控 9-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 9-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 9
集控 9-2	连接两台骨干设备的接口以及与集控 9-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 9-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 9
集控 10-1	连接两台骨干设备的接口以及与集控 10-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 10-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 10
集控 10-2	连接两台骨干设备的接口以及与集控 10-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 10-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 10
集控 11-1	连接两台骨干设备的接口以及与集控 11-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 11-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 11
集控 11-2	连接两台骨干设备的接口以及与集控 11-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 11-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 11
集控 12-1	连接两台骨干设备的接口以及与集控 12-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 12-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的

	Area 12
集控 12-2	连接两台骨干设备的接口以及与集控 12-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 12-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 13
集控 13-1	连接两台骨干设备的接口以及与集控 13-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 13-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 14
集控 13-2	连接两台骨干设备的接口以及与集控 13-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 13-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 14
集控 14-1	连接两台骨干设备的接口以及与集控 14-2 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 14-2 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 15
集控 14-2	连接两台骨干设备的接口以及与集控 14-1 互联的子接口 1 属于 OSPF2 的 Area 0，连接集控 14-1 的子接口 2 和所属接入设备互联接口属于 OSPF2 的 Area 15
接入层 110KV 变电站	属于各自集控站的相应 Area

福州地区 OSPF 划分详见下图：

福州地区OSPF划分示意图



3.3. OSPF 对外发布路由时进行聚合

为了较少在整个 OSPF 路由域中的路由条目，在区域边界路由器（ABR）和 ASBR 处，可以进行路由聚合操作，向区域外部发送聚合后的路由信息。

本次工程中可以考虑在 ABR 处对如下路由进行聚合后发布：

- 骨干节点与汇聚节点之间的互联地址；
- 汇聚节点和接入层节点之间的互联地址。

本次工程中可以考虑在 ASBR 处对如下路由进行聚合后发布：

- 所连的厂站路由器的网管地址。

注：路由聚合可以视现场更具体的情况而定。

3.4. 在 OSPF 中引入其他路由协议的路由

OSPF 可以引入其他路由协议产生的路由，包括直连路由、静态路由、RIP。本次工程的具体路由引入情况视现场情况而定。

3.5. 在 OSPF 中统一路由尺度（COST）的计算

为确保路由器选择最优路径，统一 OSPF 路由尺度（cost）的计算，计算公式为：10000/带宽，带宽的单位是 Mbps，各种接口的路由尺度如下表所示。

接口类型	Cost
GE	1
155M POS	6
100M FE	10
N×E1	500/N

通过设置合理的 Cost 值来实现流量的负载或分担：比如把接入节点连接骨干节点和汇聚节点的链路设置不同的 Cost，来实现正常情况下流量从接入节点到骨干节点，而接入节点到骨干节点的链路作为备份。

3.6. 其他路由规划

对于三级网中的 220KV 变电站在本次四级网工程改造后要接入集控站，由于 220KV 变电站已经属于三级网中 OSPF 进程 1 的非主干区域（Area1－9），而集控站属于 OSPF 进程 2，为了减少网络配置和后期维护的复杂程度，建议 220KV 变电站与集控站之间采用静态路由。

4. BGP 路由协议规划

4.1. AS 号划分

由于福建电力调度三级网已经根据国调统一分配原则进行 AS 划分，给 MPLS 网络分配了一个 AS 号 300XX。在本次四级网工程中设计在地调增加一台设备接入原有三级网，与原有设备形成备份。地调这两台接入双机设备接入四级网的汇聚设备与接入设备，由于一台设备只能属于一个 AS，因此地调的两台设备只能属于三级网原有 AS，由于地调下面还要接入多个汇聚节点，如果要进行跨域连接就会出现多个区域，这样方式不利于网络的运行，因此建议福建电力调度四级网与三级网采用相同的 AS 划分。

4.2. 路由反射器的规划

IBGP 设计目标是追求网络的稳定性，减少路由振荡；可扩展性，降低路由器开销，允许支持更多的设备；简单性，使网络易于管理。

IBGP 采用了特殊水平分割方式来避免出现路由循环，即 IBGP 路由器不向其他 IBGP Peer 转发从某个 IBGP peer 学习到的路由，因此要求所有 BGP 路由器之间必须构成 Full Mesh 全连接才能够保证路由的正确传递。这种 IBGP 全连接会增加系统 CPU 和网络传输开销，降低系统性能，严重影响网络的可扩展性。解决 IBGP 的全连接问题有两种方式：路由反射器和自治域联盟，前者的可扩展性和简单性都好于后者，因此在可以企业网中采用路由反射器（Route Reflector, RR）的方式。

IBGP 主要用于将原三级路由传递到骨干、接入层。同时将本网路由传递到三级网。由于所有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。本项目中 IBGP 规划内容主要为 RR 的规划。RR 的设计模式基本上是遵循网络的物理结构，一方面可以达到最佳的路由转发效率，提高可扩展性，同时也可以避免路由决策和数据转发的分离造成的次优路由现象。福建电力调度数据网所有

节点都作为 MPLS VPN 的 PE 节点，需要建立 IBGP 全连接，运行 MBGP 协议实现 VPN 路由及信息的传递。

福建电力调度四级网路由器数量庞大，要实现 IBGP 全连接，需要建立几千条以上连接关系，为了减少 MP-iBGP 连接的数量，建议采用路由反射策略。一般而言，一个 cluster 只有一个路由反射器，但为防止路由反射器发生故障引起路由刷新信息的终止，在每个 cluster 中配置多个路由反射器，此时该 cluster 中的每个路由反射器都必须配置相同的 cluster 标识符。本项目中 BGP 路由规划建议采用三级 RR 结构。

第一级反射器：

省调路由器为路由反射器（RR）；反射客户机为其余所有骨干层节点路由器。

第二级反射器：

地调路由器为路由反射器（RR）；反射客户机为本地区所有汇聚层节点路由器。

第三级反射器：

集控站路由器为路由反射器（RR）；反射客户机为本地区所有接入层节点路由器。

采用路由反射策略后，IBGP 连接数量大量减少，降低了管理难度，同时又便于业务扩展。

5. IP 地址分配

5.1. IP 地址分配方案

福建省电力调度数据网的 IP 地址采用 B 类地址空间：10.xx.BB.CC。IP 的第三个 8 位组 BB 为省内各单位代码，取值为 0—254。福建调度数据网主要业务有：调度自动化（EMS）管理信息系统（MIS）电量计费（TMS）保护管理系统（PIMS）电力市场 (EMOS) 通信监控系统(CCS)，对于地址分配省调每个应用系统各占用 4 段地址，各地区局应用系统共占用 2 段地址，全省厂站 RTU 和计费终端各占用 1 段地址。

5.2. 对于设备 Loopback 地址的分配

各路由器的 Loopback 地址的使用，在不同的方面都需要它的参与，这主要包括了以下的几种情况：

- 路由器的 Loopback 地址，是保证内部路由协议的正常运行的重要条件；路由器的 Loopback 地址，是建立 iBGP 会话的主要参数的选择，
- 选择 Loopback 地址作为 iBGP 会话建立的基本，对于会话的稳定性能够提供很好的支持。

综合这些方面，各路由器的 Loopback 地址，对于整个网络的正常运行，有着至关重要的作用，因而对于各个路由器的 Loopback 的分配和管理，应当采取统一的专有地址空间。通过为所有的路由器分配一个专有的地址空间，能够更为有效地进行路由器的路由配置和管理，以及方便今后的故障的诊断和排除。

Loopback 地址分配采用 32 位掩码的原则。

5.3. 对于设备间链路地址的分配

路由器间链路的 IP 地址，从业务的相关性上，他们一般不具有全局的功能，而只是提供完成两个路由器之间的连接。因而从这个角度上讲，这部分的地址空间的分配应当考虑以下的方面：

- 尽可能以分层次的方式为他们分配地址。

- 由于链路地址空间不具有全局性，因而并不需要在全网范围内为每个链路保持精确路由。而采取分层次的地址分配方式，能够将链路地址逐级汇总，从而使得这些地址在各路由器的路由表中占有较少的空间。以降低对路由器的要求，并保证路由器的处理效率。
- 提供足够的预留空间，以满足今后新增链路的需要。

采用上面的分层次的链路地址分配结构，能够保证路由处理的高效性。而在实施的过程中，应当考虑到在根据业务需要新增链路的时候，这种分层次的结构尽量不会被打破。那么，就需要在初期分配的时候，考虑到不远的将来可能进行的扩容，从而进行相应的预留。

互连链路地址采用 30 位掩码的分配方式。

5.4. 核心、汇聚局域网地址

每个局域网按照业务种类进行子网划分，每种类型的业务将工作在同一个子网，依据每类业务类型包含主机的数量，建议可分配 30 个地址。

5.5. CE 网管设备地址

主要是 QuidView 网管系统要求管理 CE 设备，但由于 CE 的上联 PE 的链路地址对全网并不是公开的，因此要单独在 CE 与 PE 的链路划分一个子接口，为此 CE 与 PE 互连的子接口将分配一个 29 位掩码的子网。

