# 再谈网络故障诊断

电子科技大学

2015. 11. 24

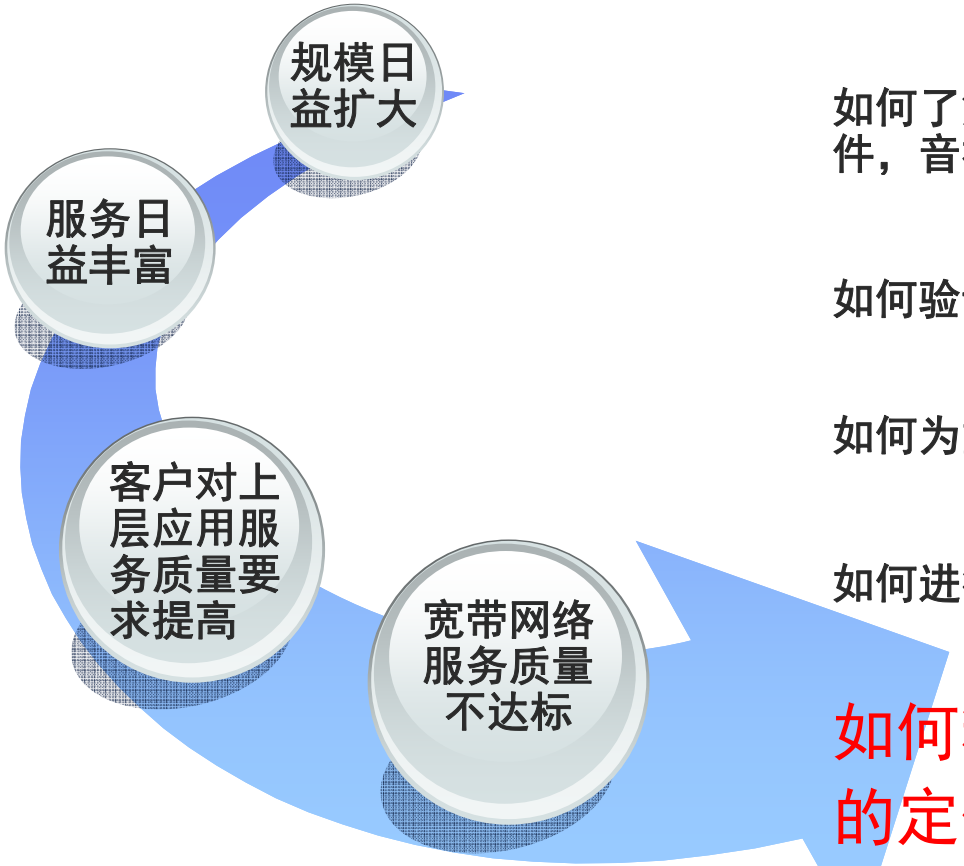
# 目录

# 提纲

## 智能故障诊断：业内的工作

# 智能故障诊断

## 宽带网络现状





如何提高对网络性能状况的感知度？

如何了解终端用户的感受？（浏览网页，件，音视频，……）

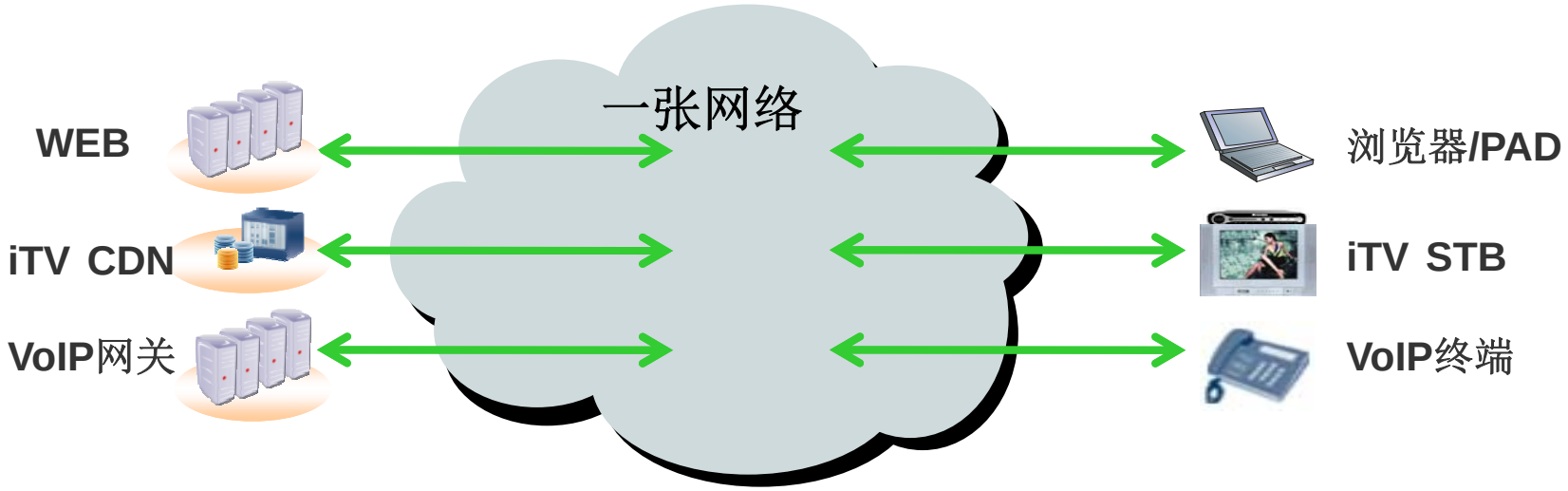
如何验证向用户提供的SLA承诺？

如何为重点客户提供定期的网络质量报告？

如何进行长时间（7×24）的性能监测以提前发现问题？

如何精准快速进行质量劣化等故障的定位和根因分析？

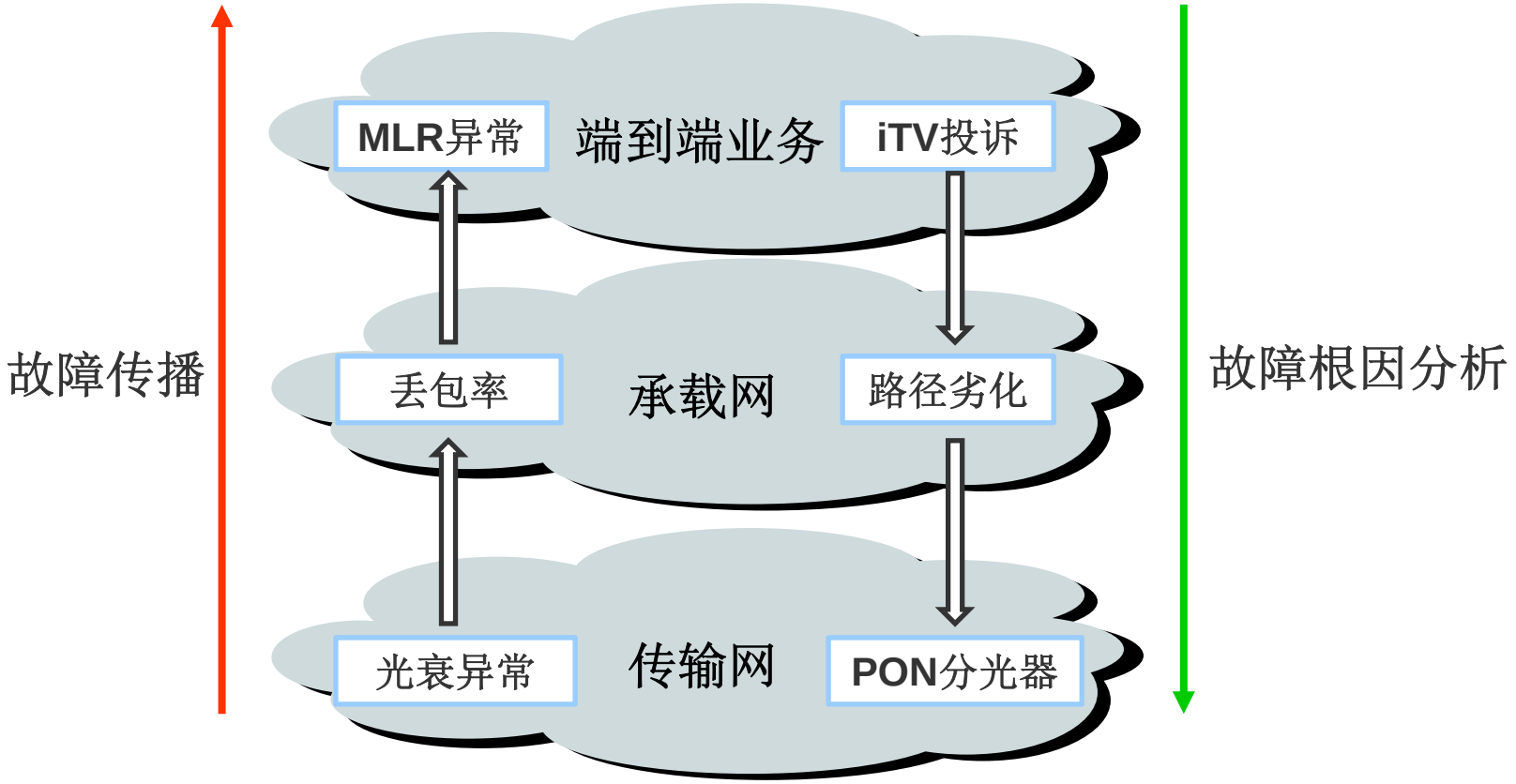
# 智能故障诊断




- 智能故障诊断：三个目的
  - 故障识别(fault identification)，或故障发现
  - 故障测试(testing)，或故障确认
  - 告警相关性分析(alarm correlation)，或故障定位

