分组策略控制方案V1.0

一. 什么是GBPC

> **GBPC (`Group-Based Policy Control`) 即基于分组的策略控制模型。**

域管系统的核心业务就是对不同部门、领域或组织的终端进行精细化管控，而这个需求就可以设计为一个GBPC通用模型。

GBPC中的策略执行者(**Who**)可以是任何设备、控制单元、终端订阅者或它们的组合单元；策略接受主体要执行的动作即策略操作类型(**How**)，如：计划执行、被动触发、订阅内容、及时命令或执行脚本等。策略内容即为策略资源(**What**)。这它们构成了分组策略三元组(`EGP`)，即：Who对What进行How的操作。

一句话概括就是： **谁(Who)对哪些策略(What)资源具有什么样(How)的操作。**

- `Who`： 策略接受主体/执行者(如：User,Terminal,Group或Organize)，属于同一切面的执行者集合。
- `What`： 策略资源,具有唯一标识型，类型，名称，内容等属性
- `How`： 操作类型，如：计划执行、被动触发、订阅内容、及时命令或及时脚本等

GBPC主要包含四个子模型：GBPC0、GBPC1、GBPC2和GBPC3。

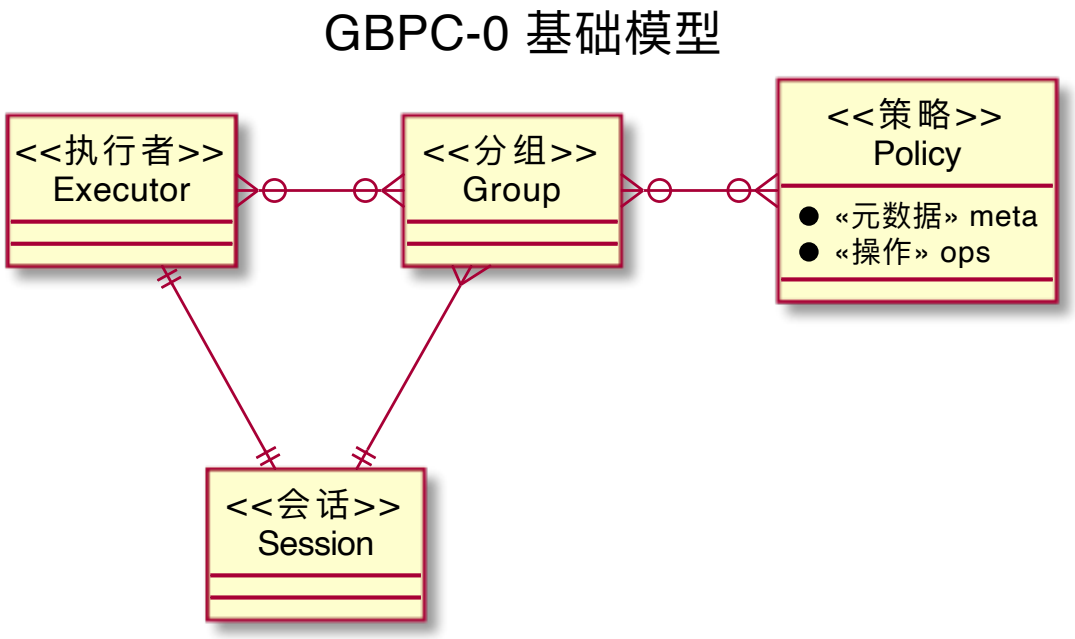
- GBPC0： 是GBPC的核心思想。
- GBPC1： 是把GBPC的分组 分层模型 。
- GBPC2： 增加了GBPC的 约束模型 。
- GBPC3： 其实是GBPC1 + GBPC2。

二. GBPC模型

2.1 GBPC0模型

GBPC0是GBPC的核心，主要由四个部分组成：**执行者(Executor)**、**分组(Group)**、**策略(Policy)**和**会话(Session)**。