6. 网络可靠性设计

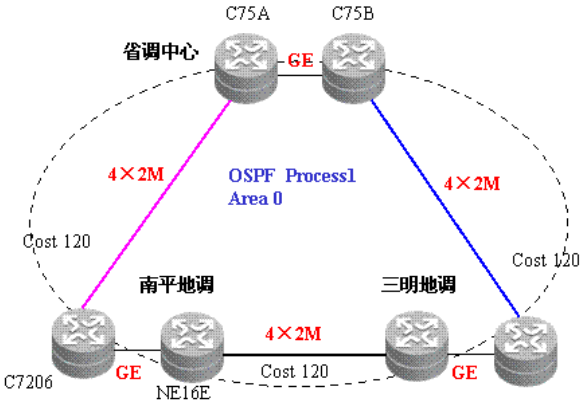
福建电力调度数据网采用 OSPF 做为 IGP 路由协议，在网络设计通过 OSPF 协议自身的特点以及合理的规划实现网络的自愈。

6.1. 三级网可靠性设计

以南平地调和三明地调的情况为例。地调和省调的设备都运行 OSPF（地调启用 OSPF 多进程，与省调联的为 OSPF Process1），以带宽参考值 1Gbps 为例，由 OSPF 自动计算接口开销（Cost 值），则南平地调直接上联省调的线路（**粉红色链路**）cost 为 120/121，经过三明地调上行的 cost 为 242/241，这样南平地调以及下属集控站等的数据，将优先通过自己的链路上行，一旦该链路出现故障，才会选择经过三明地调的链路，而一旦南平自己的链路恢复，由于这条路径 cost 值小，数据将自动切回走本地链路，不再绕行三明地调，从而达到地调线路备份的目的。

同理，三明地调的设备也可以实现线路备份。其他地市地调的线路备份与此类似。

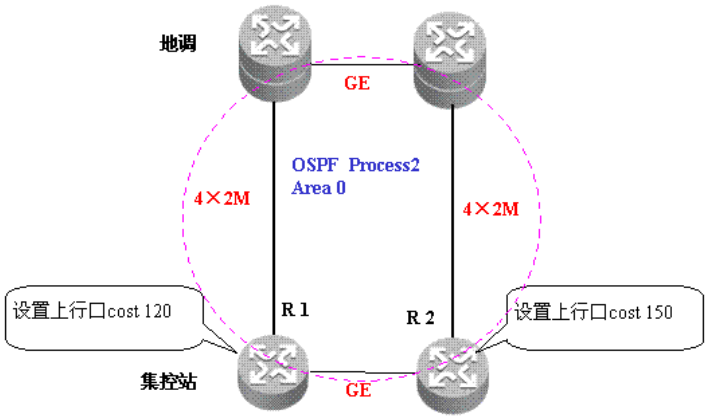
地调和省调之间运行的 OSPF 协议，也可以手工规划 Cost 值，只要保证从某地调直接上行的链路 cost，小于绕经其他地调链路的 cost 即可。



6.2. 四级网可靠性设计

集控站路由器上行链路接口，分别设置不同的开销 cost 值（缺省时候 OSPF 协议会根据参考带宽自动计算，计算公式为：接口开销=带宽参考值/接口带宽 ，规划带宽参考值为 1Gbps），OSPF 协议缺省会选择 cost 值小的链路作为主用链路，一旦该链路发生故障中断，OSPF 协议会自动切换到备用链路。如上图所示，假设某集控站两台路由器 R1 和 R2 上联地调，我们规划 R1 的上行链路作为主用链路，R2 作为备份，则可以设置 R1 上行口 Cost 120，R2 上行口 cost 150。

110KV 变电站的上行链路故障自愈情况，与此类似。



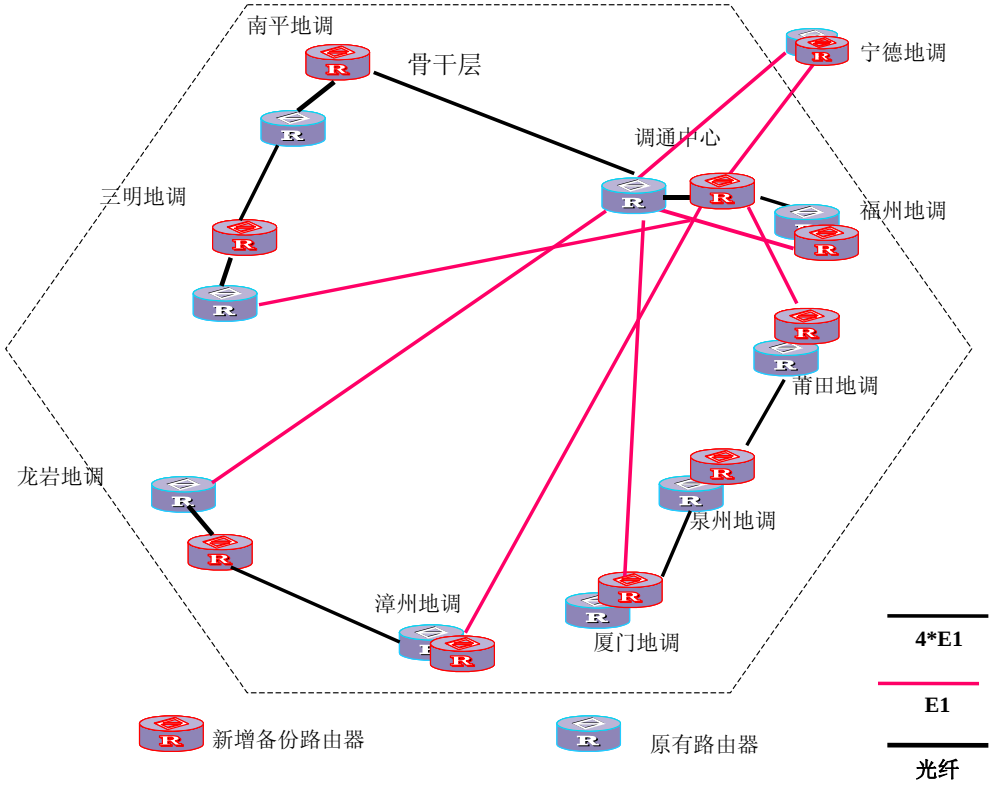
7. 互联互通

福建电力调度数据三级网中的设备为 CISCO 设备，本次四级网要在骨干层增加一台设备，在骨干层形成双机，与其他骨干节点相连同核心节点形成环形网络，同时接入汇聚节点，形成 CISCO 与华为 3Com 公司产品混合组网。

7.1. 广域网互联互通

本次工程在地调新增 NE16E 路由器与原有地调 7206 形成备份，NE16E 与 7513、7206 之间通过标准的 MPLS、OSPF 协议进行互联互通。

7.1.1. 链路互通

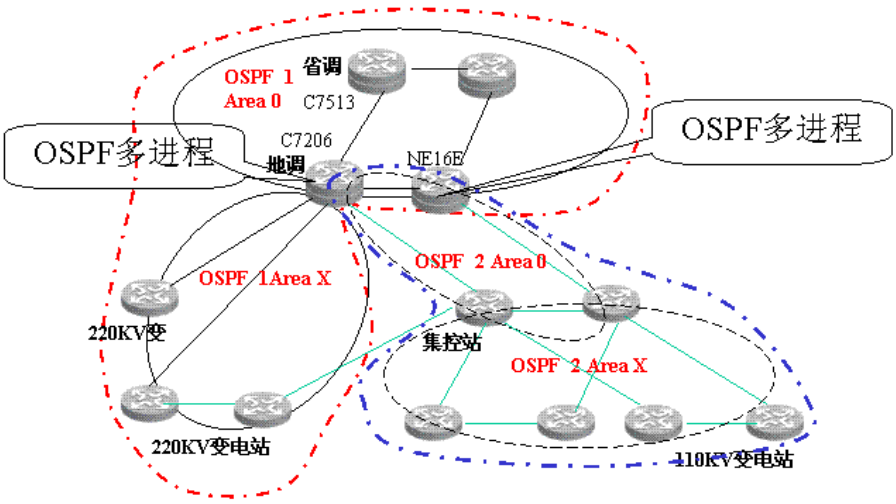


上图是骨干互联拓扑图，从图中看到，NE16E 与 7513 之间要进行 E1 捆绑以及 E1 互联， NE16E 与 7206 之间要通过以太网进行互联。另外骨干层 7206 与新增集控站 AR4640 的 E1 互通。对于 NE16E、AR4640 与 CISCO 设备之间普通 E1 的互联互通只需要在各个设备 E1 接口都采用 PPP（Point to Point Protocol）协议进行封装（Cisco 设备缺省为 HDLC 协议），同时两端接口如果需要验证请选择同样的验证方式 PAP 或 CHAP,这样就可以实现互联互通。在 NE16E 与 7513 之间进行多条 E1 捆绑时要采用 MultiLink PPP 即 MP，在配置 E1 捆绑的时候同样要在注意选择 PPP（Point to Point Protocol）协议进行封装。