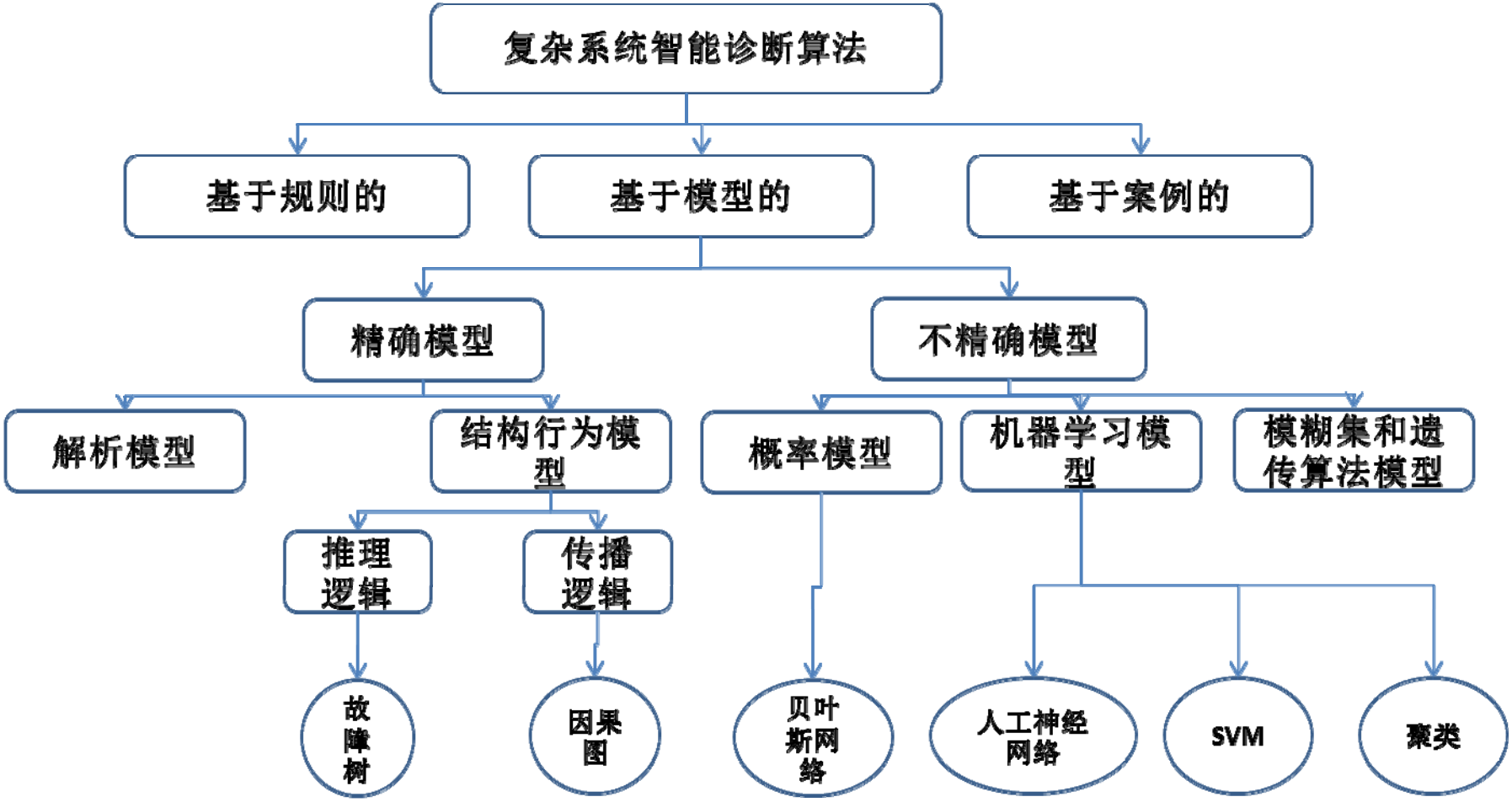
# 智能故障诊断

- 智能故障诊断：两个研究点



# 智能故障诊断

- 常见的智能诊断故障诊断方法



# 智能故障诊断

小结：从故障诊断方法的角度，可以分为两类人。

- “不懂网络的人”的方法
  - 机器学习、贝叶斯网络
  - 基于案例的推理

- “懂网络的人”的方法
  - 基于规则的推理、基于模型的推理

# 智能故障诊断

小结：从故障诊断依据的信息，也可以分为两类人。

- “懒人”所依据的信息
  - 告警事件（目前ISP共识）
- “勤快人”所依据的信息
  - 告警事件（“坏”消息）
  - 网络日常运行数据（“好”消息）

# 智能故障诊断——我们的工作

以下汇报我们的两种探索。

- 探索1：“不懂网络的勤快人”
  - 基于机器学习的故障检测与诊断(MLBR)
- 探索2：“懂网络的勤快人”
  - 基于模型的故障检测与诊断(RMBR)

# 目录

# 提纲

## 探索1：基于机器学习的故障诊断方法LMBR
## (Machine-Learning Based Reasoning)

# MLBR方法——主要思想

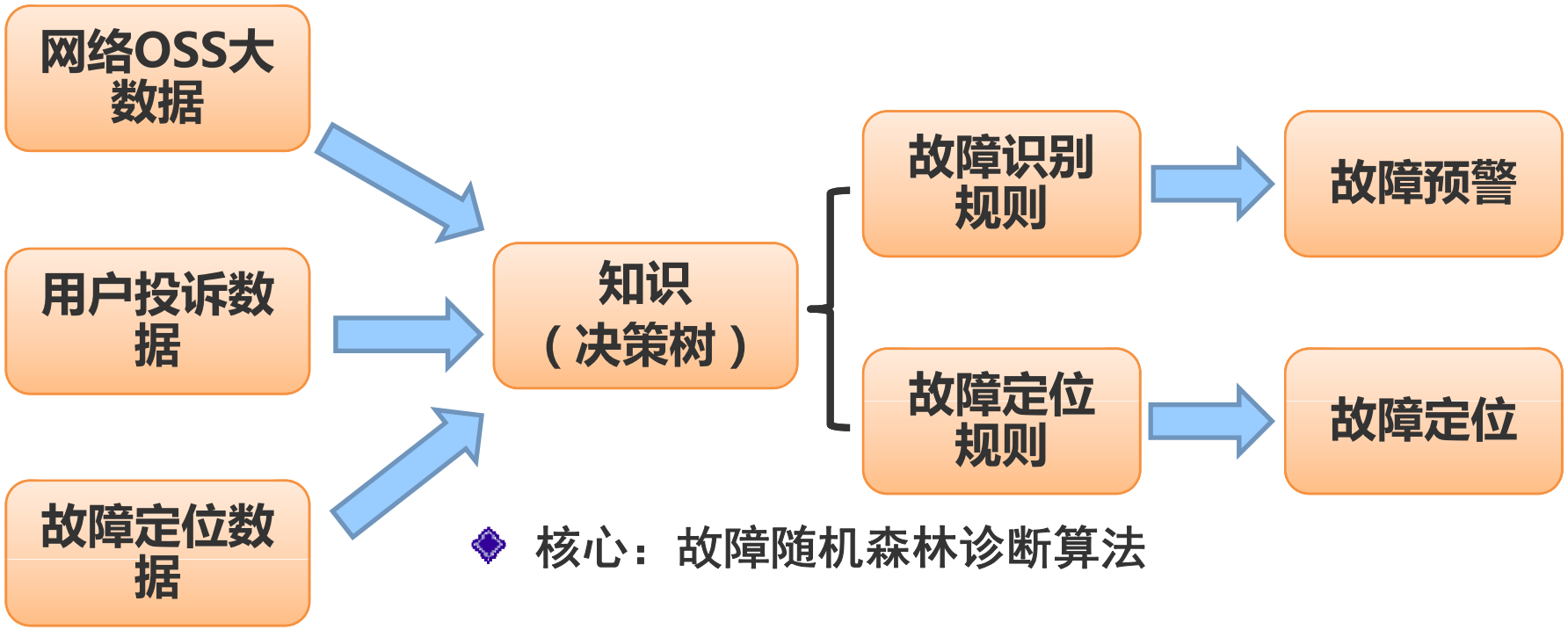
MLBR的两个出发点：

- 网络故障的规律是可学习、可挖掘的。

- 宽带网络的运行数据测量已经解决了故障状态数据采集的问题，剩下的就是对规律的学习和对知识的应用。

# MLBR方法——主要思想

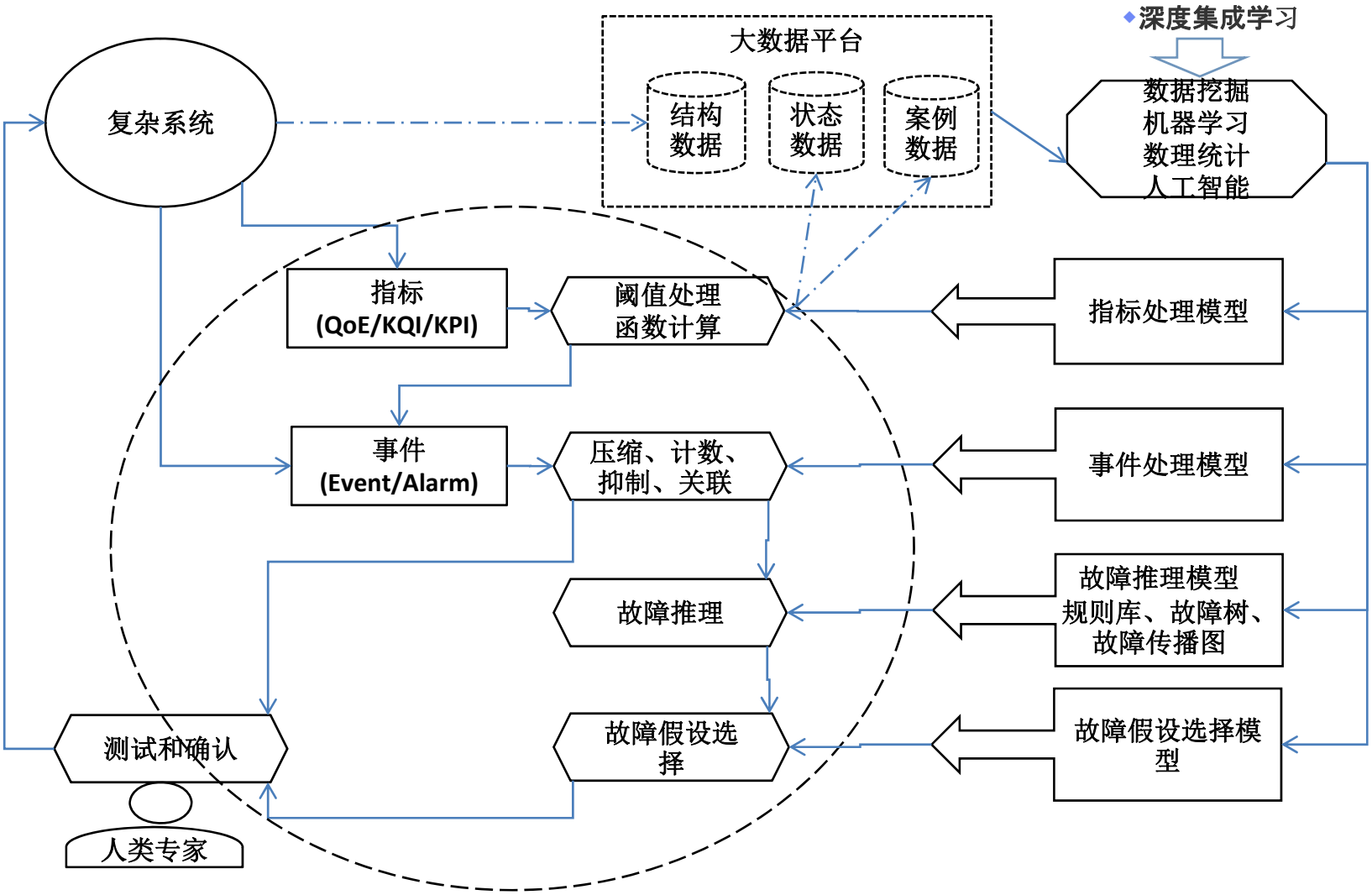
- 数据->学习->知识->应用




- 核心：故障随机森林诊断算法

# MLBR方法

## 机器学习框架



# MLBR核心——故障随机森林诊断算法

故障决策树

◆给定一个故障训练数据集D，其中每个实例，称为例子，训练数据集中包含属性A。同时给定类别集合C。对于训练数据集D，故障**决策树**是指具有以下性质的树：

◆每个内部节点都被标记一个属性Ai。

◆每个弧都被标记一个值，这个值对应于相应父结点的属性。

◆每个叶节点都被标记一个故障分类Cj。

◆**故障决策树分裂准则** 定义为在决策树算法中将训练故障数据集D中的元组划分为故障分类的最好的方法与策略，它说明在节点N上测试哪个属性合适，如何选择测试与测试的方法，从节点N上应该生长出哪些分支。

