



2016 杭州·云栖大会
THE COMPUTING CONFERENCE

云栖社区
yq.aliyun.com


复杂网络架构下的网络故障智能处理

——DC Brain之故障篇



主办单位： 杭州

 Alibaba Group
阿里巴巴集团

战略合作伙伴：

署名：何源（荆杭）
职称：阿里巴巴产品经理



扫码观看大会视频

网络故障的特殊性

体量大

几万台网络设备
几百万端口

型号多& 架构多

日志格式不统一
告警规则不统一

结构复杂

重复告警多

自身依赖

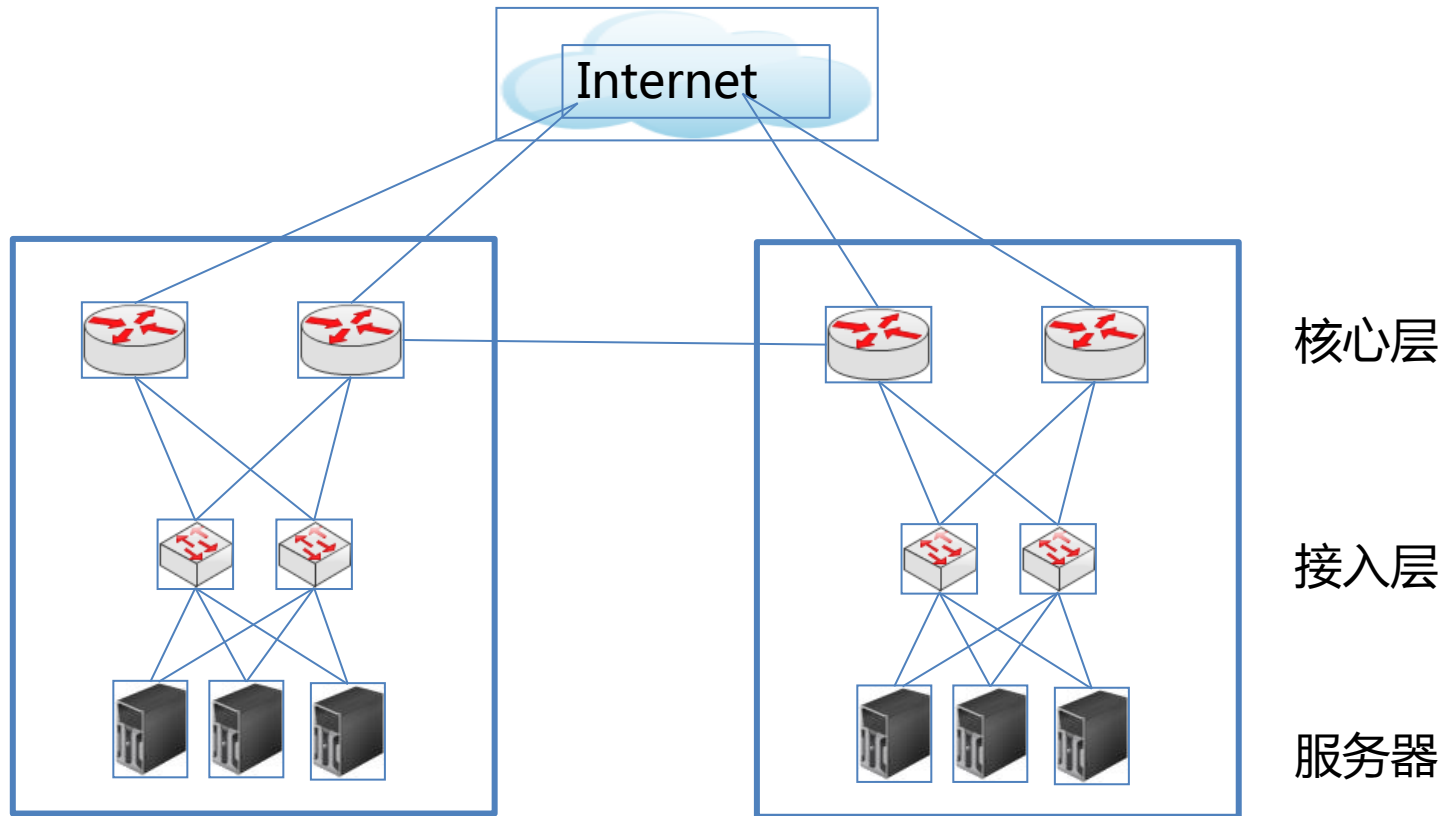
监控系统本身运行
在网络上