这是一种多对多的分配关系：执行者对应多个分组、分组对应多个策略。执行者与会话一对一，会话与分组一对多。

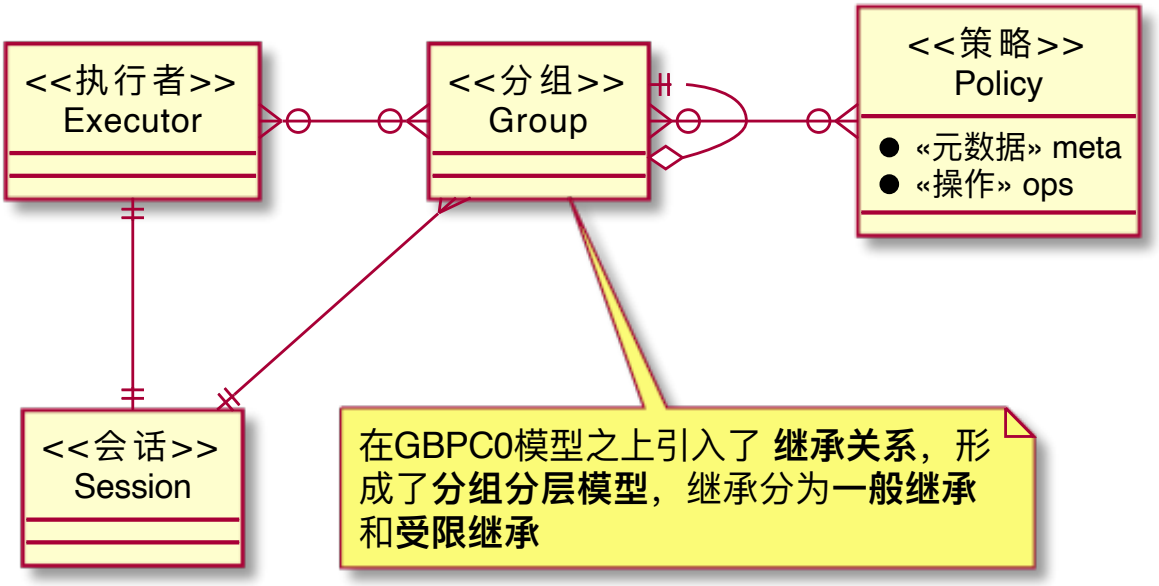


2.2 GBPC1模型

GBPC1 是在GBPC0模型基础之上增加了分组分层的概念和分组之间的继承关系。

- 一般继承： 一般继承是一个**叠加继承**(如:小组策略=部门策略+公司策略)，允许分组间的多继承。
- 受限继承：：受限继承是一个**单项继承**，它要求分组继承关系是一个树状结构，实现分组间的单继承。