对于以太网之间的互联互通只要注意双工方式和速率的匹配，采用标准的 IEEE802.1Q VLAN 协议和标准的生成树协议 STP/RSTP/MSTP 就可以实现互通。

7.1.2. OSPF 互通

NE16E 与 7513、7206 以及 AR4640 与 7206 之间运行 OSPF 动态路由协议，要使两台路由直连接口的 OSPF 网络类型一致,然后配置邻居，要注意设备两边设备 OSPF 的 Hello 报文间隔，因为根据 RFC2328 的规定，要保持网络邻居间的 hello 时钟的时间间隔的一致性。同时要保证两端设备的相邻路由器间失效时间一致。



在三级网中 NE16E 属于新增设备，在与 CISCO7206 和 7513 进行 OSPF 互通之前要了解到原有三级网的OSPF配置，例如NE16E与之相连接7206的Router ID，通常都是设备的 loopback 地址，然后根据分配给 NE16E 的 loopback 地址配置成 NE16E 的 router id，接下来在 NE16E 上面启动 OSPF，OSPF 支持多进程而且本次项目中也会用到 OSPF 多进程，首先设置与 7513 和 7206 相同的 OSPF 进程号，通常为 1。下面就要将 NE16E 配置成主干区域即 Area0，然后在与 7513 和 7206 之间互连的端口下面把路由发布出去。通过以上步骤后 NE16E 就可以与 7513、7206 建立起 OSPF 的邻居关系并且互相学习和发布路由了。另外还要分别在地调的7206和NE16E上面再起一个OSPF进程2，将7206和NE16E在OSPF进程2下面再配置成主干区域即 Area0，然后将与集控站互通端口的路由发布出去。

经过以上方法就可以实现 NE16E 与 7513、7206 的 OSPF 互联互通。

7.1.3. MPLS/VPN 互通

在 MPLS/VPN 互通方面主要 NE16E、AR4640 与 CISCO7513、7206 设备进行互通。原有三级网的 MPLS/VPN 规划中 7513 与 7206 均为 PE 设备，此次在地调节点新增的 NE16E 同样为 PE 设备。在进行互通之前首先要了解原有网络的 MPLS/VPN 规划，如：AS 号，VPN 数量、RD 规划、RT 规划。在了解这些信息后开始配置 NE16E，与 7513 和 7206 进行 MPLS/VPN 的互联互通。

首先要在 NE16E 设备上面配置 LSR 的标识 ID、启用 MPLS 和 LDP 协议，另外还要进入接口模式，使能接口的 LDP 功能。

经过上述的基本配置，NE16E 即可提供 MPLS 转发和 LDP 信令功能。这里需要注意的是 CISCO 有 tag switching 和 LDP 两种，要选择 LDP。

以上是完成 NE16E 的基本 MPLS 配置，PE 的配置比较复杂，为了完成与 7513 和 7206 的互联互通，还要完成下几个部分：

1、配置 BGP/MPLS VPN Site，即有关 vpn-instance 或 vrf 的配置，根据原来的 vpn 设置，在 NE16E 上面创建 VPN，然后在创建好的 VPN 下面将 RD 配置成与 7513、7206 上面相同的 RD，为了确保 NE16E 上面的 VPN 能与 7513、7206 上面的 VPN 互通关键是配置 RT，也就是 vpn-target，将 NE16E 上面的 import-extcommunity 和 export-extcommunity 配成与 7513、7206 上面的 route-target import 和 route-target export 完全一致，这样才能保证相同的 VPN 能进行互通。

2、配置 IGP，实现 PE 内部的互通；在这里要将 NE16E 的 AS 号配置成与 7513、7206 相同的 AS 号，然后将 NE16E 的 router id 当作路由发布出去这样可以用 loopback 接口与其他设备建立 BGP 的邻居关系；接着与 7513、7206 建立 BGP 邻居关系即在 NE16E 上面邻居中配置 7513、7206 的 loopback 地址，同时也要在 7513、7206 上面配置 NE16E 的 loopback 地址，这样 NE16E 就可以与 7513、7206 建立起 BGP 的邻居关系并交换 BGP 路由信息。

3、由于 MPLS/VPN 之中是靠 MP-IBGP 来传递 VPN 路由信息，因此还要配置 MP-IBGP，首先在 NE16E 之中进入 MP-BGP 的 vpnv 4 地址族,在其下面再配置 MP-BGP 邻居，这里的邻居还是 7513、7206 的 loopback 地址，同时也要在 7513、7206 上面配置 NE16E 的 loopback 地址。这样 NE16E 就可以与 7513、7206 建立起 MP-BGP 的邻居关系就可以交换 MPLS/VPN 路由了，最后就要发布 VPN

路由，由于业务接入都是通过交换机方式接入到 NE16E 上面，因此对于业务路由都是本地路由即直联路由；直接这些直联路由引入 MP-BGP 之中。

通过以上就可以实现 NE16E 与 7513、7206 的 MPLS/VPN 互联互通，交换 VPN 路由信息。对于集控站的 AR4640 与 7206 的 MPLS/VPN 互联互通方式方法与上面完全一致。

7.2. 局域网互联互通

地调节点的局域网接入采用两台以太网交换机，地调两台路由器 7206 与 NE16E 之间运行 VRRP 协议保证业务主机接入的可靠性。

7.2.1. VRRP 介绍

在基于 TCP/IP 协议的网络中，为了保证不直接物理连接的设备之间的通信，必须指定路由。目前常用的指定路由的方法有两种：一种是通过路由协议（比如：内部路由协议 RIP 和 OSPF）动态学习；另一种是静态配置。在每一个终端都运行动态路由协议是不现实的，大多客户端操作系统平台都不支持动态路由协议，即使支持也受到管理开销、收敛度、安全性等许多问题的限制。因此普遍采用对终端 IP 设备静态路由配置，一般是给终端设备指定一个或者多个默认网关(Default Gateway)。静态路由的方法简化了网络管理的复杂度和减轻了终端设备的通信开销，但是它仍然有一个缺点：如果作为默认网关的路由器损坏，所有使用该网关为下一跳主机的通信必然要中断。即便配置了多个默认网关，如不重新启动终端设备，也不能切换到新的网关。采用虚拟路由冗余协议 (Virtual Router Redundancy Protocol，简称 VRRP)可以很好的避免静态指定网关的缺陷。

在 VRRP 协议中，有两组重要的概念：VRRP 路由器和虚拟路由器，主控路由器和备份路由器。VRRP 路由器是指运行 VRRP 的路由器，是物理实体，虚拟路由器是指 VRRP 协议创建的，是逻辑概念。一组 VRRP 路由器协同工作，共同构成一台虚拟路由器。该虚拟路由器对外表现为一个具有唯一固定 IP 地址和 MAC 地址的逻辑路由器。处于同一个 VRRP 组中的路由器具有两种互斥的角色：主控路由器和备份路由器，一个 VRRP 组中有且只有一台处于主控角色的路由

器，可以有一个或者多个处于备份角色的路由器。VRRP 协议使用选择策略从路由器组中选出一台作为主控，负责 ARP 相应和转发 IP 数据包，组中的其它路由器作为备份的角色处于待命状态。当由于某种原因主控路由器发生故障时，备份路由器能在几秒钟的时延后升级为主路由器。由于此切换非常迅速而且不用改变 IP 地址和 MAC 地址，故对终端使用者系统是透明的。

7.2.2. VRRP 原理

一个 VRRP 路由器有唯一的标识：VRID，范围为 0—255。该路由器对外表现为唯一的虚拟 MAC 地址，地址的格式为 00-00-5E-00-01-[VRID]。主控路由器负责对 ARP 请求用该 MAC 地址做应答。这样，无论如何切换，保证给终端设备的是唯一一致的 IP 和 MAC 地址，减少了切换对终端设备的影响。

VRRP 控制报文只有一种：VRRP 通告(advertisement)。它使用 IP 多播数据包进行封装，组地址为 224.0.0.18，发布范围只限于同一局域网内。这保证了 VRID 在不同网络中可以重复使用。为了减少网络带宽消耗只有主控路由器才可以周期性的发送 VRRP 通告报文。备份路由器在连续三个通告间隔内收不到 VRRP 或收到优先级为 0 的通告后启动新的一轮 VRRP 选举。