◆**故障故障决策树分裂准则随机选择ID3，C4.5和CART， 例如ID3用信息增益最大化准则来选定分裂属性：**

$$I(p,n) = -\frac{p}{p+n}\log_2\frac{p}{p+n} - \frac{n}{p+n}\log_2\frac{n}{p+n}$$

如果以属性A作为决策树的根，A具有v个值 $\{v_1, v_2, \cdots, v_v\}$，它将A分为v个子集 $\{e_1, e_2, \cdots, e_v\}$，假设中含有p个正例和n个反例，那么，以属性A为根所需的信息期望如下公式所示：

$$E(A) = \sum_{i=1}^{v}\frac{p_i + n_i}{p+n}I(p_i, n_i)$$

因此，以A为根的信息增益如下公式所示：

$$gain(A) = I(p,n) - E(A)$$

◆针对一个网络故障Fi生成故障诊断随机森林的算法如下：

① 准备带标签的网络状态数据集。

② 从网络状态向量中，选取和故障Fi相关联的事件，形成针对故障Fi的特定状态子向量。

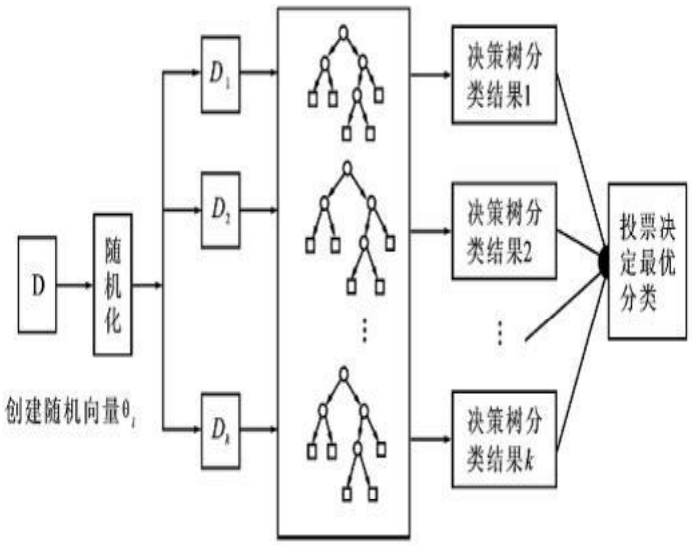
③ 启动N个决策树生成任务（JOB）

④ 每个决策树生成任务随机选取训练数据集，随机选取一个决策树生成算法，得到各自的决策树。

⑤ 将N个决策树的结果进行汇总，形成一个故障决策森林模型。

# MLBR方法

## 决策树与随机森林




- 多层次故障随机森林生成
- 每个故障随机森林并行生成，多个故障随机森林并行生成
- 两个方向的推理，诊断推理和定位推理（根因分析）

## 建模

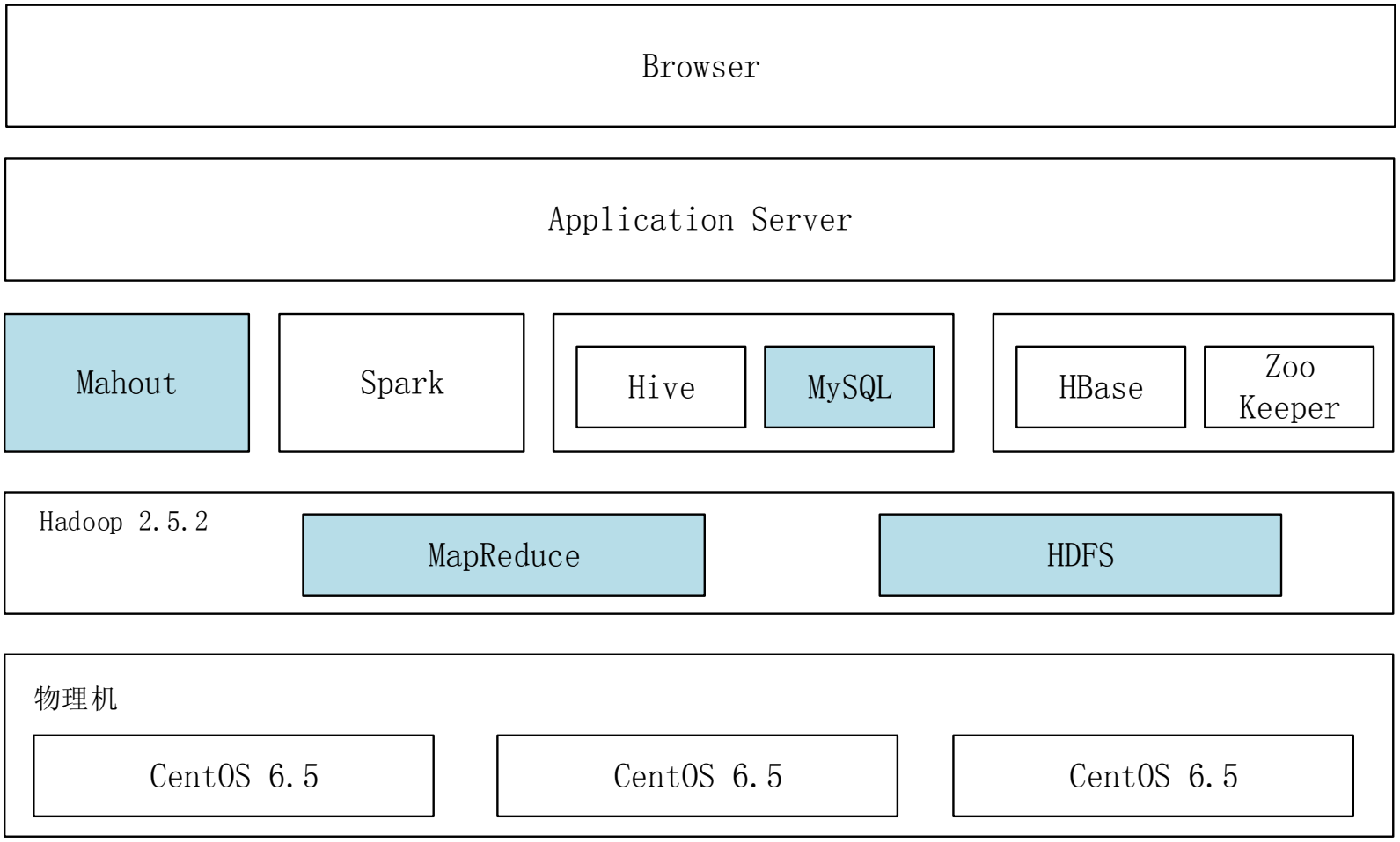
① 事件量化、指标量化
② 为诊断和定位分别选择和定义特征向量，保证独立性，消除共线性
③ 用大数据随机森林算法训练故障随机森林
④ 每个故障随机森林和多个故障森林并行训练建模

## 故障推理

① 在故障特征向量内的事件发生时触发推理过程。
② 用故障诊断随机森林来判断是否发生或即将发生故障。
③ 如果发生故障，触发调用故障定位随机森林来判断故障的位置。

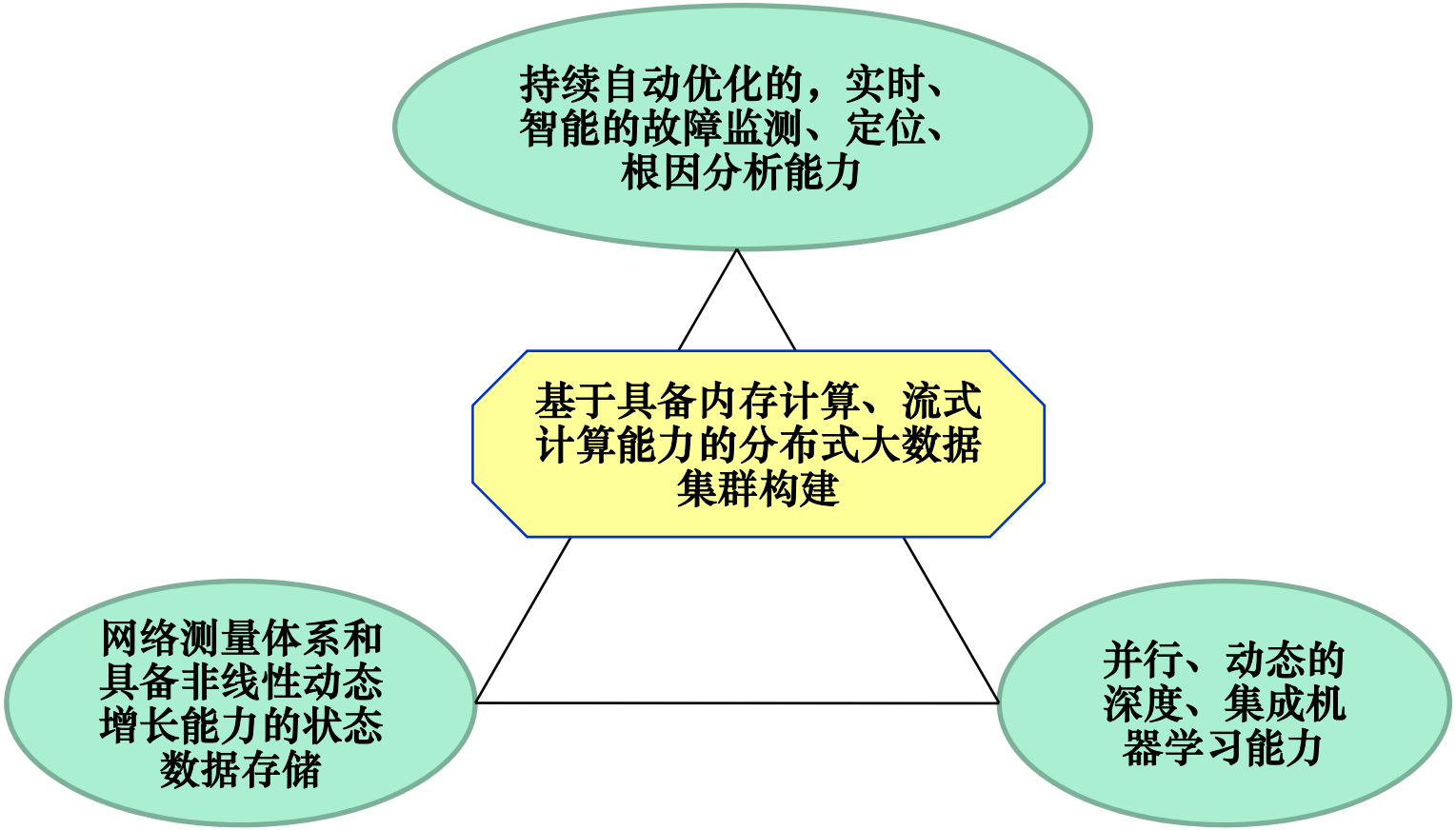
# MLBR方法

## 技术实现框架



# MLBR方法

- 主要特色


持续自动优化的，实时、
智能的故障监测、定位、
根因分析能力
基于具备内存计算、流式
计算能力的分布式大数据
集群构建
网络测量体系和
具备非线性动态
增长能力的状态
数据存储
并行、动态的
深度、集成机
器学习能力