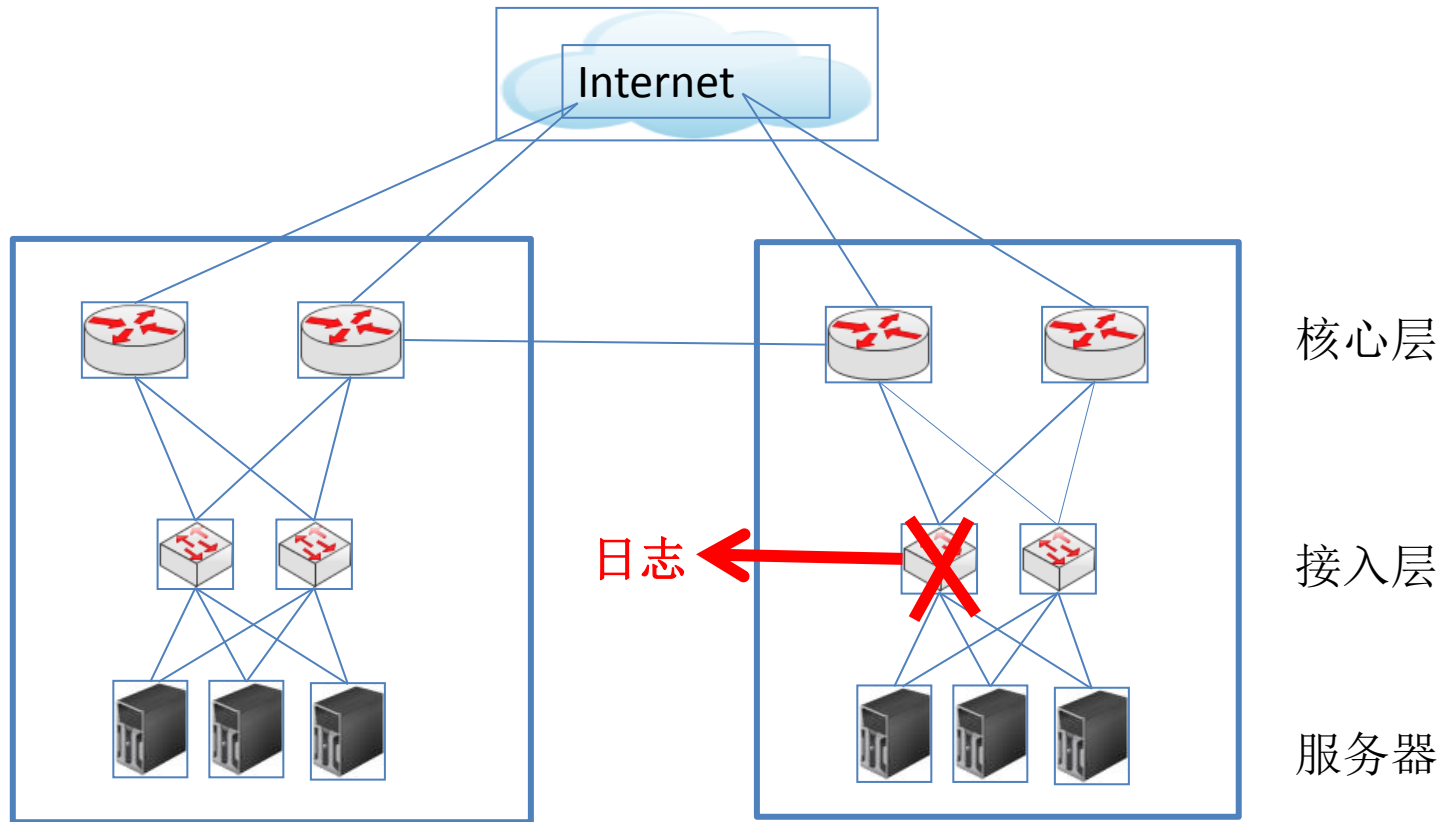


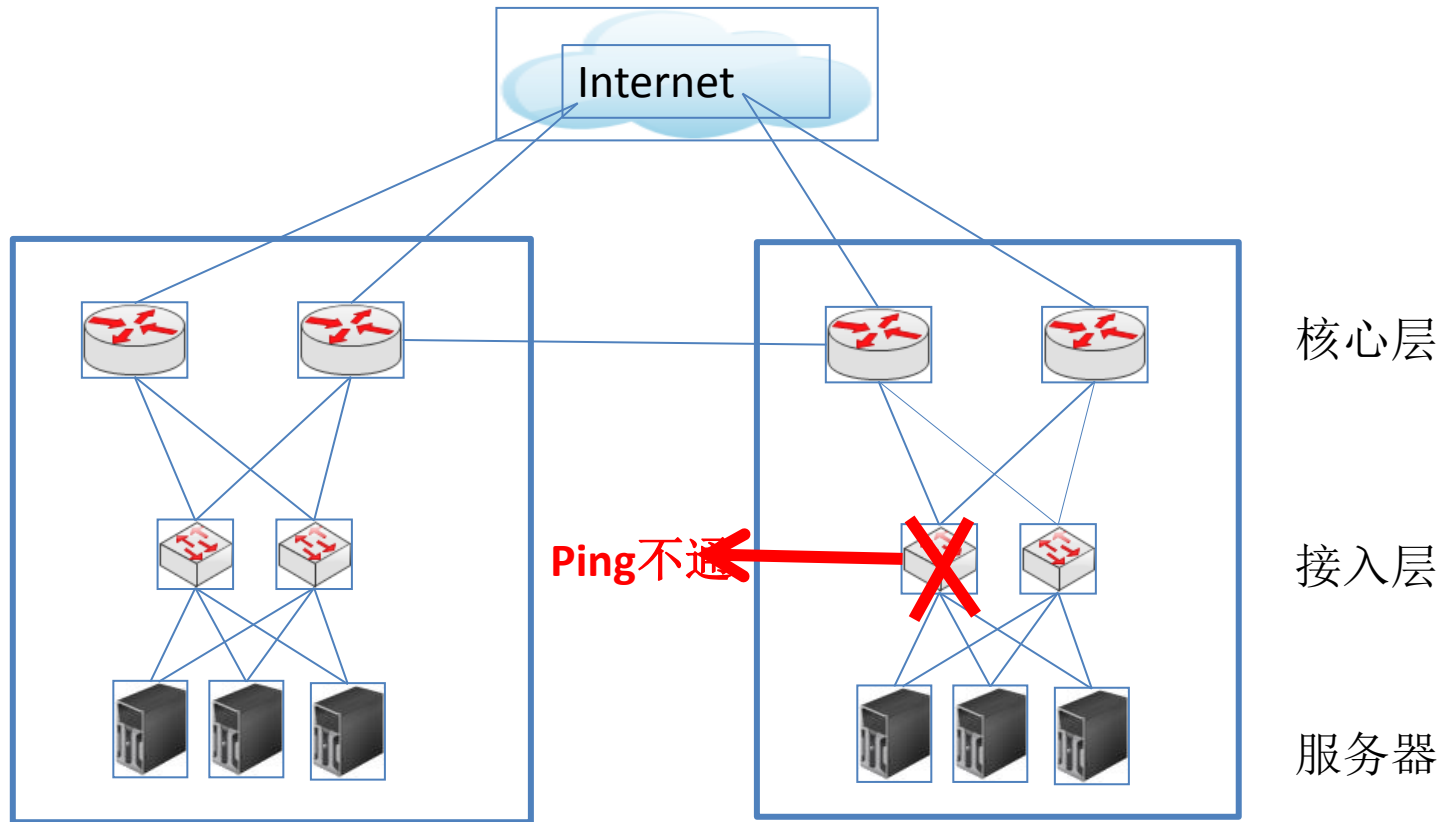
大家普遍遇到的困难