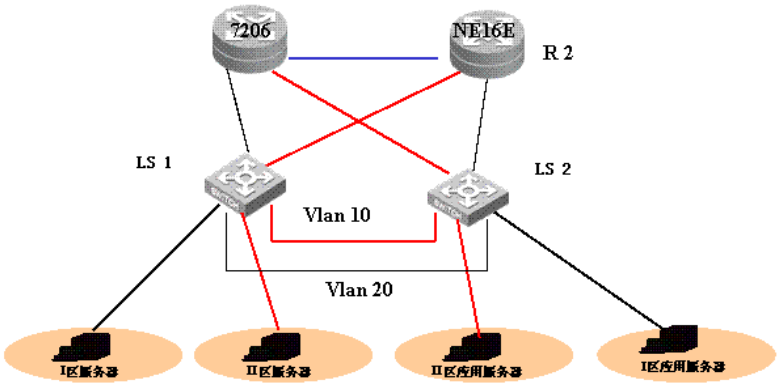
在 VRRP 路由器组中，按优先级选举主控路由器，VRRP 协议中优先级范围是 0—255。若 VRRP 路由器的 IP 地址和虚拟路由器的接口 IP 地址相同，则称该虚拟路由器作 VRRP 组中的 IP 地址所有者；IP 地址所有者自动具有最高优先级：255。优先级 0 一般用在 IP 地址所有者主动放弃主控者角色时使用。可配置的优先级范围为 1—254。优先级的配置原则可以依据链路的速度和成本、路由器性能和可靠性以及其它管理策略设定。主控路由器的选举中，高优先级的虚拟路由器获胜，因此，如果在 VRRP 组中有 IP 地址所有者，则它总是作为主控路由的角色出现。对于相同优先级的候选路由器，按照 IP 地址大小顺序选举。VRRP 还提供了优先级抢占策略，如果配置了该策略，高优先级的备份路由器便会剥夺当前低优先级的主控路由器而成为新的主控路由器。

为了保证 VRRP 协议的安全性，提供了两种安全认证措施：明文认证和 IP 头认证。明文认证方式要求：在加入一个 VRRP 路由器组时，必须同时提供相同的 VRID 和明文密码。适合于避免在局域网内的配置错误，但不能防止通过网络

监听方式获得密码。IP 头认证的方式提供了更高的安全性，能够防止报文重放和修改等攻击。

7.2.3. 互通方案

华为 3Com 和 Cisco 路由器都支持 VRRP 协议，Cisco 路由器缺省支持 HSRP(私有协议)，Cisco 在 IOS 12.0(22)S 开始支持 VRRP 协议，Cisco IOS 12.2(13)T、Cisco IOS 12.2(14)S 支持 VRRP 协议，具为了实现互通需要原有设备 7206 的软件版本支持 VRRP 协议。



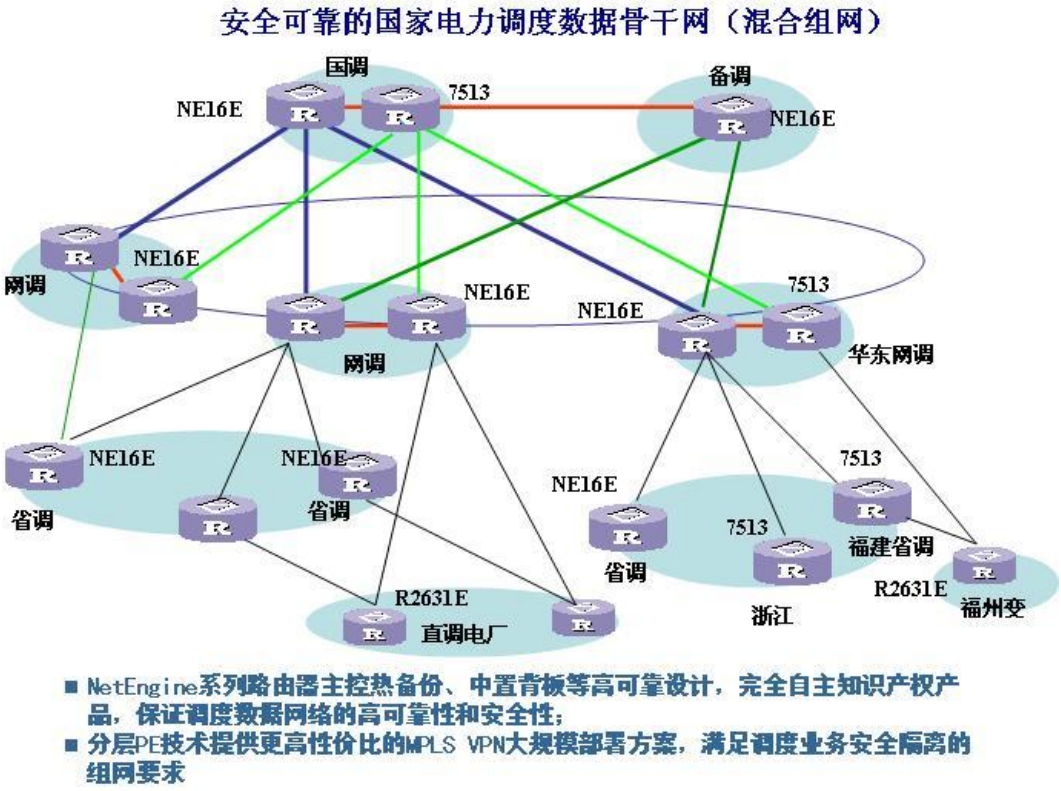
如上图所示，华为路由器 NE16E 和 cisco 路由器 7206 之间运行 VRRP 协议实现自动故障切换，NE16E 和 7206 组成一个 VRRP 路由器组，因为华为路由器 NE16E 的处理能力高于 cisco 路由器 7206，则将 NE16E 配置成 IP 地址所有者，局域网的默认网关设定为 NE16E。则 NE16E 成为主控路由器，负责 ICMP 重定向、ARP 应答和 IP 报文的转发；一旦 NE16E 失败，7206 立即启动切换，成为主控，从而保证了对客户透明的安全切换。

同时在 NE16E 和 7206 上联的广域网接口启用 VRRP 监视接口功能，这样即使 NE16E 仍然工作，但当其的广域网接口不可用时，可能希望由 7206 来执行网关工作更好地扩充了备份功能，即不仅在备份组所在的接口出现故障时提供备份功能，而且在路由器的其它接口不可用时，也可以使用备份功能。

7.3. 部分互联互通案例

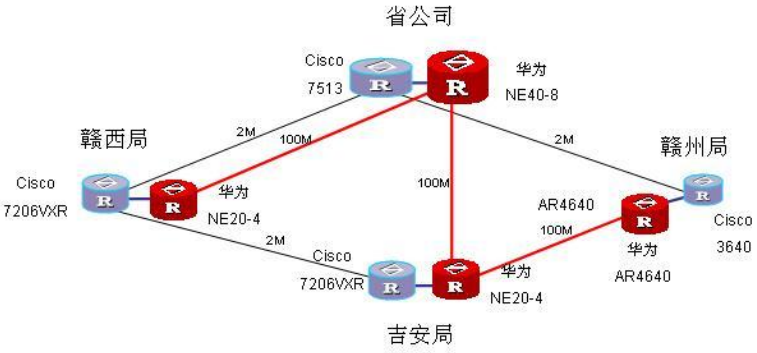
7.3.1. 国家电网公司调度数据网

在国家电网公司全国调度数据网中，有 4 台 Cisco7513 设备分别放置在国调 2、华东 2、福建、浙江与 30 余台 NE16E 混合组网，Cisco7513 与 NE16E 运行 OSPF 协议，全部做为 PE 设备，整网运行 MPLS/VPN，国家电网公司全国调度数据网从建设至今运行良好，已经通过国家电网公司最终验收。



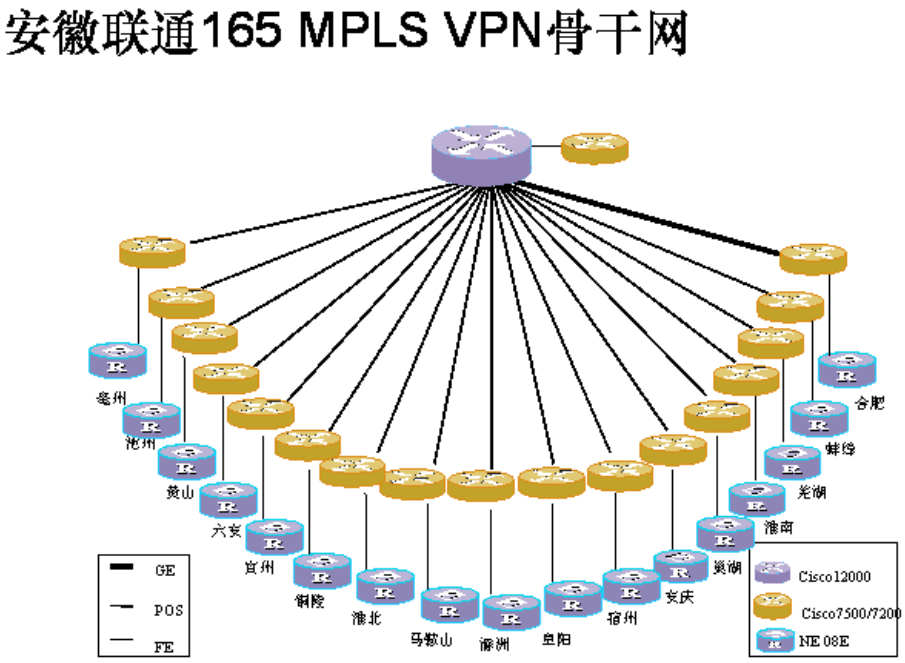
7.3.2. 江西电力广域网

江西电力广域网原有设备为 CISCO7513、7206VXR，3640，均为单台进行组网，为了增加网络的可靠性采用华为公司 NE40、NE20、AR4640 与原有 CISCO 设备进行互备，在广域网与 CISCO 设备运 OSPF 路由器，对局域网接入华为与 CISCO 设备之间运行 VRRP 保证业务接入的可靠性，江西电力广域网改造后运行良好，网络的可靠性大大增加。