# MLBR方法

- 案例1：宽带用户健康档案系统

- 问题描述：
  - 某省电信积累了大量的OSS数据，但未发挥作用
  - 日常采集的运行指标多达107种
  - 面对用户投诉，急需解决两个问题：
    （1）哪些指标能够有效预警用户投诉？
    （2）如何自动找出故障根因，定位故障？

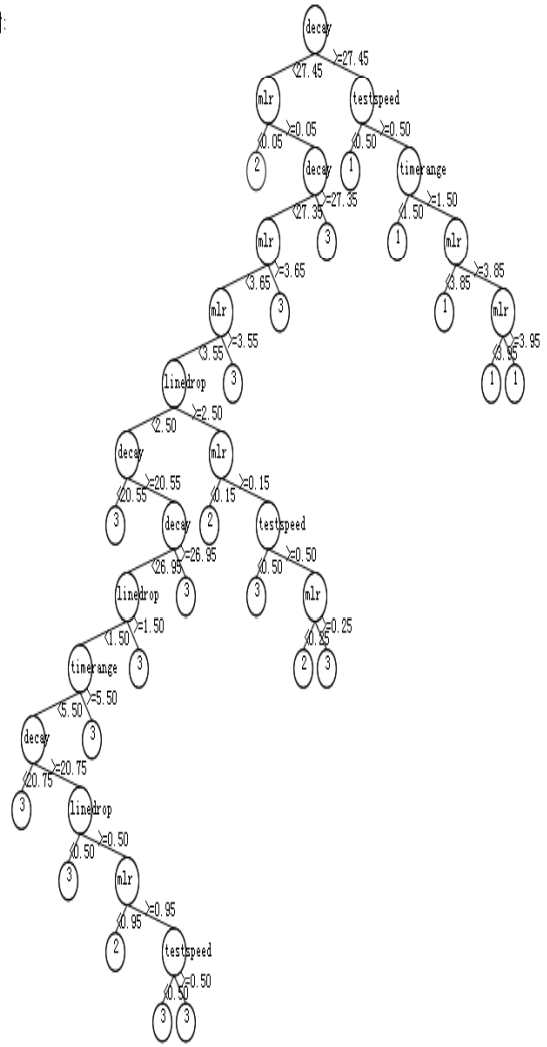
# MLBR方法

## 案例1：宽带用户健康档案系统

- 通过机器学习，从107个指标中筛选出最关键的2个指标，用于预警
- 其余指标不作为预警来源，但被纳入故障定位规则

## 机器学习过程

- 准备四类训练数据：(1)未投诉用户的各类指标采样；(2)投诉用户前2天的各类指标采样；(3)投诉用户人工故障定位结果(精确到网元)；(4)网络资源树。
- 将前三类数据分别打上0, 1, 2标签，用随机森林算法，训练故障随机森林。
- 自动选举最终的2棵决策树，分别为故障判断决策树、故障定位决策树。
- 解析两棵决策树，获得故障预警规则、故障定位规则，并获得相应的关键指标知识。



# MLBR方法

## 案例1：宽带用户健康档案系统

- 基于2个关键指标的故障预警规则

# MLBR方法

- 案例1：宽带用户健康档案系统
  - 基于多个指标的故障定位规则
  - 实现单用户故障的快速定位

# 目录

# 提纲

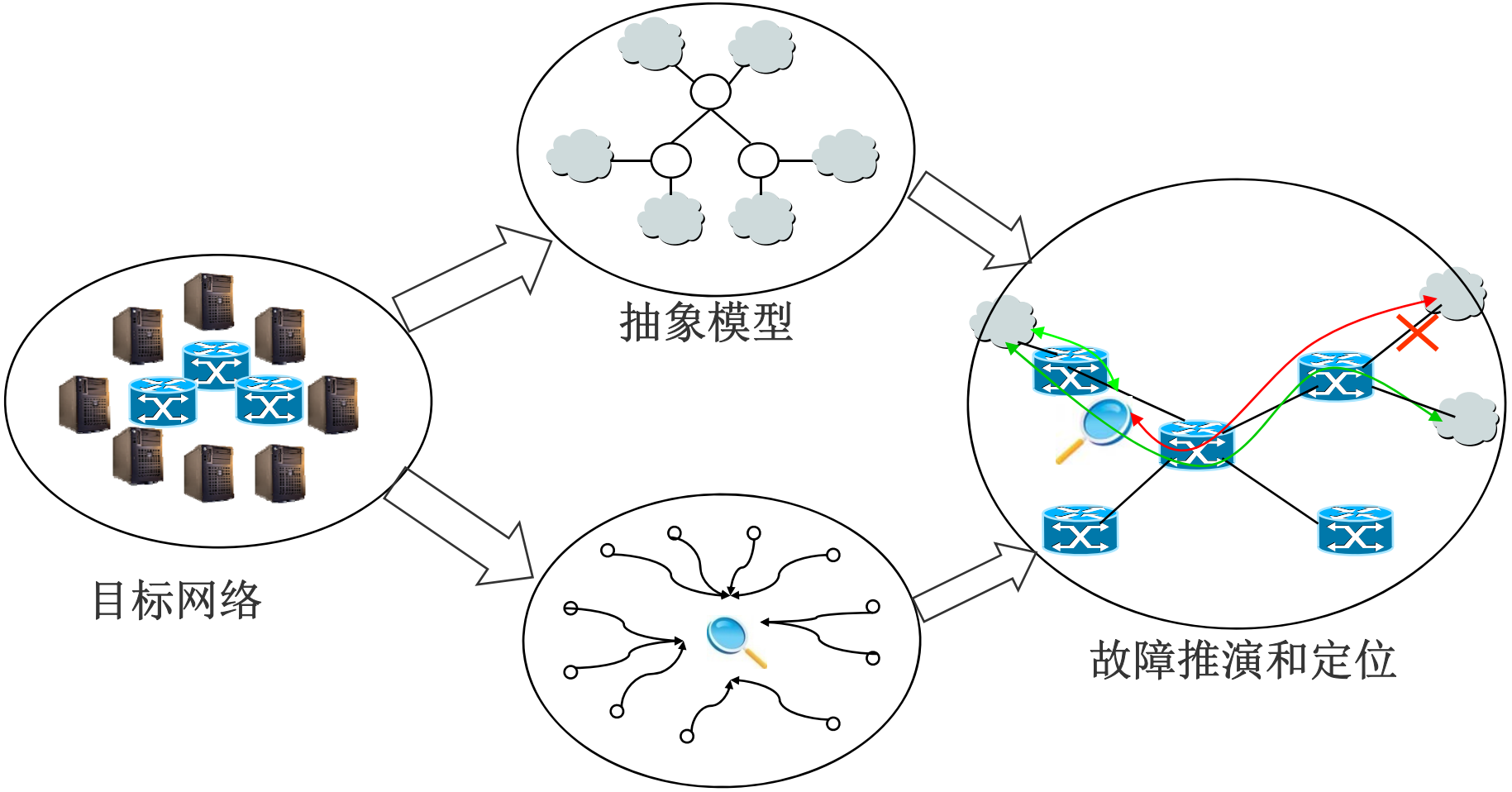
## 探索2：一种故障诊断方法RMBR
## (Routing-Model Based Reasoning)

# RMBR方法——主要思想

**RMBR的两个出发点：**

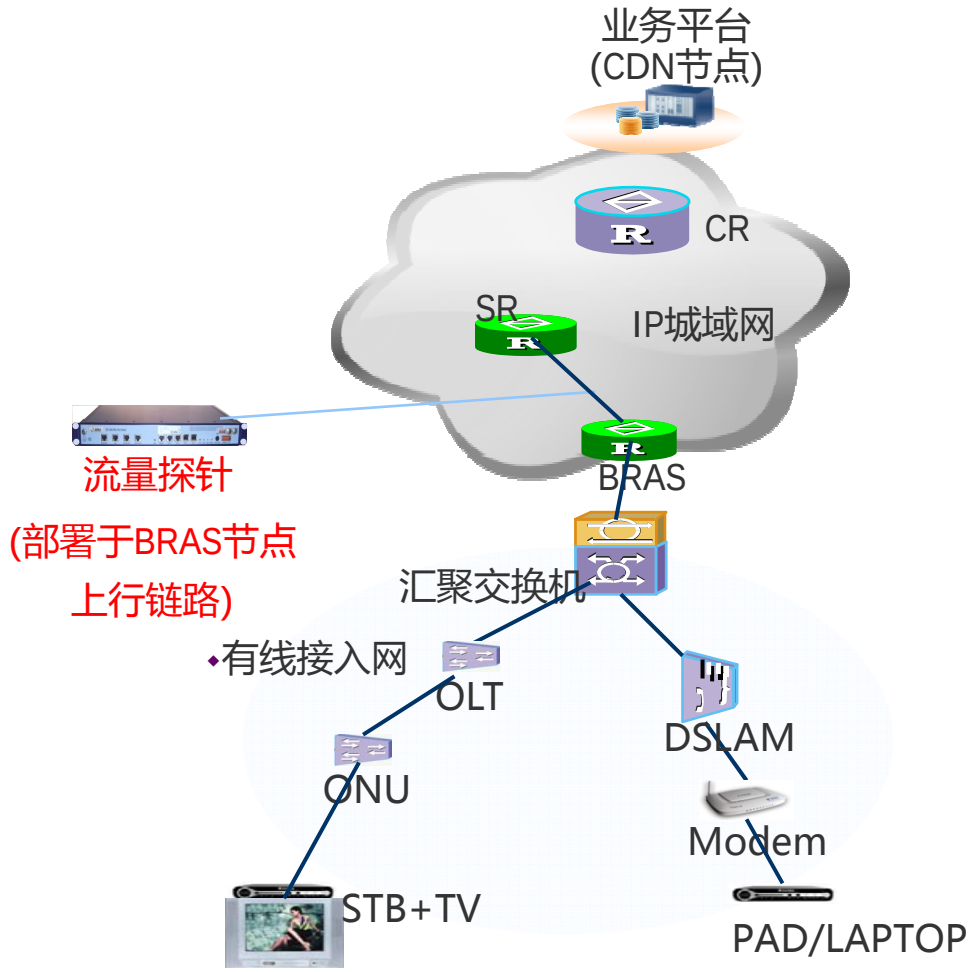
- 网络和应用的状态是可建模、可演算的
- 网络故障对用户的影响，大多会表现在流量上