GBPC-1 分层模型



2.3 GBPC2模型

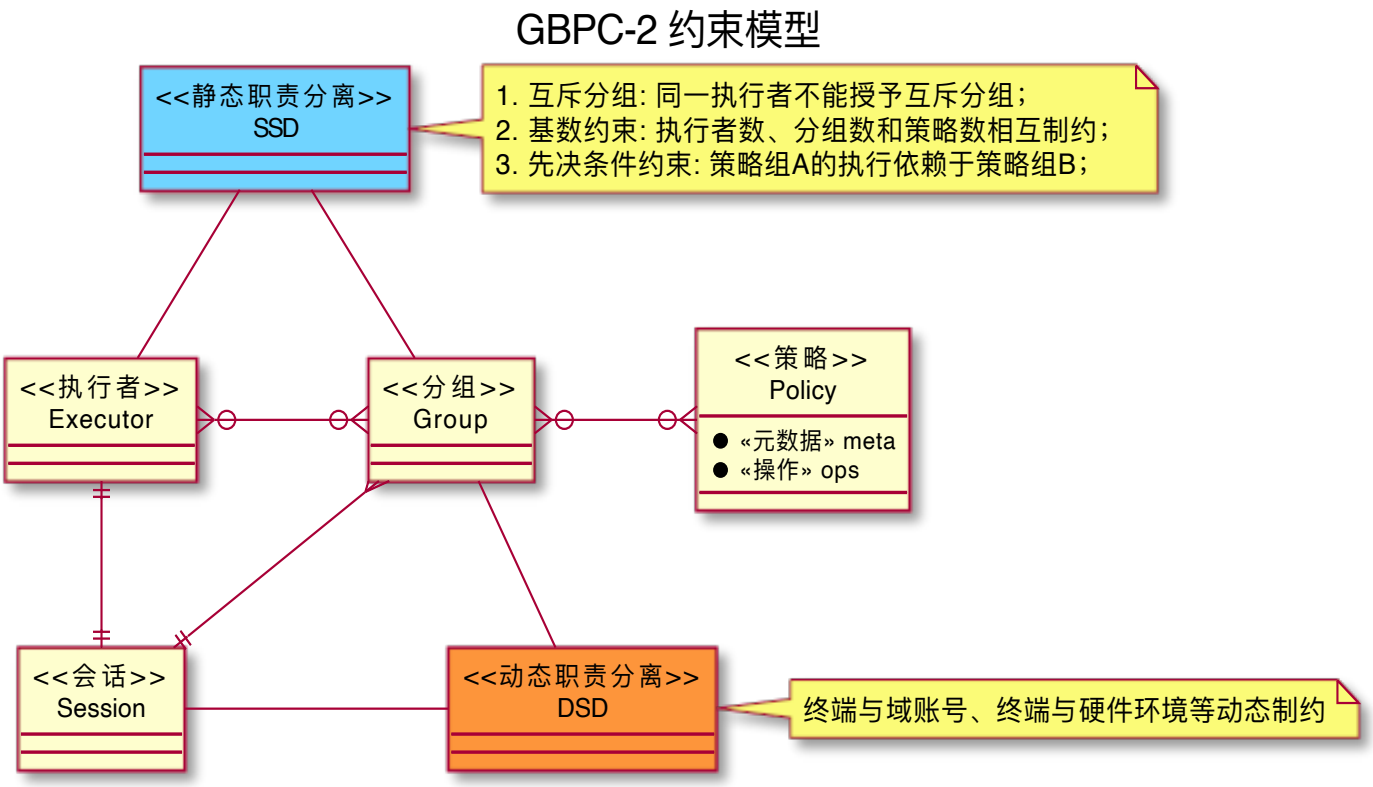
GBPC2 是在GBPC0模型基础之上引入了静态职责分离(SSD)与动态职责分离(DSD)概念。

静态职责分离：

- 互斥分组： 同一个执行者不能授予互斥关系的多个策略分组，如: `会计策略组` 与 `审计策略组` 互斥,`admin策略组` 与 `guest策略组` 互斥。
- 基数约束：
  1. 一个分组对应的 `策略数量` 应该是受限的；
  2. 一个分组中 `执行者数量` 应该是受限的；
  3. 一个执行者拥有的 `分组数量` 应该是受限的；
- 先决条件分组： 执行者想拥有A分组就必须先拥有B分组，即保证执行者拥有X策略的前提是拥有先Y 策略。 如： 执行 `启动X服务` 策略的前提是拥有 `安装X服务` 的策略。