7.3.3. 安徽联通

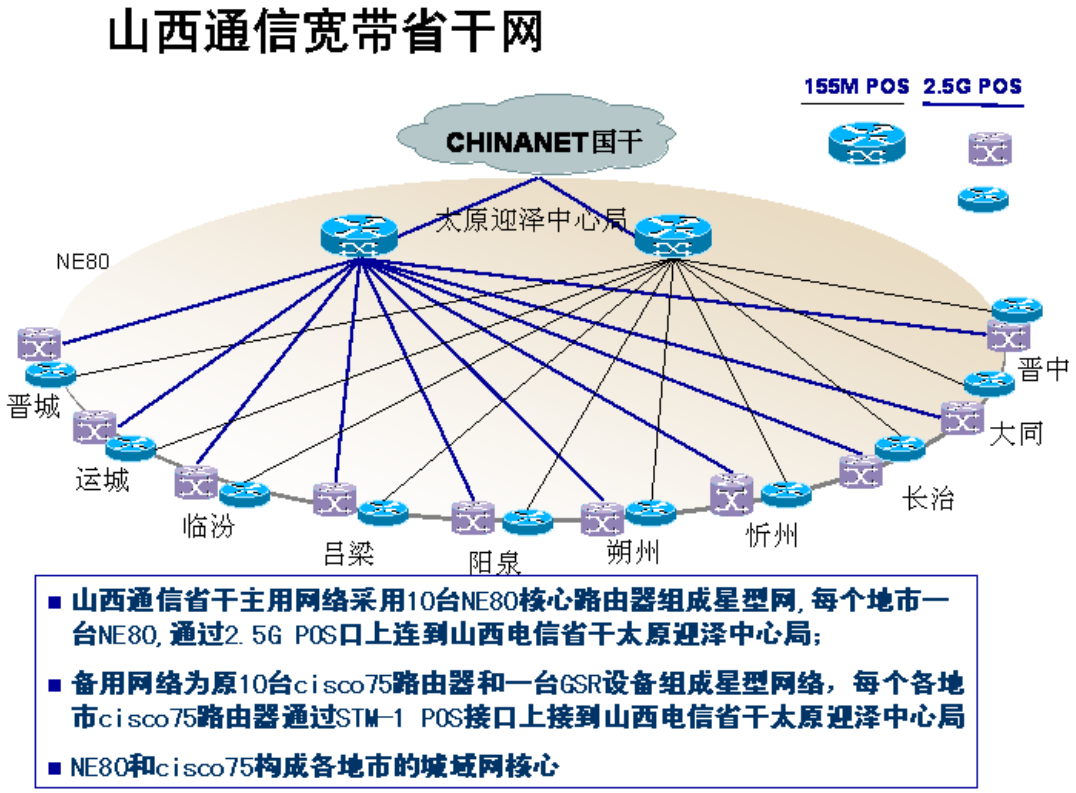
在安徽联通 165 网络中，使用 Cisco 公司的 Cisco7500/Cisco7200 系列作为 P 设备，华为公司的 NE08E 作为 PE 设备，整网开展 MPLS VPN 业务。



■安徽联通，采用CISCO路由器作为P设备，17台华为公司的Quidway NE08E作为PE设备，整网开通MPLS VPN业务

7.3.4. 山西通信省干网

在山西通信省干网中，华为公司的 NE80 和 Cisco7500、Cisco GSR12008 混合组网。使用 OSPF 路由协议，在省干开展 MPLS VPN 业务。



7.3.5. 部分互通案例名单

华为 NE 系列路由器还在运营商与 CISCO 设备进行互联互通，下面是部分名单：

运营商名称	设备型号、数量	路由协议	组网方式	业务功能
中国电信 CN2	NE80E(VRP5.10) 16 台 Juniper T640 若干 Cisco GSR12416 若干	BGP,IS-IS	NE80E 作为 CN2 北方九省骨干节点，与 Juniper T640、Cisco 12416 设备互	MPLS VPN、QOS、组播

			通	
广东电信 163 骨干网	NE5000(VRP3.10) 10 台 NE80(VRP3.10) 6 台 GSR 124xx 2 台 GSR 120xx 22 台	BGP,IS-IS	华为和 Cisco12416 作为国干超级核心，NE80 和 GSR 在边缘。	Internet
广东电信城域网(深圳等)	NE5000E(VRP5.10) 8 台 NE80E(VRP5.10) 2 台 GSR 120xx 若干	BGP,IS-IS,OSPF	作为深圳、东莞、佛山等电信城域网的出口路由器，与广东电信 163 骨干网连接。	Internet MPLS L3 VPN
哈尔滨通信 IPTV 城域网	NE5000E 2 台 NE80E 4 台	BGP,OSPF	作为 IPTV 城域网核心和汇接层，与 Juniper M40 互通	组播
中国铁通 CNGI	NE5000E 4 台 NE40 2 台 M320 3 台 M40E 1 台	BGP4+,OSPFv3	华为 NE5000E 作为北京节点核心、汇聚和网关节点，NE40 作为接入节点。	IPv6
电信北方 10 省 163 骨干网	NE80(VRP3.10) 90 台 GSR124xx 40 台 M160/M40 20 台	BGP,IS-IS	一般省份 Juniper、Cisco 在核心，华为在边缘汇聚 其中河南、山东两省华为在核心。	Internet IP QOS MPLSQoS MPLS L3 VPN, VOIP（NGN）
上海 163	NE80(VRP3.10) 1 台 GSR 124xx 5 台 M20 1 台	BGP,OSPF	华为、Cisco、Juniper 同时作为核心	Internet
辽宁移动 CMNET 骨干	NE80(VRP3.10) 6 台，出口连 CMNET 国(M160)	BGP,IS-IS	华为在核心，少量 Cisco 设备在边缘	Internet

贵州移动 CMNET 骨干	NE80(VRP3.10) 8 台 GSR12012 2 台	BGP,IS-IS	Cisco 在核心，华为在汇聚层	Internet
安徽移动 CMNET 骨干	NE80(VRP3.10) 2 台 M160/M40 18 台	BGP,IS-IS	Juniper 在核心，华为在汇聚层	Internet
山西通信 169 骨干网	NE80(VRP3.10) 10 台 GSR12416 2 台	BGP,OSFP	Cisco 在核心，华为在边缘	Internet, MPLS L3 VPN
内蒙通信 169	NE80(VRP3.10) 6 台 GSR12000 10 台	BGP,OSFP		
江苏通信 169 骨干网	NE80(VRP3.10) 21 台 GSR 12416 2 台	BGP,IS-IS	Cisco、华为在核心，华为在边缘	Internet, MPLS L3 VPN
广东通信 169 骨干网	NE80(VRP3.10) 4 台 GSR 12416 2 台 NE16(VRP3.10) 10 台	BGP,OSPF	华为和 Cisco 在核心，华为在边缘	Internet
甘肃通信 169	NE80(VRP3.10) 3 台 NE40(VRP3.10) 2 台 GSR 12416 2 台	EBGP OSPF	Cisco 在核心，华为在边缘	Internet, MPLS L3 VPN 跨域
新疆通信 169 骨干网	NE80(VRP3.10)3 台 GSR 12012 2 台	BGP,OSPF	华为、Cisco 在核心，华为在边缘	Internet
陕西通信 169 骨干网	NE80(VRP3.10)9 台 GSR 12016 2 台	BGP,OSPF	Cisco 在核心，华为在边缘	Internet
陕西广电 163 骨干网	NE80(VRP3.10)12 台 M160/M40 2 台	BGP,OSPF	华为、Juniper 在核心，华为在边缘	Internet, MPLS L3 VPN
河南 CRNET 骨干	NE80(VRP3.10)10 台 GSR 12416/12012 6 台	BGP,OSPF	Cisco 和华为混合组网，同时在核心和边缘	Internet
长城宽带全国骨干网	NE80(VRP3.10) 3 台 M20 3 台 Cisco GSR 2 台 Cisco 75xx 40 多台	BGP,IS-IS	华为、Juniper 在核心，Cisco 在边缘	Internet

中国广电骨干网	NE80(VRP3.10) 2台 M160/M40 40多台	BGP,OSPF	Juniper 在核心，华为在边缘	Internet
英国FiberNET国家骨干	NE80(VRP3.10) 40多台 对端设备 Cisco 124xx	BPG,ospf	华为承建全网，与其他运营商的Cisoc 设备之间运行EBGP	MPLS L2 VPN
泰国 TA 国家骨干	NE80(VRP3.10) 90多台 对端设备 Cisco 12xxx	BGP,OSPF	华为承建全网，与其他运营商的Cisoc 设备之间运行EBGP	Internet, MPLS L2/L3 VPN