# RMBR方法——主要思想



# RMBR方法

- Step1-在网络的关键路径中部署流量测量点



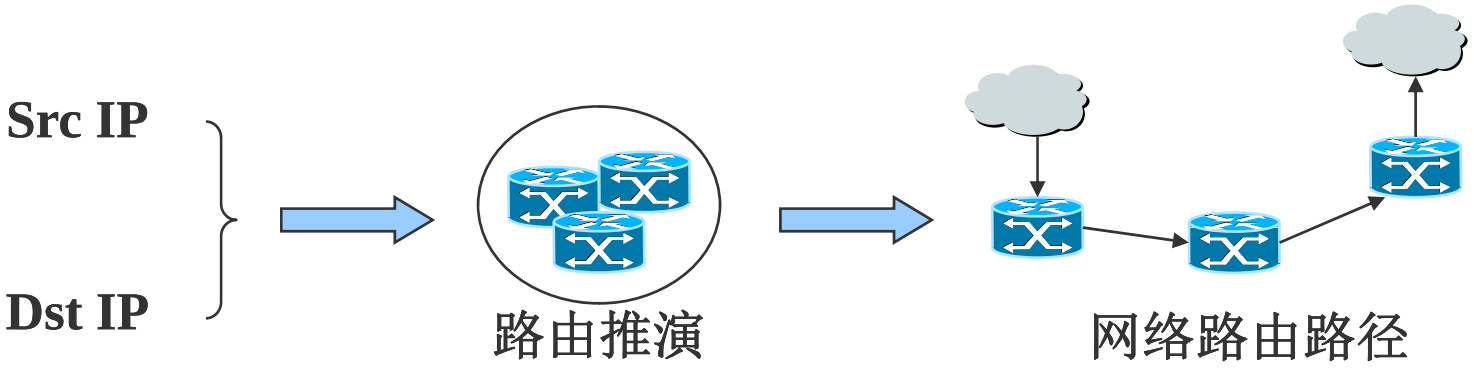
# RMBR方法

- Step2-获得端到端（IP对）之间的路径质量
  - 路径质量由若干约束参数组成，如：丢包率、时延、可用带宽等


关键点：从流量流量中挖掘端到端路径约束参数的方法与评价模型

# RMBR方法

- Step3-建立路由模型，实现任意IP对的路径推演



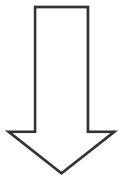

关键点：路由推演模型的建立和实时路径推演算法

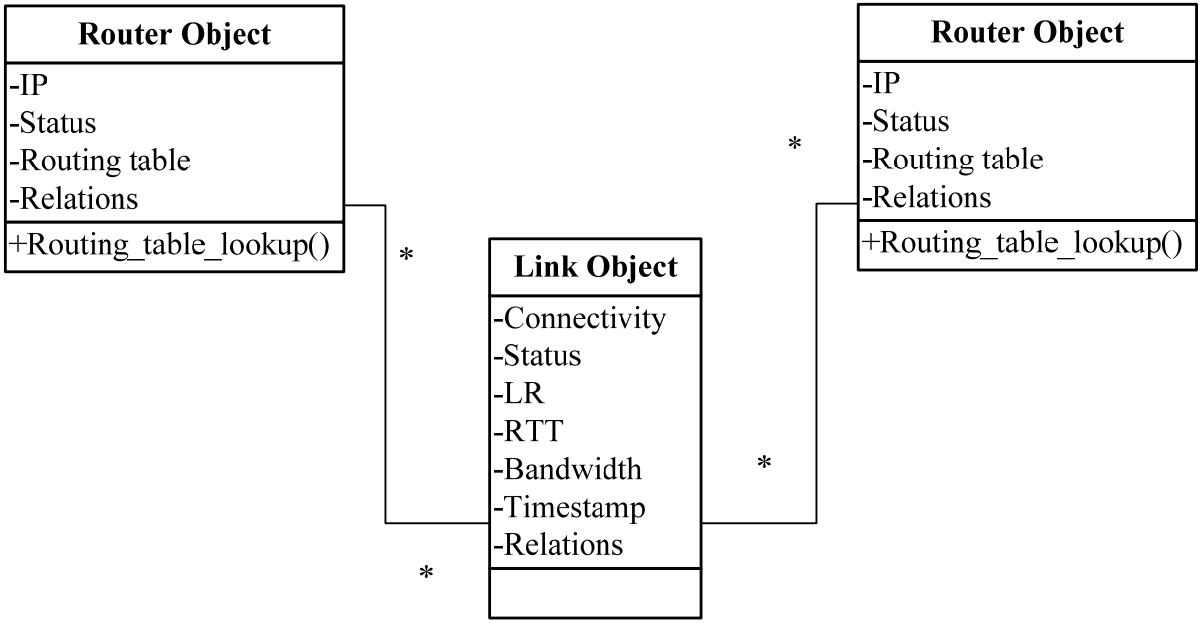
（Routing Path Simulation, RPS）

# RMBR方法

- 网络路由模型的建立——从路由器到OO对象

路由表采集
动态路由跟踪





# RMBR方法

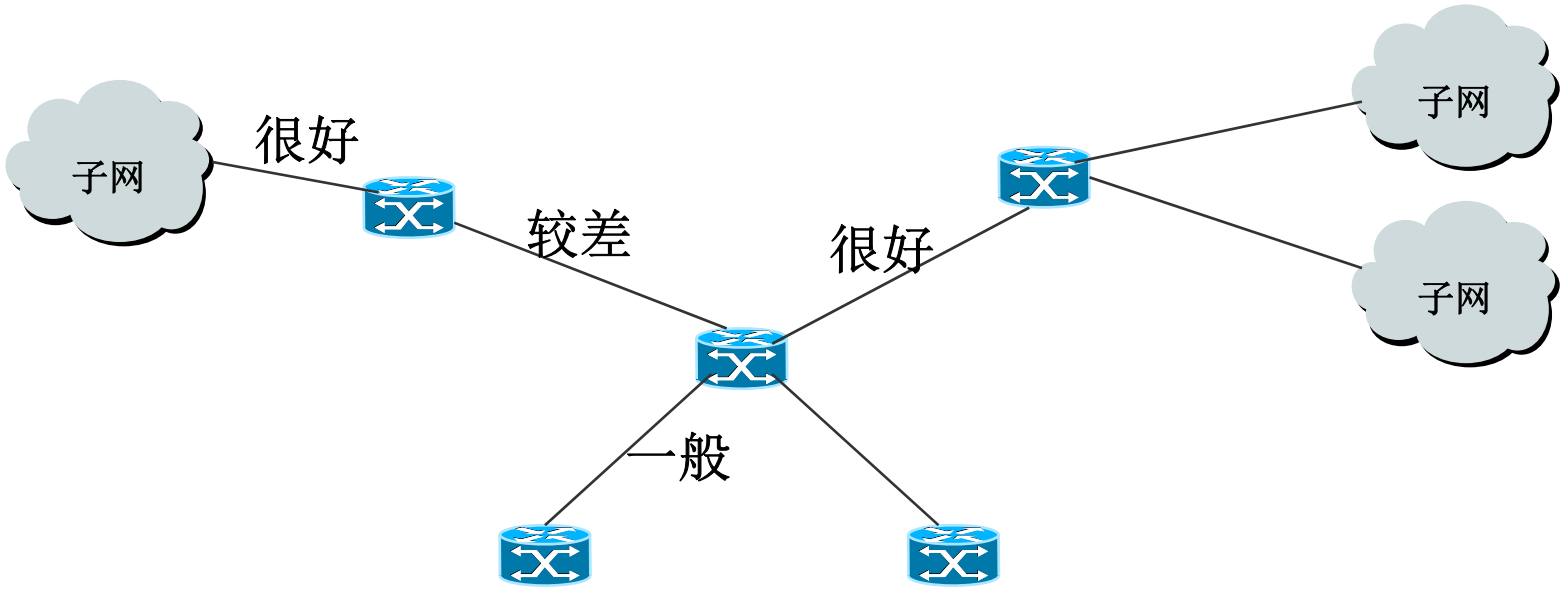
## RPS算法功能

RPS 功能实现对任意 IP 对的路由路径推演，即：给定源 IP 地址（$IP_{src}$）和目标 IP 地址（$IP_{dst}$），通过逐跳路由表查找的方式，确定 IP 分组在网络中的转发路径。

将 $IP_{src}$ 标识的网络节点记为 $s$，$IP_{dst}$ 标识的网络节点记为 $d$，则 $s$ 和 $d$ 之间的网络路径为 $PATH_s^d = \{s, e_1, v_1, \ldots, e_k, v_k, \ldots, e_n, d\}$，其中 $v_1 \cdots v_{n-1}$ 为路由器对象，$v_k$ 称为第 $k$ 跳路由器；$e_1 \ldots e_n$ 为链路对象，$e_k$ 称为第 $k$ 跳链路。这些对象序列代表了 IP 分组在目标网络中的转发和传输过程。