动态责任分离：

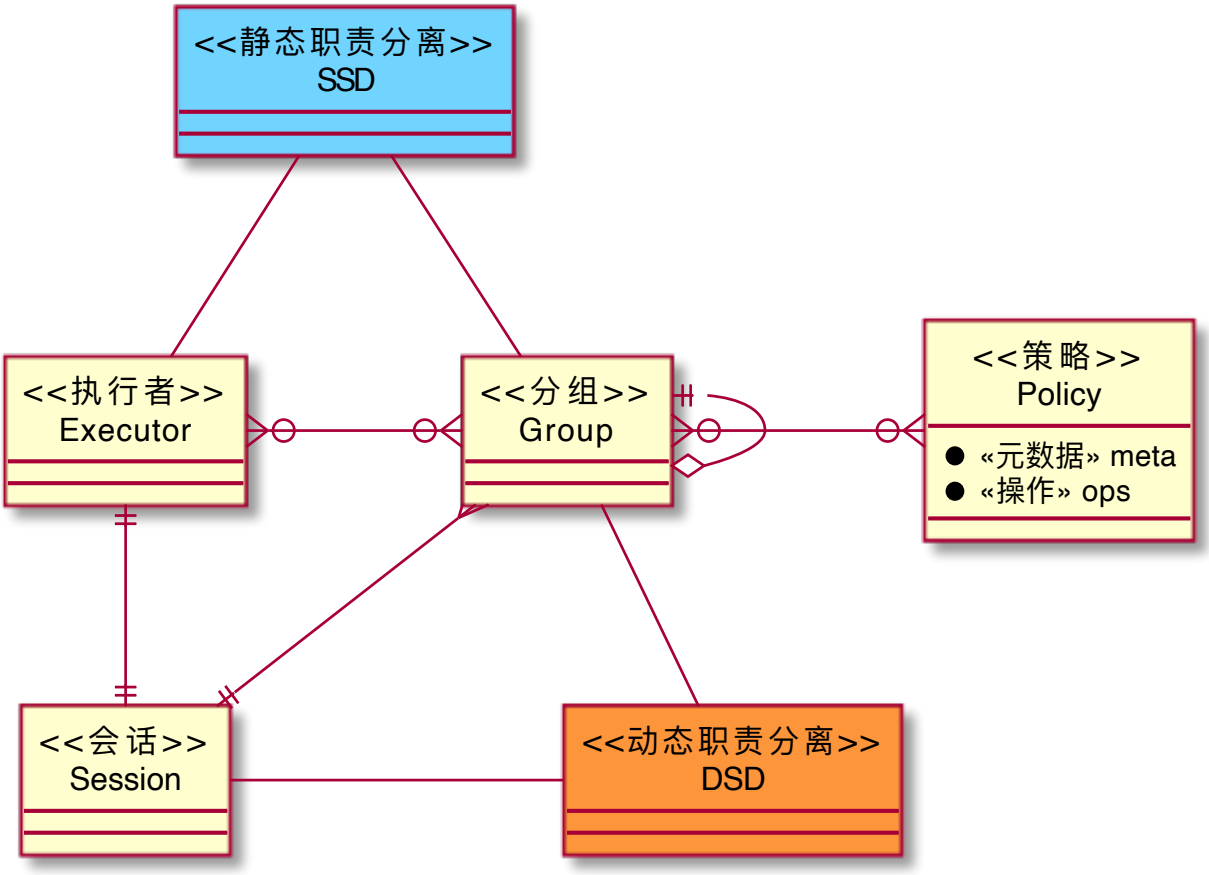
- 用户与终端变动不匹配的情况下，需要根据终端的域账号动态判断是否需要执行当前分组策略。