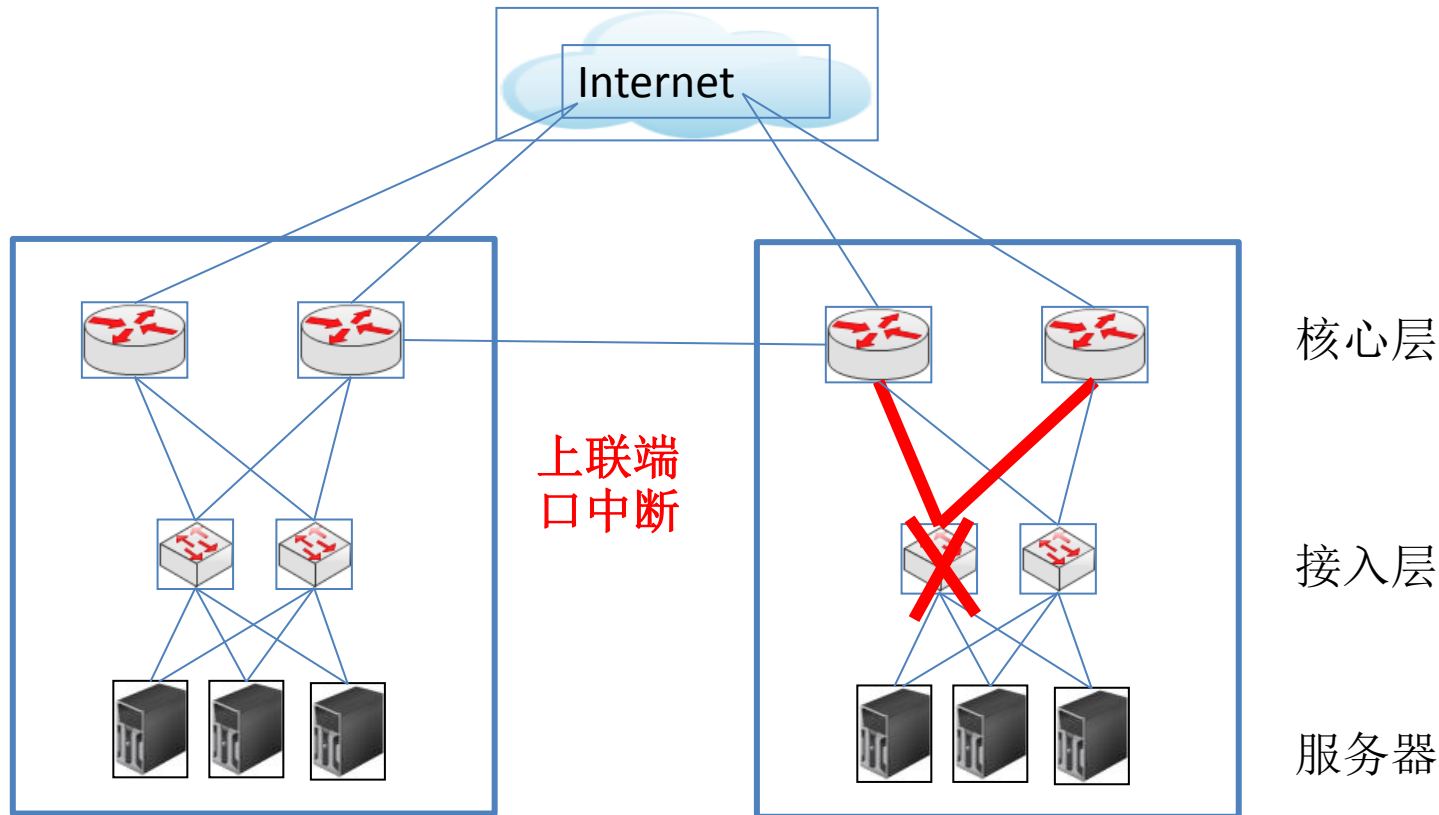
数据量非常大
海量告警，告警淹没
依赖关系复杂
逻辑关系复杂，代码写死

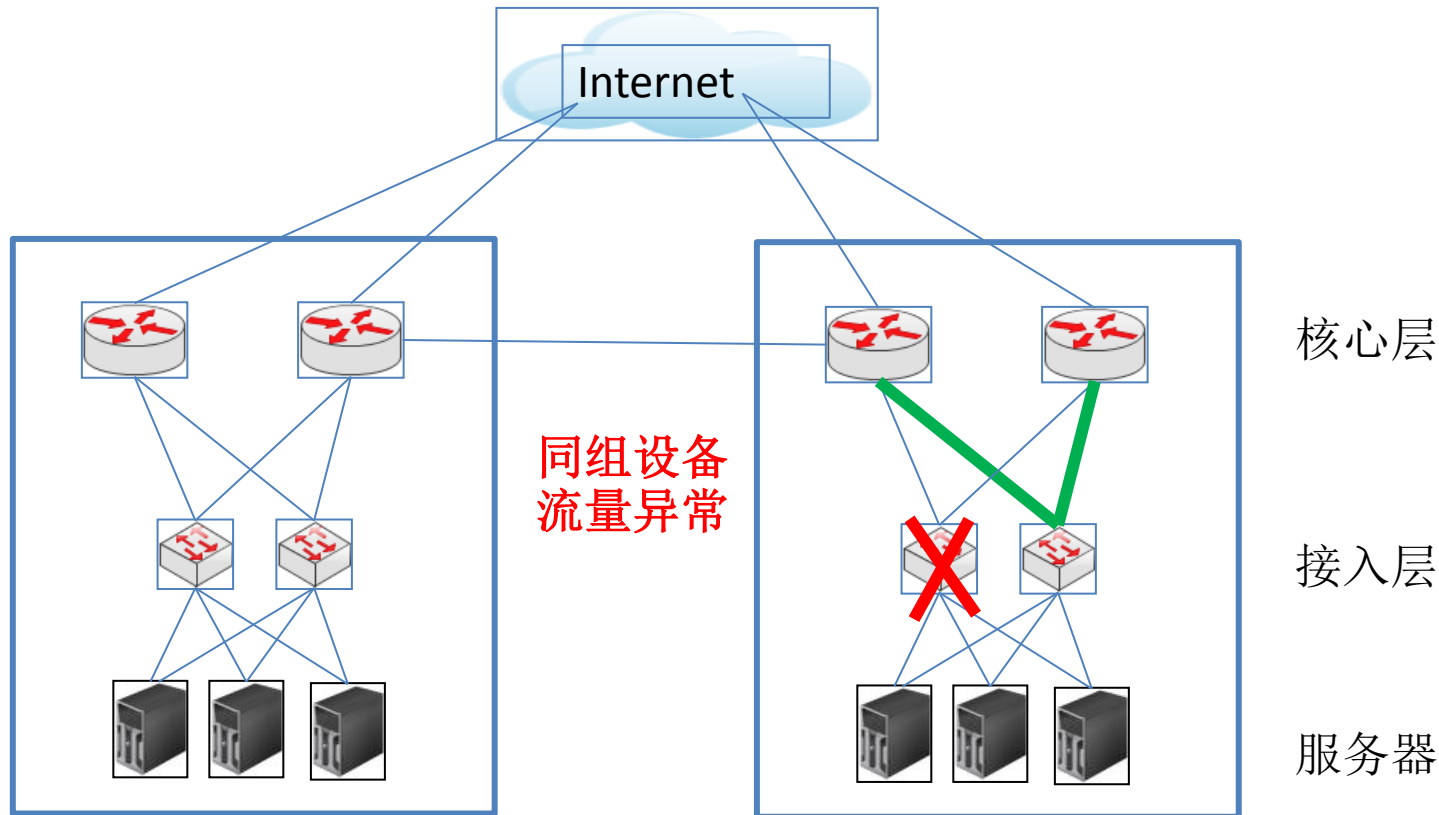