华为路由器包括NE、AR系列产品，采用统一VRP软件系统，具有良好的兼容性。NE、AR 路由器与思科、Juniper 路由器进行过多次权威的第三方互通测试。在运营商和各个行业用户现网上，NE、AR系列产品互通性和兼容性经受了大规模实际应用的考验。

8. 业务接入方案

8.1. 总体规划原则

福建电力调度数据网的业务包括调度中心及各厂站的各种应用系统，一般通过局域网交换机将业务接入到骨干网PE。

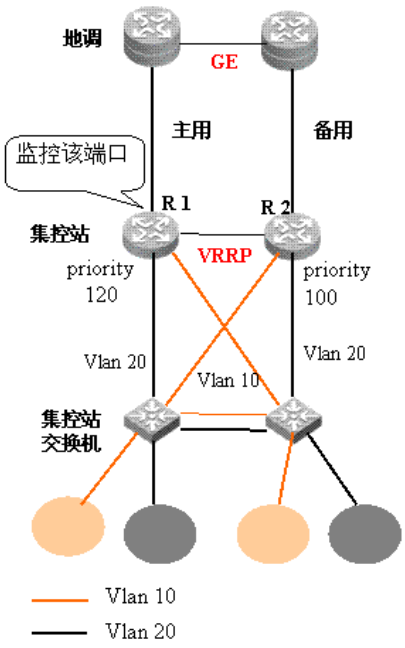
各应用系统通过其通信前置机或通信网关与交换机连接，一般主机或业务系统通过默认路由指向本地局域网的路由网关而与远程通信，并利用的网关的三层

特性隔离局域网的本地流量及广播报文不进入骨干设备，并在局域网内采用802.1Q 标准的 VLAN 技术实现不同应用系统的隔离。

8.2. 各节点业务系统接入

本期调度专网承载的业务按照安全区分区要求划分为 2 个 VPN 分别进行信息交换，分别为安全区 I VPN 和安全区 II VPN，对应实时和非实时二类业务，二类业务存在于各个节点（厂站及调度中心）。各业务系统通过 FE 端口接入当地调度数据专网交换机。为了保证各级节点调度数据的可靠在每个节点都配置 2 台交换机提供业务接入。

对于具体实现方式见下图



集控站两台路由器 R1 和 R2 启用 VRRP 协议，虚地址作为服务器的网关；假设缺省 R1 线路主用，可以规划 R1 作为主用路由器，R1 作为 vlan10 和 vlan20 主用网关，缺省时候 vlan10 和 vlan20 的数据都通过 R1

上行地调；一旦 R1 出现故障，R2 将自动接管虚地址，两个 vlan 的数据通过 R2 上行。

VRRP 协议还可以监控端口，这样可以避免数据绕行。比如缺省 R1 主用，VRRP 协议可以监控 R1 的上行端口，一旦 R1 的上行端口出现故障，VRRP 协议

将自动把 R1 的 priority 值减小（具体数值可设），让 R2 获得虚地址，承担起数据转发的责任；否则，如果不监控端口并进行 VRRP 状态切换，当 R1 上行口故障时候，R1 还是两个 vlan 的网关，两个 vlan 的数据将先发到 R1，然后 R1 再通过两台交换机，转发给 R2，进而上行到地调。

由于地调与 110KV 变电站的接入方式与县调一样，因此实现方案和集控站完全一样。

9. MPLS VPN 设计和配置

9.1. VPN 部署方案

福建电力数据网采用 MPLS VPN 实现业务的安全接入。

三层 MPLS VPN 的基本能力由 RFC2547 描述，考虑到目前路由数目和流量不是很大，采用普通的 MPLS VPN 方式部署。

福建电力调度数据网中路由器设备：包括骨干路由器、汇聚路由器、接入路由器，全部启用 MPLS。

骨干层、汇聚层、接入节点通过接入交换机接入本地业务系统，均做为 PE。在节点内部，各业务系统以 VLAN 方式隔离，或以不同交换机接入到 PE，在 PE 上以 VLAN 方式接入。

本次工程在莆田、泉州、厦门、漳州、龙岩、三明、南平各增加一台备份路由器，福州局增加两台路由器，宁德采利用福州局替下的路由器形成冗余网络。这样在骨干层就会形成 7206＋NE16E、NE16E＋NE16E、7206＋7206 的三种组合，根据骨干层的三种组合 MPLS/VPN 部署有两种方案。

方案一：四级网全网设备都实施分层 PE 技术。

方案二：只在集控站实施分层 PE 技术。

9.1.1. 方案一

按照目前福建电力调度四级网的拓扑设计要到跨域非常困难，不采用跨域方式就面临以下问题：

- 由于 MPLS/VPN 是扁平结构，所有设备都要维护 VPN 的路由信息，这样对于三级网的骨干设备同时维护三级网的路由信息又要维护四级网大量新增设备的路由信息，会大大增加设备的负载，对于 7206 的性能是一个严峻的考验，同时四级网接入设备也要维护大量路由信息，也会对设备的性能产生影响
- 用不跨域方式如何控制两级调度数据网之间的路由发布就成了一个问题，不

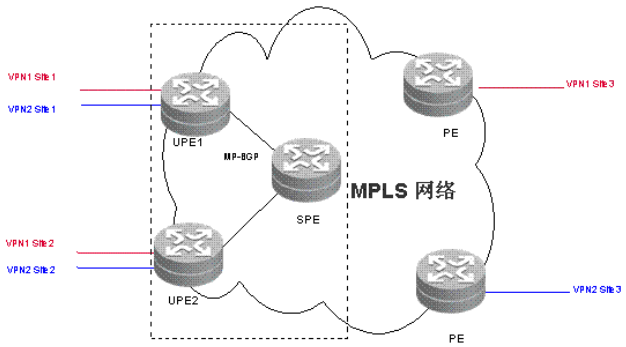
能把地区调度数据网的所有路由都发布到省网之中，一是会对省网的稳定造成巨大的影响，二是省网只是需要地区调度数据网之中某个节点的数据，这就需要地区调度数据网只能发布给省网需要互通的私网和公网路由（Loopback 地址），要在同一个 AS 域做到这点是非常困难的。由于无法做到很好的路由控制，地区调度数据网的大量路由信息势必会发布到省级调度数据网之中，从而影响省级调度数据网的正常运行。

由于福州地区的设备全部华为的路由器，就可以利用华为公司的分层 PE 技术解决这个问题，即实现了跨域方式中良好的路由控制，又减少设备的压力

分层 PE 的结构如下图所示，直接连结用户的设备称为下层 PE(Underlayer PE 或 User-end PE，用户侧 PE)，简写为 UPE，连结 UPE 并位于网络内部的设备称为上层 PE(Superstratum PE 或 Sevice Provider-end PE，服务运营商侧 PE)，简写为 SPE。这种框架结构称为 PE 的分层结构(Hiberarchy of PE)，简写为 HoPE。

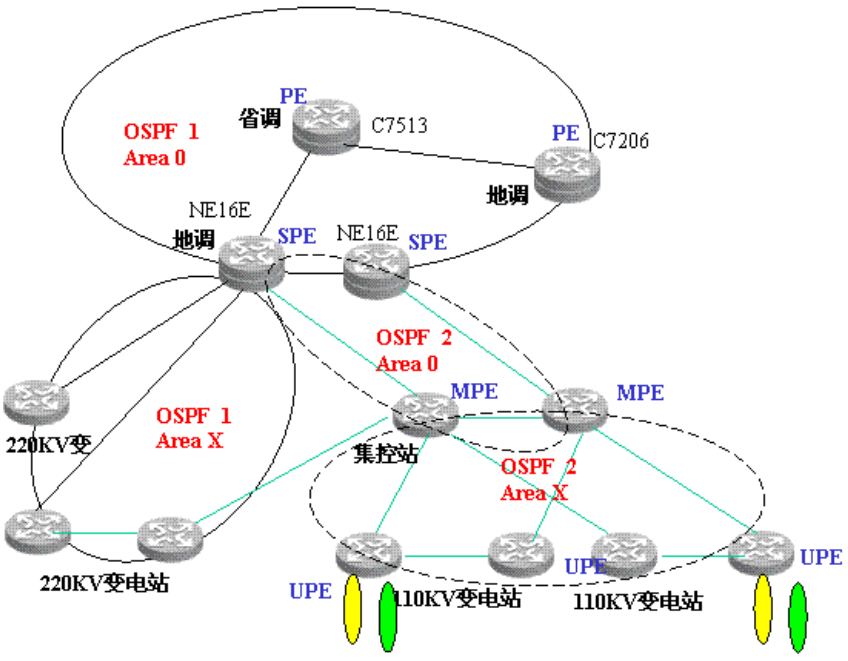
多个 UPE 同 SPE 构成分层式 PE，它们之间的分工是：

- UPE 维护其直接连接的 VPN 的路由，但不维护 VPN 中其它节点的路由或仅维护它们的聚合路由；SPE 维护其通过 UPE 所连接的节点所在的 VPN 中的所有路由，包括本地和远程节点中的路由。
- UPE 为其直接连接的节点的路由分配内层标签，并通过 MP-BGP 随 VPN 路由发布这个标签给 SPE；SPE 不发布远程节点中的路由给 UPE，而是只发布 VRF 默认路由或聚合路由给 UPE，并携带标签。