2.4 *GBPC3模型*

GBPC3 是集聚了GBPC1和GBPC2的全部特点，即 **GBPC3=GBPC1+GBPC2** 。

GBPC-3 组合模型

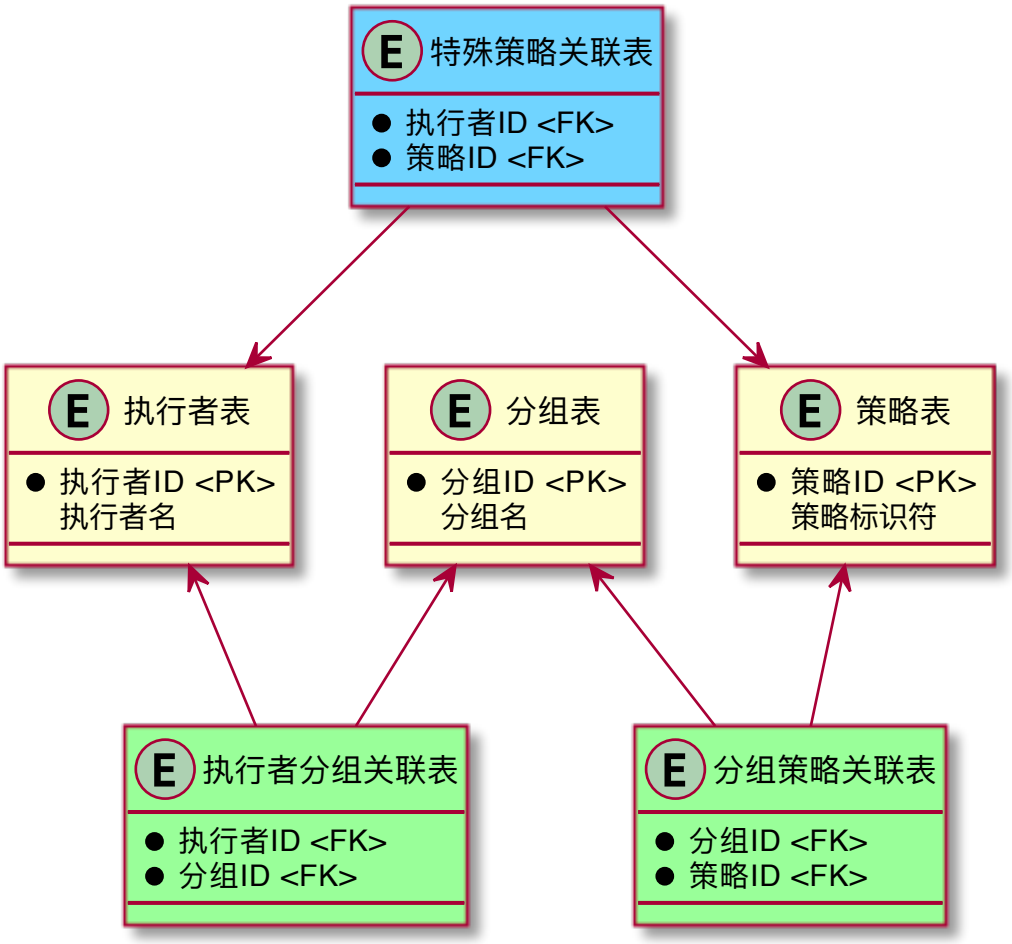


三. GBPC项目模型

3.1 *简单应用模型*

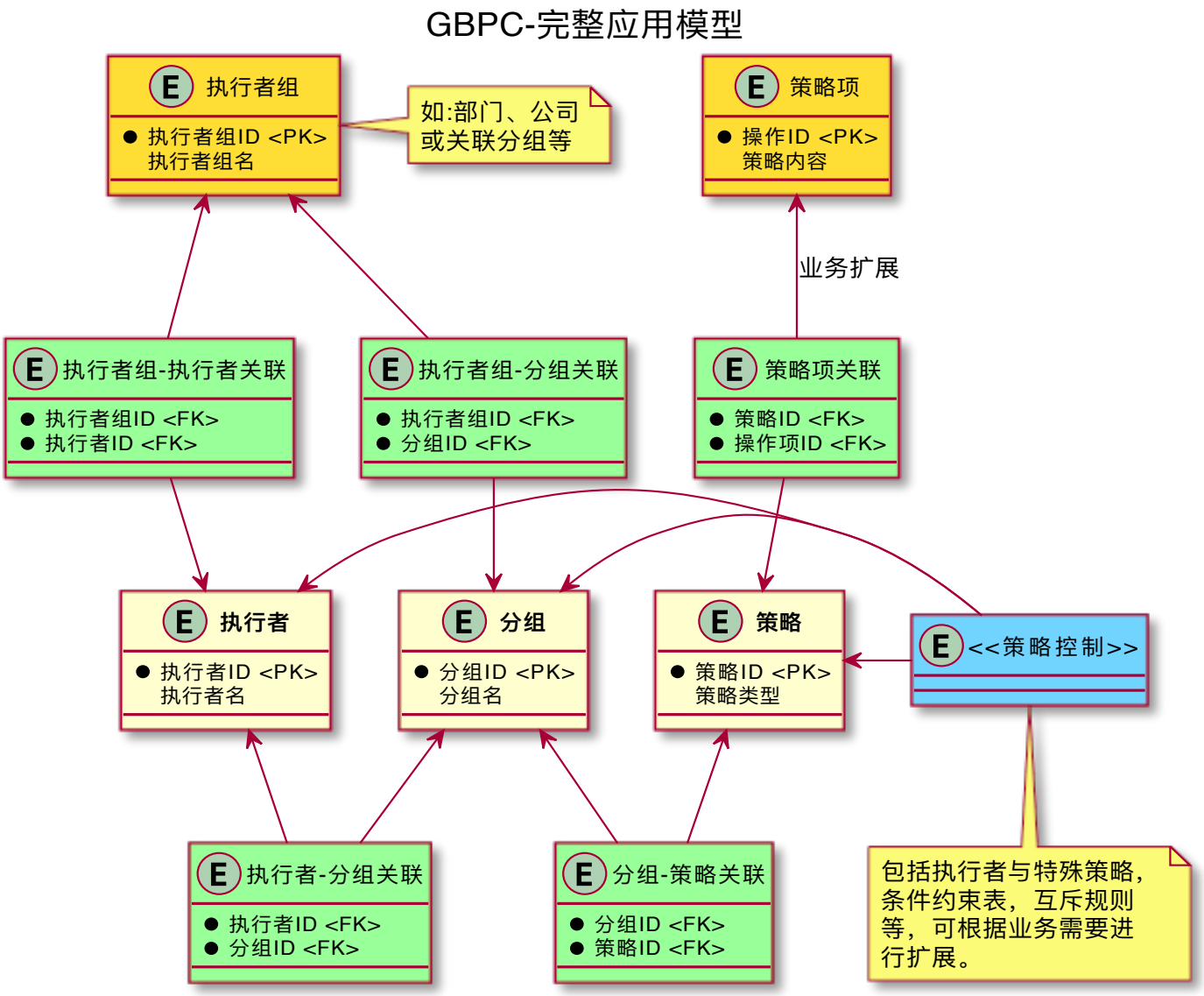
针对简单的策略系统，实体关系只需体现为执行者表、分组表、策略表和它们之间的关联关系。

GBPC-基础应用模型



3.2 *完整项目示例*

> 复杂的策略系统，核心实体仍然为**执行者**、**分组**和**策略**三元组，其余的实体均可抽象为**EGP扩展关联关系**，或**EGP**的**分类标签**。
>
> 域管策略系统本质上与操作系统策略无异，