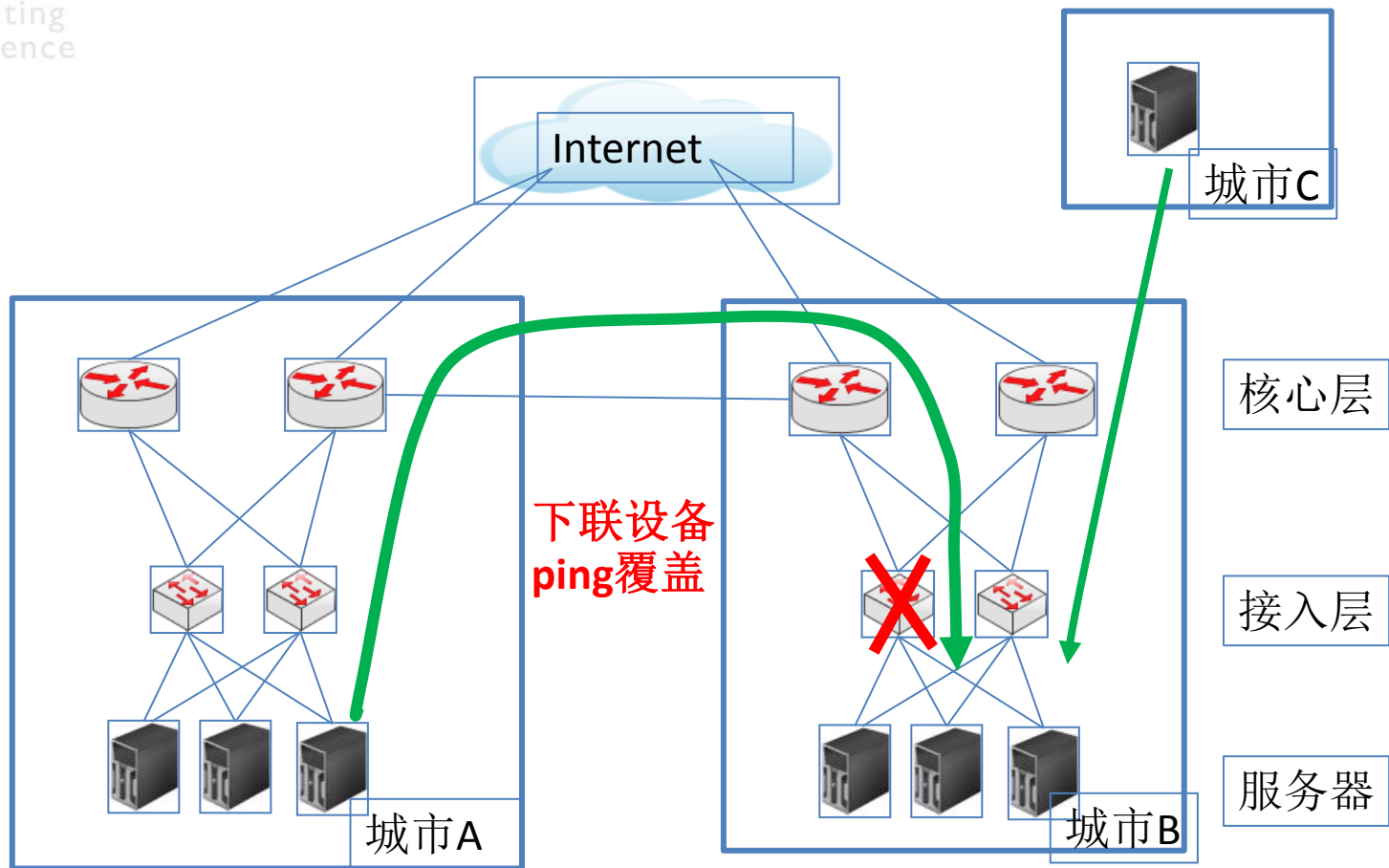








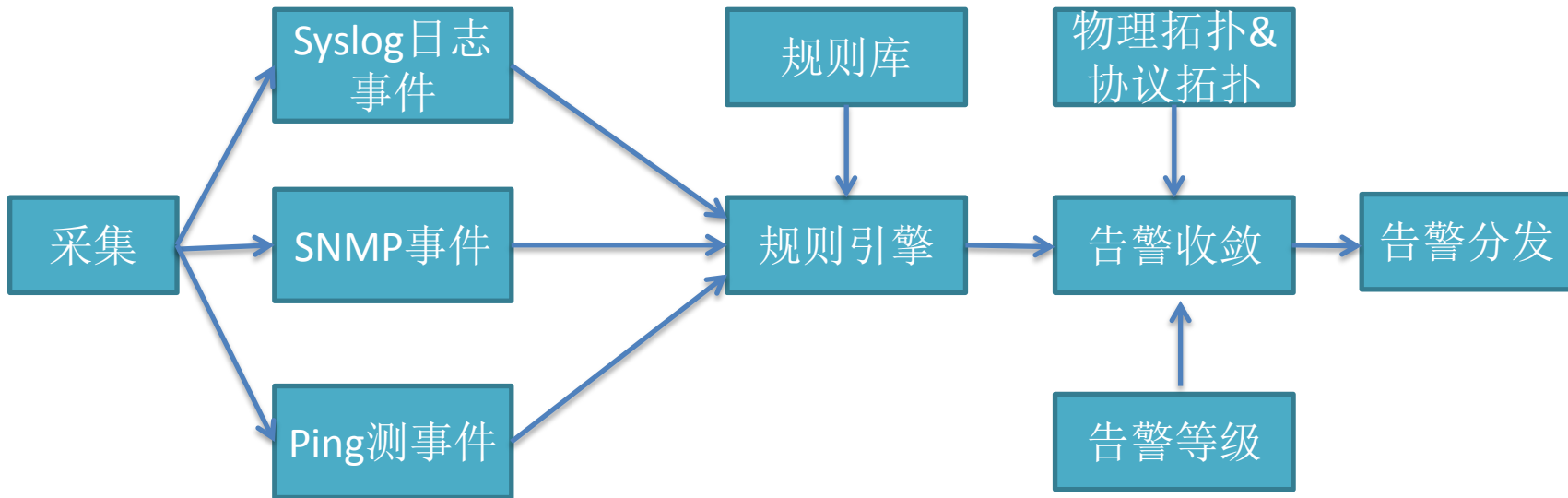