分层式PE

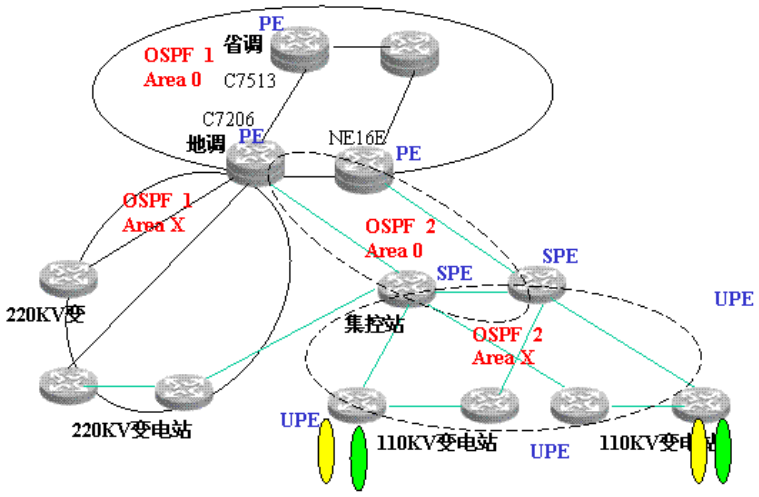
采用分层 PE 技术后 SPE 就成 UPE 设备的代理包括公网路由和私有路由，更上一级设备根本感知不到 UPE 的存在，如果想与 UPE 互通只需要与 SPE 互通就可以了，这样通过分层 PE 技术就可以做到与跨域方式一样的路由控制。在第二种组网方式中地市调度数据网的设备直接接入到省级调度数据网的设备上会对省网产生一定的影响，建议再添加一台或两台设备做为地区调度数据网的核心设备，与省级调度数据网的设备进行互联。然后将核心设备配置为 SPE，汇聚设备（集控站/县调）设为 UPE，由于分层 PE 技术支持嵌套，因此汇聚设备还可以是接入设备的 SPE 担当 MPE，接入设备为 UPE，这样通过分层 PE 技术减少骨干和汇聚层设备上面的路由信息。同时省网如果想与地区调度数据网中的某个节点互通只需要与四级网的核心设备互通，而不需要知道这个节点的精确路由即路由控制无需连接四级网中的低端设备，不但解决四级网有大量节点接入到省级调度数据网的问题，同样可以到达跨域方式的屏蔽网内拓扑及具体设备的效果。



福州地调设备全为NE16E，集控和110KV变也全为华为3Com设备。

9.1.2. 方案二

对于除福州以外的地区由于骨干层设备无法做到全部为华为设备，为了减少路由数量，由于汇聚层和接入层全部是华为设备可以在接入层因此在汇聚层和接入层运行分层 PE 技术，汇聚层设备做为 SPE，接入层做为 UPE，通过分层 PE 减少 7206 上面的路由数量，降低对 7206 的压力。



有七个地调设备为C7206和NE16E共存，集控站和110KV变电站为华为3Com设备

9.2. VPN 相关公共资源规划

9.2.1. VRF 命名规则规定

实时 VPN：vpn-rt

非实时 VPN：vpn-nrt

RD—router distinguish 命名规则

使用 16bits：32 bits 格式，分配规则为 『AS 号：VPN 类别』。其中 AS 号统一使用骨干 AS 号 300XX；VPN 类别：实时 VPN——100AA1；非实时 VPN——100AA2。

设备	实时 VPN 的 RD	非实时 VPN 的 RD
骨干/骨干接入节点和接入层设备	300XX：100**AA**1	300XX：100**AA**2

RD 中黑体字部分 AA 参见地调基本编码，该编码采用各地区电话区号的后两位：

福州-91	莆田-94	泉州-95	厦门-92	宁德-93
漳州-96	南平-99	三明-98	龙岩-97	

9.2.2. RT—Route-target 命名规则

使用 16bits：32 bits 格式，分配规则为 『AS 号：VPN 类别』。其中 AS 号统一使用骨干 AS 的 300XX。

四级网具体的访问规则如下：

- 同一 VPN 内：地调与集控站可以互访、地调与地调所属接入路由器可以相互访问；
- 同一 VPN 内：集控站与本身所属接入路由器可以相互访问。
- 同一 VPN 内：原则上集控站与集控站之间不可以相互访问，接入路由器与接入路由器之间不可以相互访问。
- 不同 VPN 内的设备肯定不可以相互访问。

实时和非实时 VPN RT 规划列举见下表：

设备类型	RT（Import）	RT（Export）	NRT（Import）	NRT（Export）
地调路由器	300XX:100AA1	300XX:200AA1	300XX:100AA2	300XX:200AA2
接入路由器	300XX:200AA1	300XX:100AA1	300XX:200AA2	300XX:100AA2
集控站路由器	300XX:200AA1	300XX:100AA1	300XX:200AA2	300XX:100AA2

如福州地区四级网 RT 规划：

设备类型	RT（Import）	RT（Export）	NRT（Import）	NRT（Export）
地调路由器	300XX:100911	300XX:200911	300XX:100912	300XX:200912
地调所属接入路由器	300XX:200911	300XX:100911	300XX:200912	300XX:100912

集控站路由器	300XX:200911	300XX:100911	300XX:200912	300XX:100912

每个集控站路由器在上述基础上再**增加**如下规则：

设备类型	RT（Import）	RT（Export）	NRT（Import）	NRT（Export）
集控站路由器	300XX:1AA**BB**1	300XX:2AA**BB**1	300XX:1AA**BB**2	300XX:2AA**BB**2
集控站所属接入路由器	300XX:2AA**BB**1	300XX:1AA**BB**1	300XX:2AA**BB**2	300XX:1AA**BB**2

其中每个集控站的黑体字部分 **BB** 参见下面集控站基本编码，该编码采用集控站所属 OPSF 的区域号（每个集控站一个区域，以 14 个集控站举例）

集控 1-01	集控 2-02	集控 3-03	集控 4-04	集控 5-05	集控 6-06	集控 7-07
集控 8-08	集控 9-09	集控 10-10	集控 11-11	集控 12-12	集控 13-13	集控 14-14

如果不同集控站之间存在互访需求，则在两台集控站设备上同时增加如下 RT 规则：

设备类型	RT（Import&Export）	NRT（Import&Export）
集控 1 路由器	300XX: AA**BBCC**1	300XX:AA**BBCC**2
集控 2 路由器	300XX: AA**BBCC**1	300XX:AA**BBCC**2

其中：**BBCC** 分别是集控 1 和 2 的基本编码，序号小的放在前面。

例如：集控 1（01）要求与地调互访，与下面的所属接入路由器互访，与集控 3（03）和集控 14（14）两个集控站互访，则在集控 1 上的 RT 规则为：

设备类型	RT（Import）	RT（Export）	NRT（Import）	NRT（Export）
集控 1	300XX:200911 300XX:100911 300XX:191011 300XX:9101031 300XX:9101141	300XX:100911 300XX:200911 300XX:291011 300XX: 9101031 300XX: 9101141	300XX:200912 300XX:100912 300XX:191012 300XX:9101032 300XX:9101142	300XX:100912 300XX:200912 300XX:291012 300XX: 9101032 300XX: 9101142

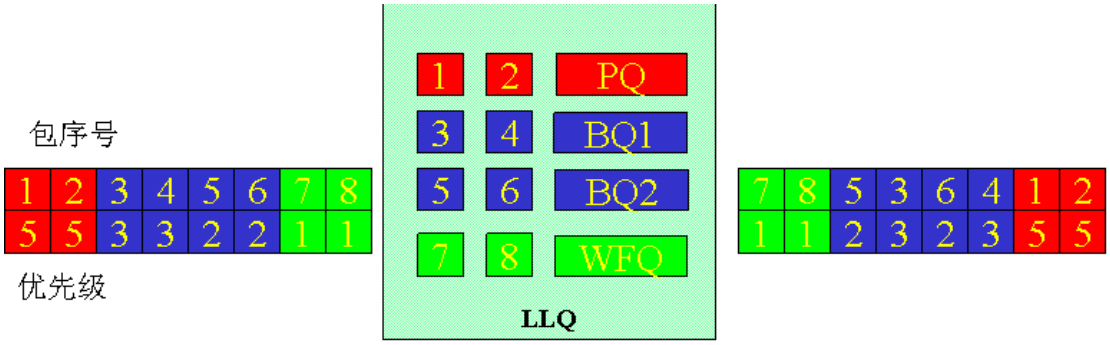
以上四级网中 **VPN** 互访控制的举例，如果三级网要与四级网进行互访控制，方法与上面完全一致，都是通过控制 **RT**，即在需要互访的两个站点同时增加相同 **Import** 和 **Export** 配置。