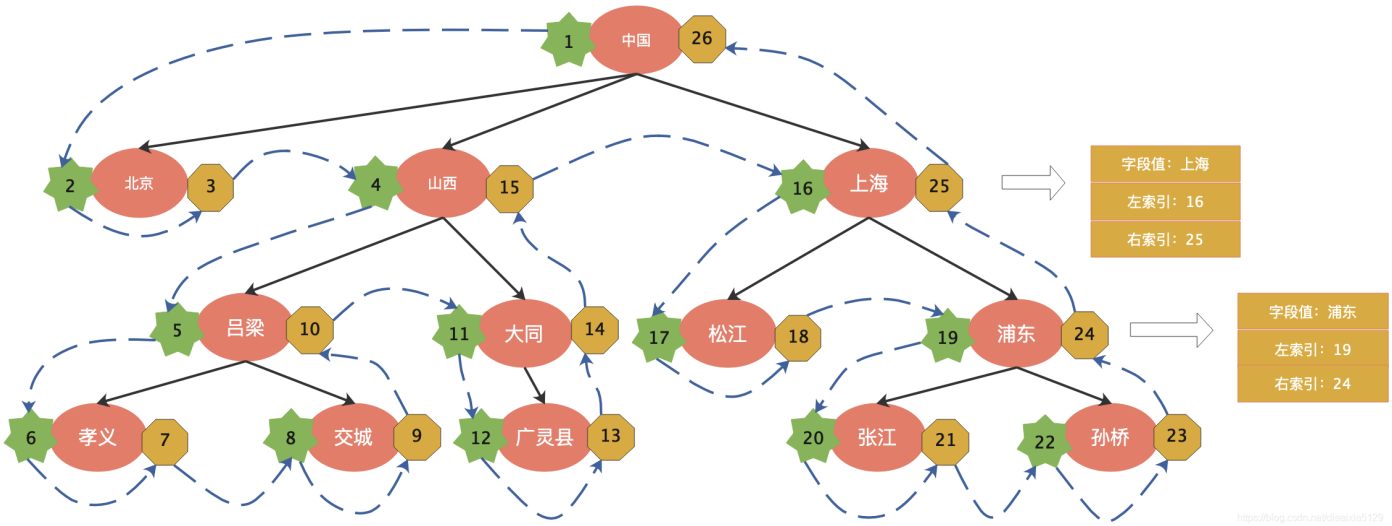
四. GBPC数据库设计

GBPC结构中较为难实现的就是嵌套分组关联，目前有以下三种数据库设计方案：

4.1 MPT

预排序遍历树算法(modified preorder tree traversal algorithm)