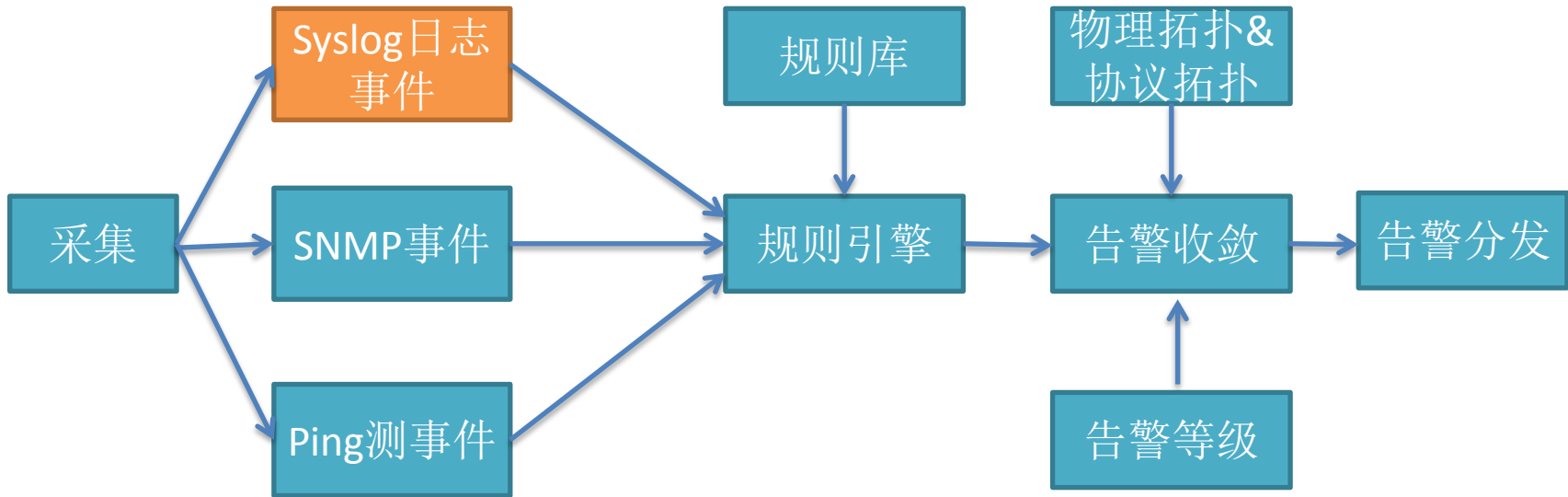
检测手段多元化，交叉覆盖
规则可扩展，可自定义
基于pagerank算法的告警收敛
告警监控系统冗余部署