# RMBR方法

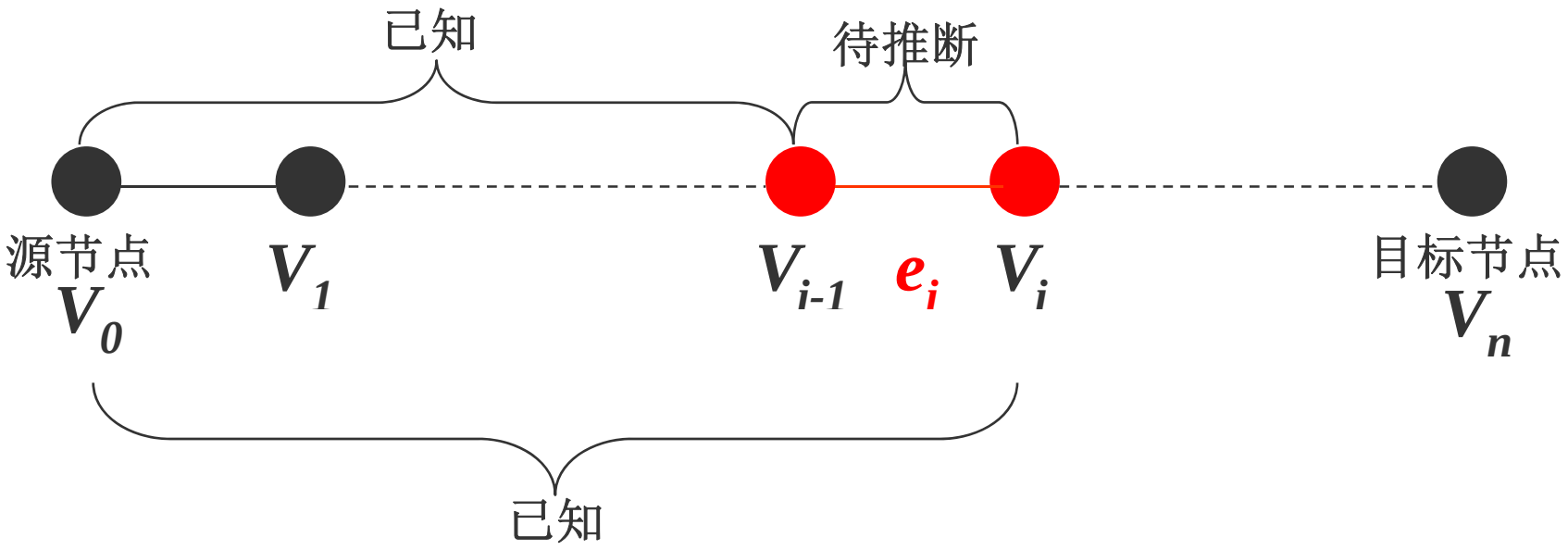
- Step4-基于路由模型的链路状态评价




关键点：**RMBR推理算法，断层分析(Network Tomography)**

# RMBR方法

- 基于NT的链路状态分析算法LMT
  - 理论依据——NT原理
  - 已知路径path中从源点到第i跳节点及其前一跳节点的路径质量的情况下，可以反向推导第i跳链路的属性：



# RMBR方法

- 基于NT的链路状态分析算法LMT
  - 理论依据——NT原理
  - 将网络性能近似为一般线性模型

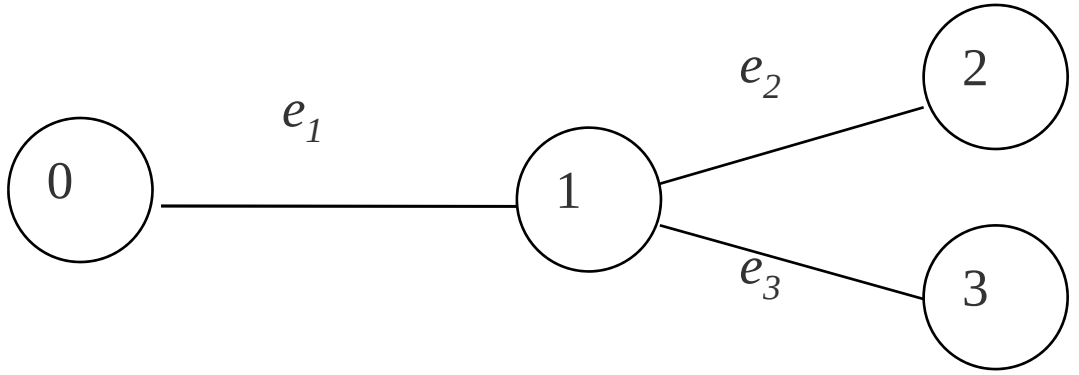
$$y = Ax + \varepsilon$$

$y$：测量获得的向量值（端到端性能指标）
$A$：路径矩阵
$x$：需要推测的向量值（单跳链路性能指标）
$\varepsilon$：测量噪声

# RMBR方法

## 基于NT的链路性能分析算法LMT

已知0号节点到2号、3号节点的路径成功率分别为 $P_2$, $P_3$。试图推断三跳链路的成功率。




两条测量路径分别为(0,1,2)和(0,1,3)，路径矩阵表示为

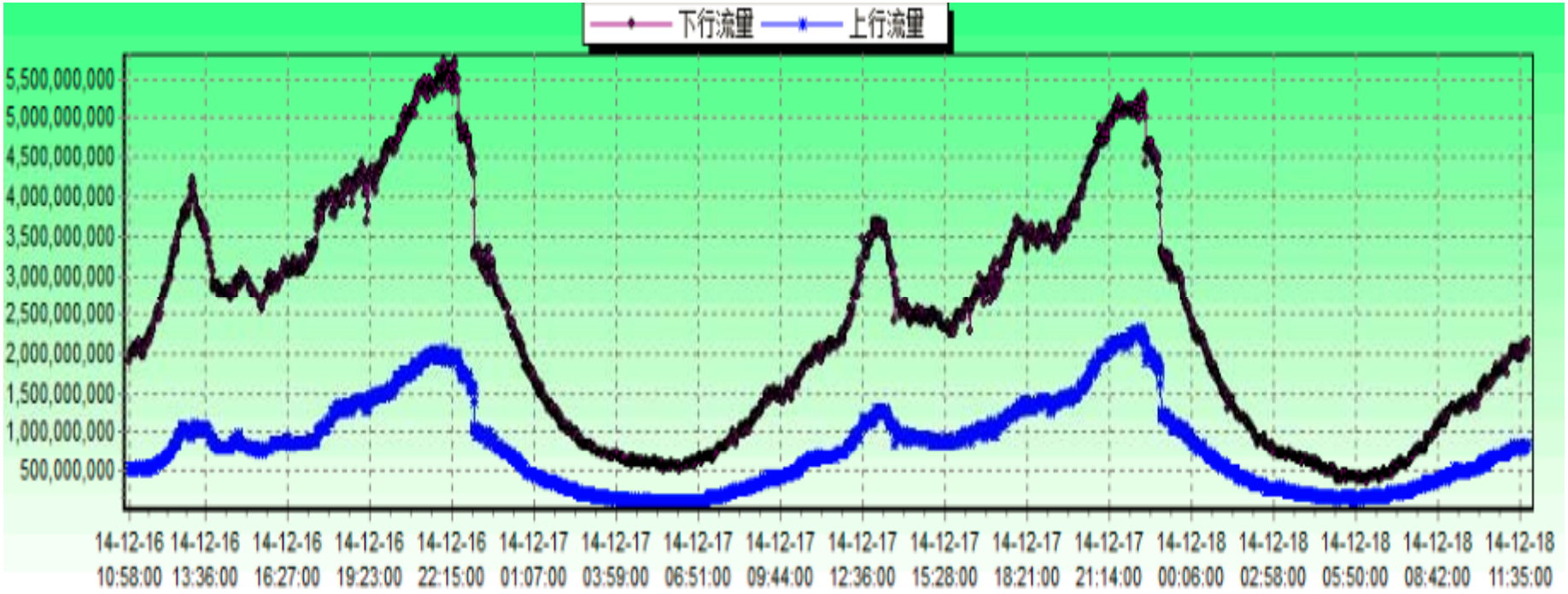
$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

试图求解$\theta_1$、$\theta_2$、$\theta_3$

$$\begin{bmatrix} \log p_2 \\ \log p_3 \end{bmatrix} \approx \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} \theta_1 \\ \theta_2 \\ \theta_3 \end{bmatrix}$$