> 预排序的意思就是我们在查询前对存到数据库中的数据进行一次特殊的排序，给每条数据添加两个字段：左索引和右索引，添加的方式如下图所示

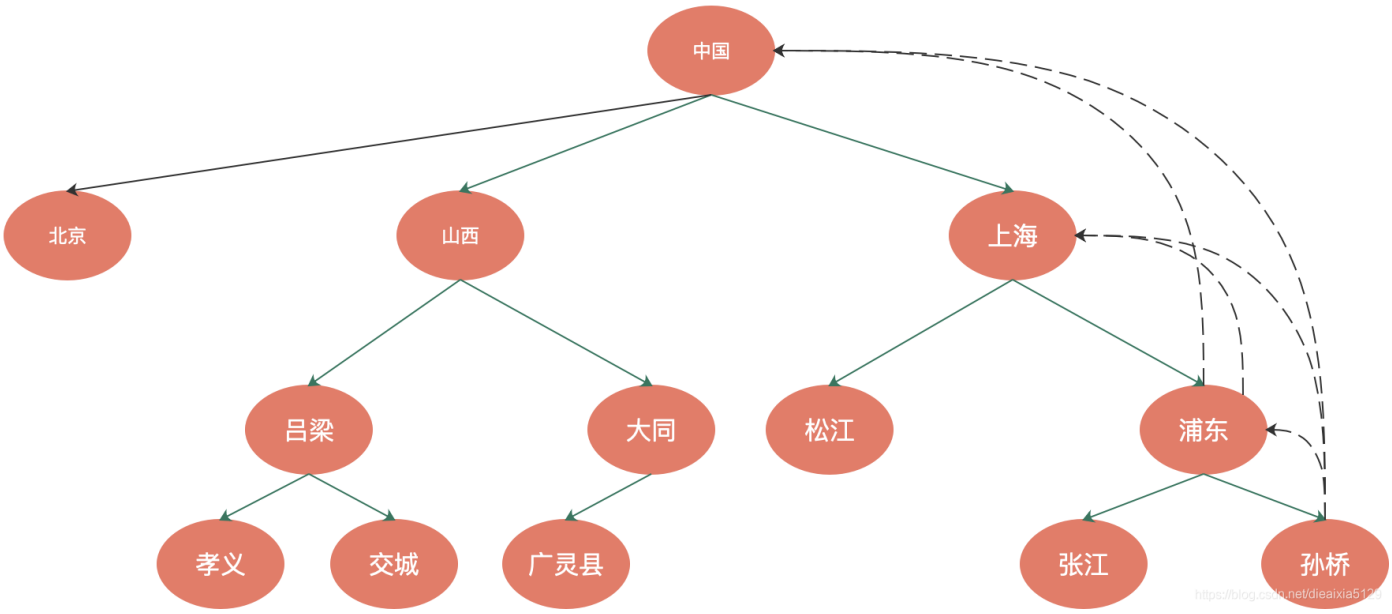


数据库中的表结构如下所示：

id	name	lindex	rindex
1	上海	16	25
2	浦东	19	24

4.2 *ClosureTable*

> 闭合表(ClosureTable)则是新增一张表，用于记录节点直接的关系（父节点，子节点，深度），如下图中的孙桥和浦东，会生成以下关系记录；



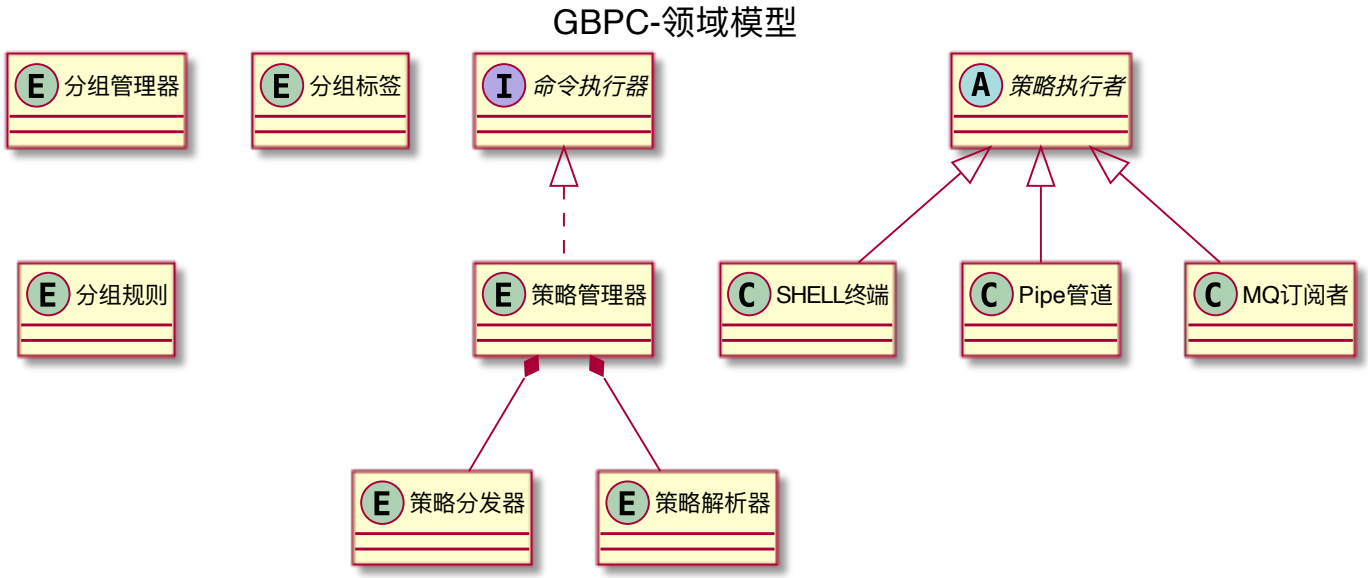
id	child	parent	deepth
1	孙桥	浦东	1
2	孙桥	上海	2
3	孙桥	中国	3
4	浦东	上海	1
5	浦东	中国	2
6	上海	中国	1

4.3 *GraphDB*

> 基于图数据库的设计(neo4j)：待验证...

五. GBPC领域建模

待续...



六. GBPC项目落地

参考： https://github.com/hollson/gbpc

参考链接

- https://wenku.baidu.com/view/879cb3cba7e9856a561252d380eb6294dc8822c1.html
- https://docs.microsoft.com/zh-cn/internet-explorer/ie11-deploy-guide/group-policy-objects-and-ie11

- https://en.wikipedia.org/wiki/Group_Policy
- https://segmentfault.com/a/1190000039204025
- https://www.toutiao.com/article/7005515203127345697