10. QoS 部署方案

福建电力调度数据网采用 Differ Serv，主要有实时业务、非实时业务等。实时业务：EF 业务，（即保证带宽，又保证时延）；非实时业务和网管业务：AF 业务（保证带宽，时延要大于 EF 业务）；其它业务：BE 业务，无带宽和时延保证，在网络不发生拥塞时可以保证服务质量。

QOS 保证的实现举例如下：在本地以太网交换机到路由器的出口处，进行流分类、流标识、CAR 限速、802.1p 映射、GTS 整形等操作。将业务设置为不同的优先级。

- 实时业务：Ip Precedence=5
- 网管数据：IP Precedence=3
- 非实时业务：IP Precedence=1



在骨干网中实施基于 CBWFQ/LLQ 的队列调度，保证带宽和优先级。在发生拥塞时，如果 1、2 为实时业务，3、4 为网管数据，5、6 为非实时业务，7、8 为其它数据。按照 8、7、6、5、4、3、2、1 的顺序到达，通过 LLQ 队列调度后，将实时业务映射到 PQ 中，将准实时业务和网管数据映射到 BQ 中，将其它数据映射到 WFQ 中，通过相关调度算法，发包顺序变为 2、1、4、6、3、5、8、7，实现了给不同的业务，提供了不同的等级的 QoS 服务。

福建电力调度数据网的 MPLS/BGP VPN 应用中，在 VPN 网络内部可以对报文进行分类、着色，各种 QoS 处理。报文在骨干网 PE 间传送时，QoS 属性被透传到对端 PE，中间不会被修改。

另一方面，在骨干网上可以对 VPN 用户的数据流进行 QoS 处理。使用 MPLS

报文标签头的 EXP 字段保存 COS，在网络中按照既定的规则，将不同 COS 值的报文对应于不同的 PHB，按照相应规则进行队列调度，报文丢弃等处理。这里 COS 的值在入口 PE 上被设定，将 VPN 用户 IP 报文的优先级或 DSCP 值映射为 MPLS 报文的 COS 值，这里设定的服务类型仅在骨干网内有效。

用 LLQ 进行 QOS 保障的实现举例如下：在以太网交换机上，将业务设置为不同的 IP 优先级。在路由器上将 IP 优先级映射为 MPLS 优先级。

实时业务中的 EMS 业务：Ip Precedence = 5，进入 LLQ 队列，占用 200K 的带宽；

按照如上调度原则，当网络发生拥塞时调度方式如下：当网络发生拥塞时，PQ 队列将确保至少 200K 的带宽，但是如果 PQ 队列的流量也超过 200K 时，超过的部分将得不到带宽保证，而会被随机丢弃。

11. 网络管理方案

11.1. 总体需求

福建电力数据网将在福建省调建立一套全网网管中心系统（对整个网络的设备进行设备管理），及一套 VPN 网管系统（对整个网络的 VPN 进行管理，包括业务部署、业务监控）。

全网网管中心全面负责全网设备的管理，能对全网所有设备进行监视和控制，包括网络中 P、PE、CE 设备的管理。VPN 网管系统对 VPN 提供提供部署、审计、监控 PE 连接状态、流量统计功能。

根据福建电力数据网网络规模的要求，采用华为 Quidview 网管系统对其进行网络管理。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。

11.2. 对 PE 与 CE 设备统一网管

本次工程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 L3 上使用 VLAN Trunk 功能）。每台 CE 设备的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，直接连接在福建省调局域网上。

11.3. 网管职能划分

- 拓扑集中显示

直观显示整个网络，提供多种不同的视图，使管理员从不同的角度掌握全网资源状况和运行状态；并且提供便捷的功能入口，在网络拓扑上可以完成大部分的管理操作。

- 故障集中监控

直观显示整个网络的故障状况，提醒管理员告警的发生和清除；以便管理员监控整个网络的运行情况，并采取相应的措施。

11.4. VPN 网管

福建电力数据网的 VPN 网管通过 VPN Manager 系统实现，该系统立足于管理 MPLS VPN 网络，实现客户管理、业务部署、性能监控和故障监控功能的无缝融合，是开展 MPLS VPN 业务的管理工具。

VPN Manager 可以提供端到端 VPN 业务管理解决方案。

VPN Manager 解决了 VPN 业务管理中必须解决的以下问题：

- 直观的、可观察的业务规划
- 快速的、可调度的业务部署
- 已部署业务的发现
- 业务故障告警、检测
- 客户管理
- 全网资源管理
- 网络性能监控
- 多厂商设备的管理

VPN Manager 的功能覆盖了 VPN 业务的整个生命周期的管理，从业务规划、业务审计、业务部署到业务监控。

VPN Manager 同样接在福建省调（主）的局域网下，为了便于统一管理 VPN Manager 采用与设备网管相同的物理设备。

11.5. 路由器/交换机相关参数设置

11.5.1. SNMP 相关版本设置

SNMP 协议的相应版本，本次工程统一使能 SNMP V2 版本。

11.5.2. SNMP 设置团体名

SNMPV2 采用团体名认证，与设备认可的团体名不符的 SNMP 报文将被丢弃。SNMP 团体（Community）由一字符串来命名，称为团体名（Community Name）。不同的团体可具有只读（read-only）或读写（read-write）访问模式。具有只读权限的团体只能对设备信息进行查询，而具有读写权限的团体还可以对设备进行配置。

11.5.3. 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 地址或管理地址。

12. 网络安全方案

12.1. 通过 MPLS VPN 确保不同类型业务及地域之间的有效隔离

VPN 技术具有天然的安全特性，不同的 VPN 用户之间由于无法获知对方的路由信息，从而可以理解为存在于不同的私有网络之中，而 MPLS VPN 由于在公网中使用 LSP 隧道进行标签交换，较之普通的 IP 转发具有更好的安全级别。

本次工程通过规划两大类 VPN（实时与非实时），确保两种不同业务之间的设备无法获知对方的路由信息。在同一种业务中通过对 MPLS VPN 中 RT（Route-Target）属性的合理设置，可以保证即使是相同的业务，如果没有互访需求，也无法相互访问。

12.2. 通过用户状态进行存取控制功能，保证设备控制安全

华为系列路由器和交换机的命令行提供分级保护功能，禁止低优先级的用户更改设备的重要配置，进入高优先级模式时进行密码验证。

用户的用户级别与命令优先级的关系是：用户只能使用命令优先级不大于用户级别的命令。用户可以根据自己的需要定义命令的优先级，使其在不同的用户级别下使用。

12.3. 限制对 SNMP 和 Telnet 用户访问

对远程登录用户，提供了 LINE 验证、本地验证和 AAA 验证三级验证。不同的用户可设置不同的用户级别，从而对设备有不同的操作权限（见上）。对 Telnet 用户还可进行的限制有：

- 配置 VTY 类型 LINE 的呼入呼出限制 telnet 用户访问

通过在 PE 设备上设置 ACL，限制只允许源地址为公网，并禁止其他所有 VPN 内部用户的私网地址进行登录。此项措施可以简单有效的防止 VPN 用户通过 CE 对 PE 设备进行非法访问。

- 配置团体名限制对设备的 SNMP 访问

SNMP 采用团体名认证，与设备认可的团体名不符的 SNMP 报文将被丢弃。SNMP 团体（Community）由一字符串来命名，称为团体名（Community Name）。不同的团体可具有只读（read-only）或读写（read-write）访问模式。具有只读权限的团体只能对设备信息进行查询，而具有读写权限的团体还可以对设备进行配置。

12.4. 路由信息交换的认证

在运行路由协议的路由器上，有些端口具有不安全的属性，最据代表性的如以太网口，该类型的接口由于需要发布本接口网段的路由信息，所以需要启动路由协议，但由于以太网的广播属性，攻击者很容易将一台同样运行 OSPF 协议的路由设备连接到以太网中，并进而获得整网的路由信息及拓扑结构。所以必须在上述端口上启用 Passive interface 命令，启动该命令后，该接口的网段路由可以照常发布出去，但该接口不会再收发 OSPF 协议报文，也就不会再与任何其他路由设备建立邻居关系，从而避免了路由泄漏。

12.5. 对所有重要事件记录 log 日志

对于网络安全，不仅要关注网络的事前防范能力，更要做好对事后跟踪能力方面的考虑，在安全事件发生前后，可以通过对用户上网端口、时间、访问地的记录，全面提供用户上网的追溯能力，从而为后期的分析提供第一手的资料。

实际上日志记录等功能是一个非常良好的追溯手段，在出现问题时可以根据记录迅速查找源头，防止事态进一步扩大；同时可以通过法律惩治罪犯，以警后人。

- 利用 Syslog 记录重要的设备信息(如告警，设备状态变化信息)，可以为故障定位排除提供有利数据。

日志记录支持控制台（ console ）、Telnet 终端和哑终端（ monitor ）、日志缓冲区（ logbuf ）、日志主机（ loghost ）等多个方向的日志输出。在条件允许的情况下，对关键设备的日志输出建议采用日志主机的方式。