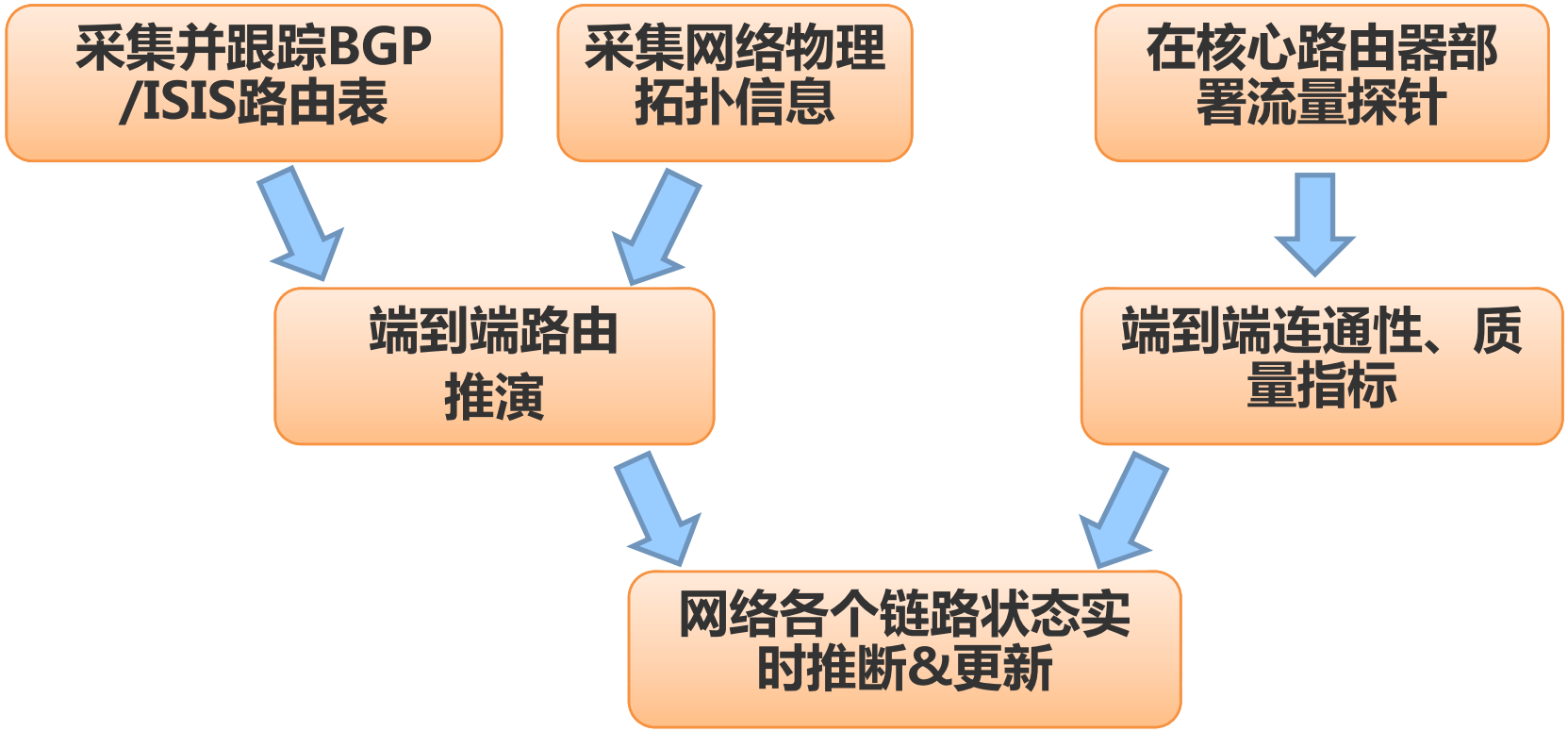
# RMBR方法

- 案例2：有规律的主干链路中断事件
  - 宏观现象：流量有有规律地陡降，显然不正常



# RMBR方法

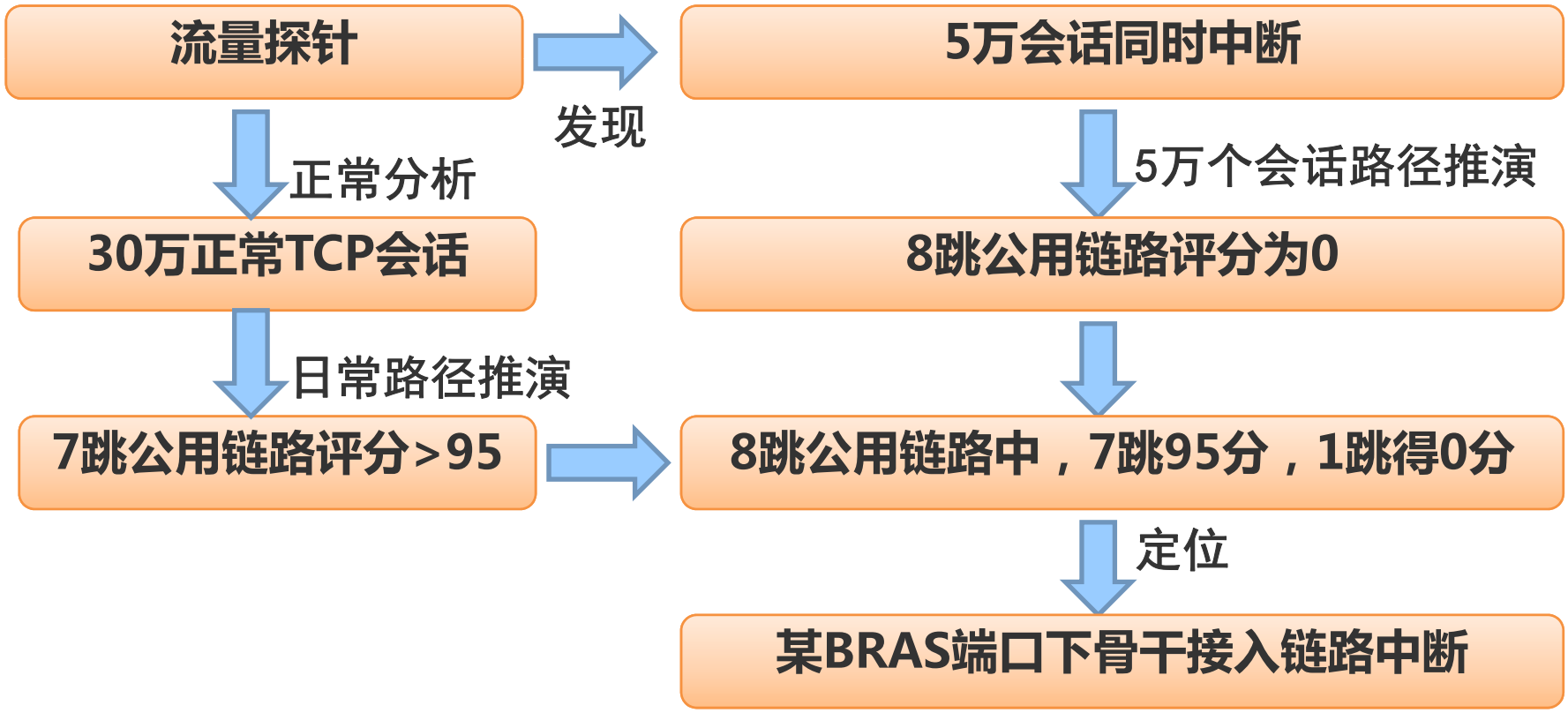
- 案例2：有规律的主干链路中断事件
  - 故障推理和定位过程



# RMBR方法

## 案例2：有规律的主干链路中断事件

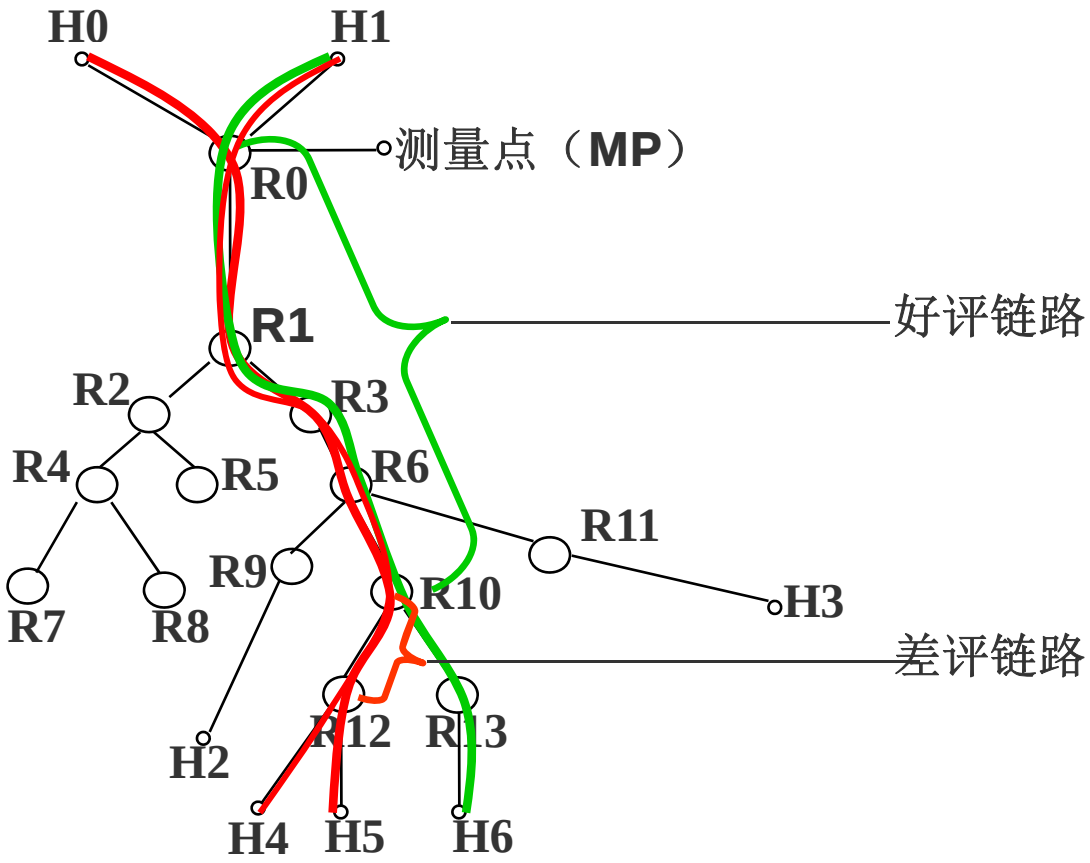
- 故障推理和定位过程




真实原因：某大学城夜间拉闸

# RMBR方法

- 案例2：有规律的主干链路中断事件
  - 故障推理和定位过程



# RMBR方法

## 案例3：9.3阅兵后的上网故障

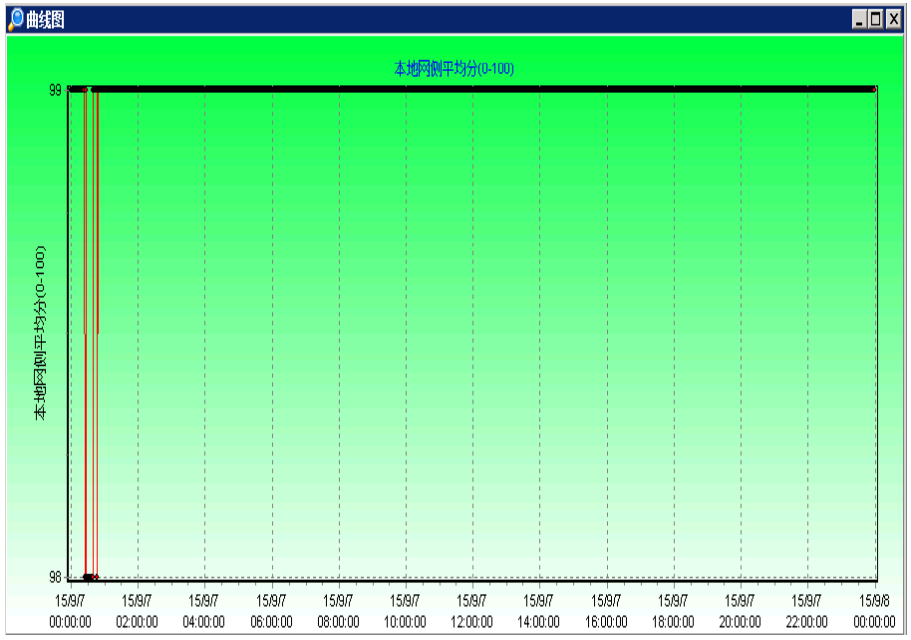
- 宏观现象：大量用户上网慢，网页打不开
- 网管监测：设备、端口、服务器、出口、内容源均无告警
- 日常拨测：所有网内设备和路径均正常运转，性能良好

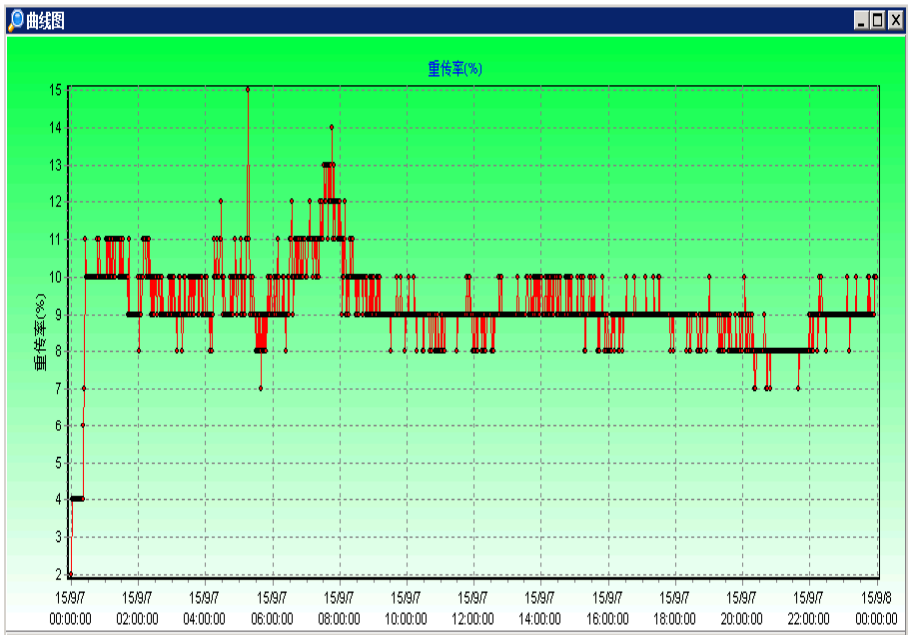
# RMBR方法

## 案例3：9.3阅兵后的上网故障

### 故障推理和定位过程

(1)端到端连通性和质量均无异常，验证了网络自身的正常



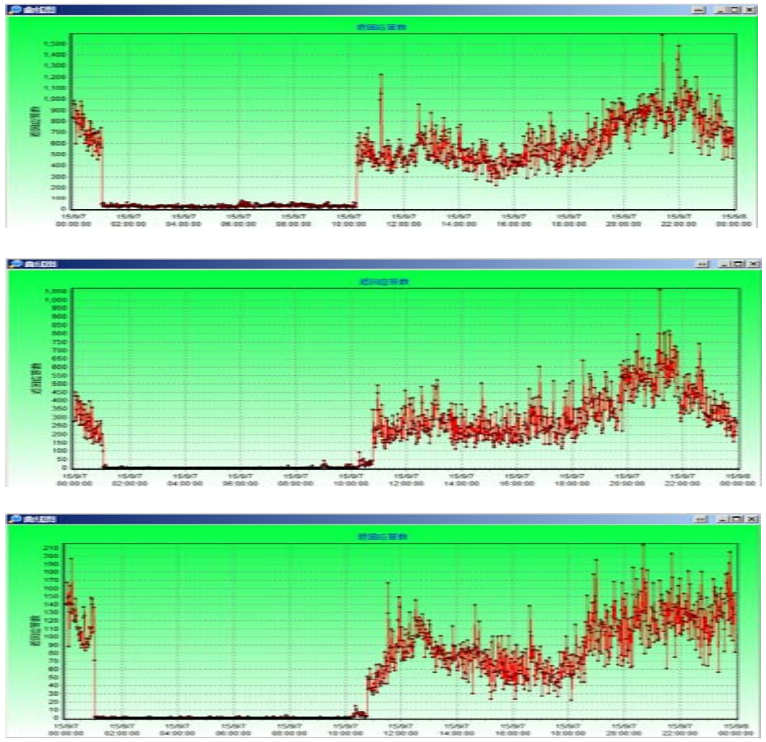



# RMBR方法

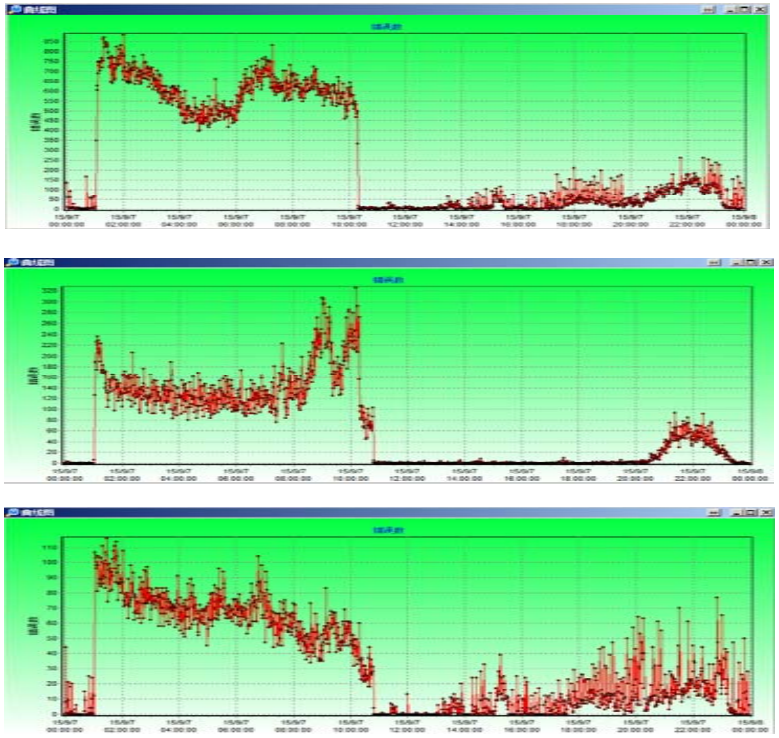
## 案例3：9.3阅兵后的上网故障

### 故障推理和定位过程

(2)流量探针事件发现：3台主用DNS服务器异常



DNS成功解析次数/秒



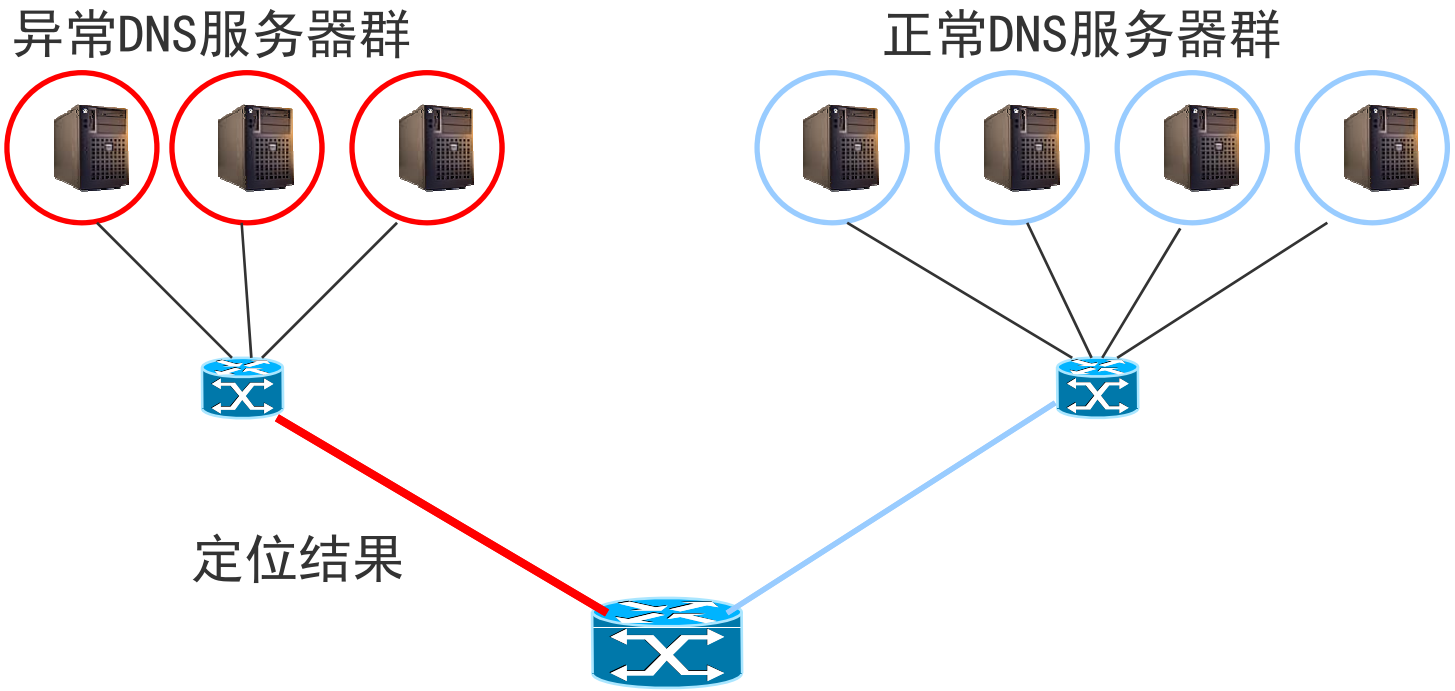
DNS失败次数/秒

# RMBR方法

## 案例3：9.3阅兵后的上网故障

### 故障推理和定位过程

(3) 故障推理

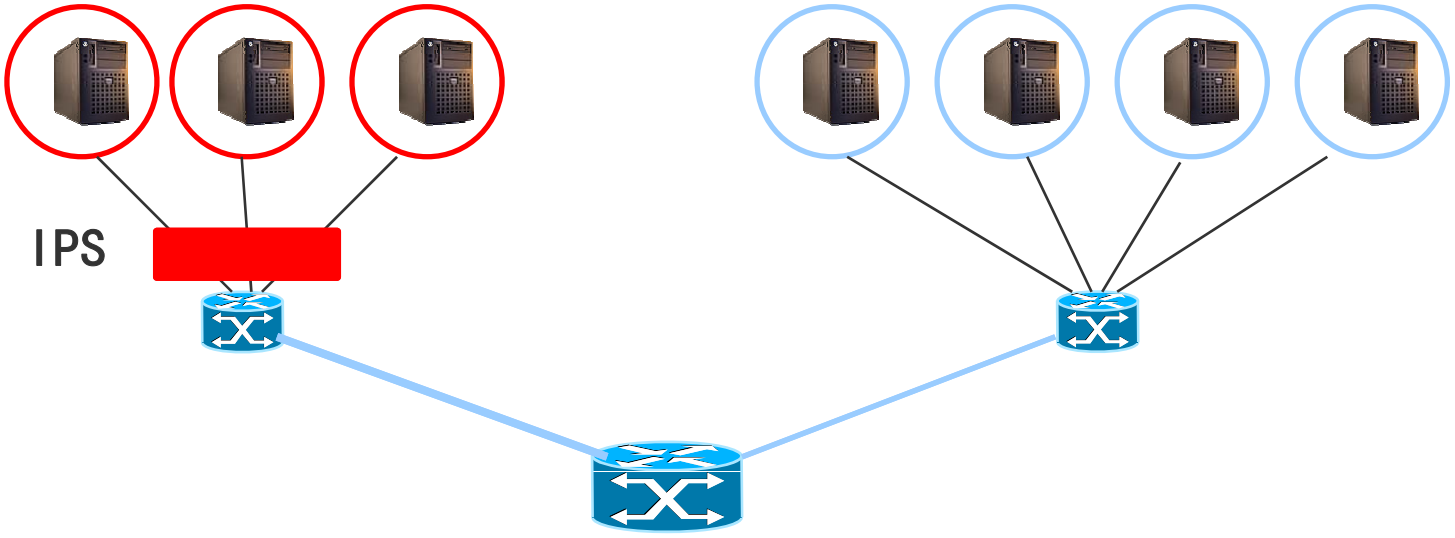


# RMBR方法

## 案例3：9.3阅兵后的上网故障

### 故障推理和定位过程

(4) 人工验证




阅兵期间关闭的某些应用和服务器的突然放开，导致了大量突发DNS请求，引发IPS对某些IP的智能防御。

# 请批评指正