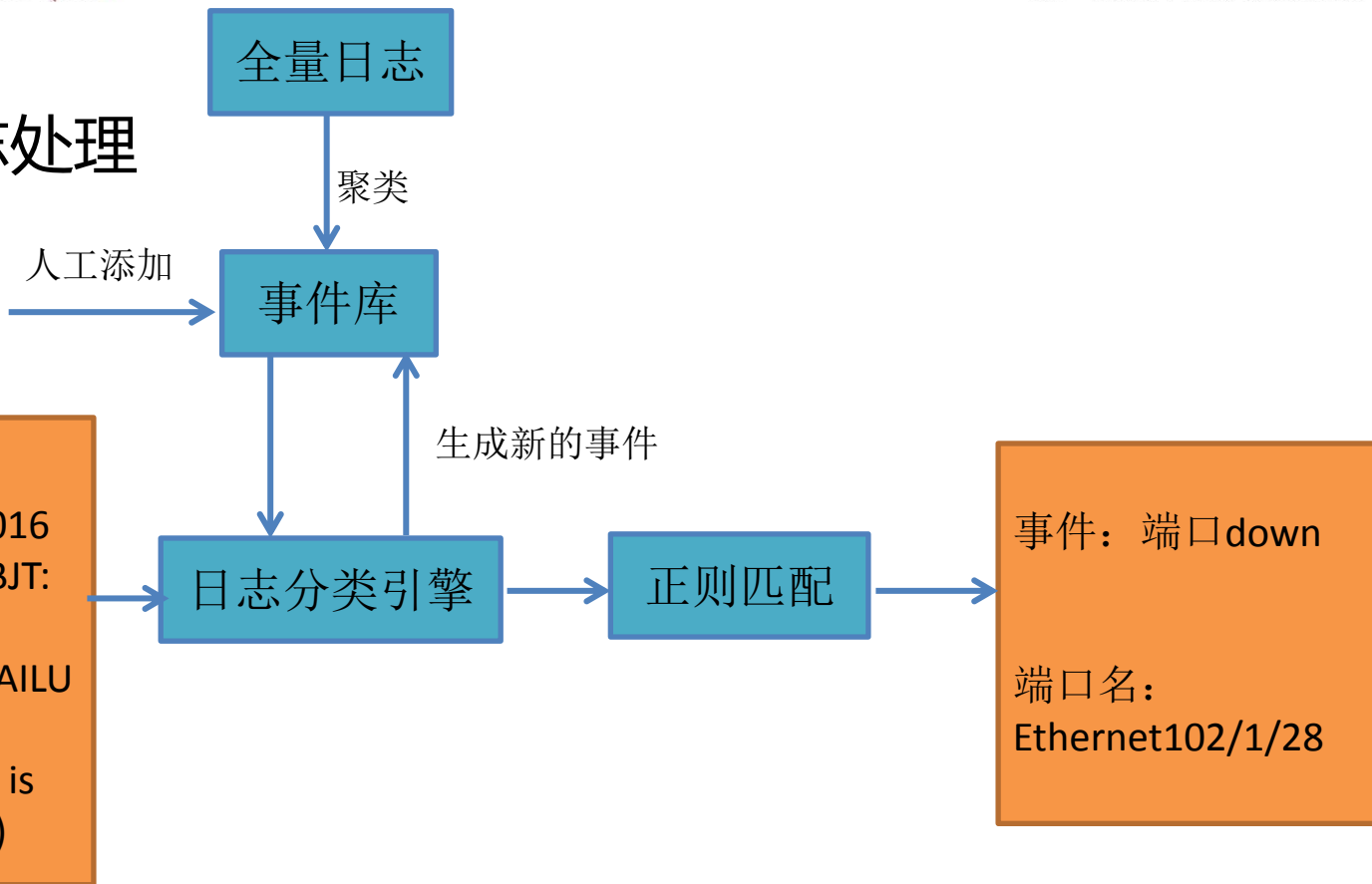
总体思路



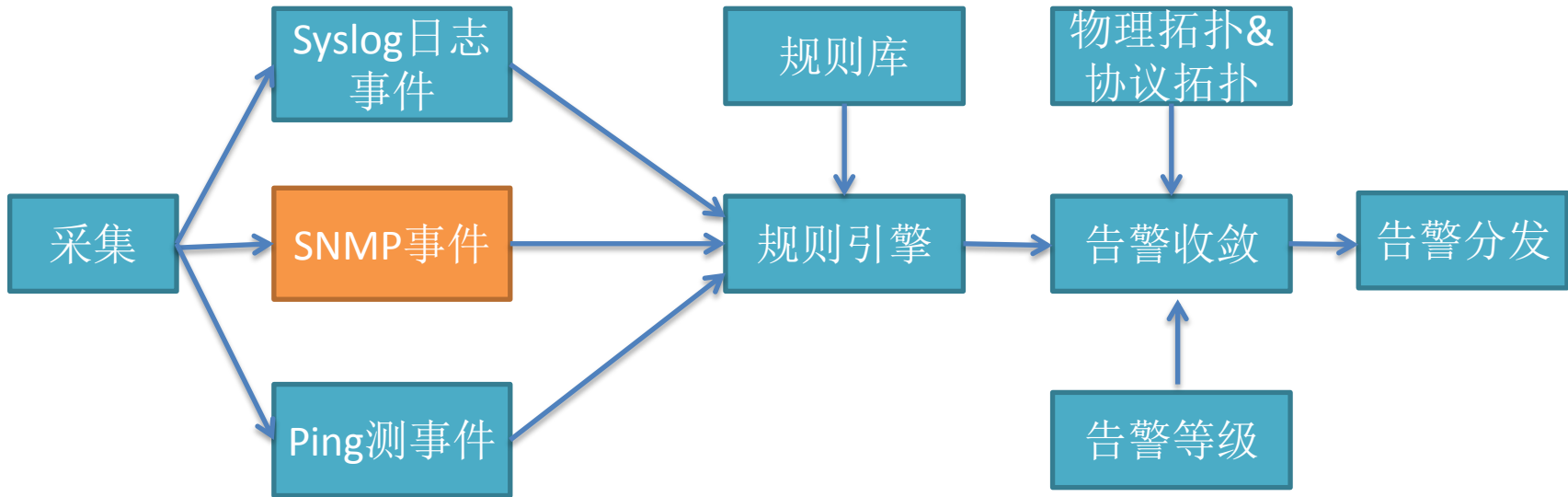
总体思路



syslog日志处理



总体思路



SNMP事件处理

端口流量

端口状态

端口丢、
错包

BGP状态



丢包超过阈值

流量水位90%

流量突跌

端口突变为
down

BGP协议down

同电路组流量不均

绝对值

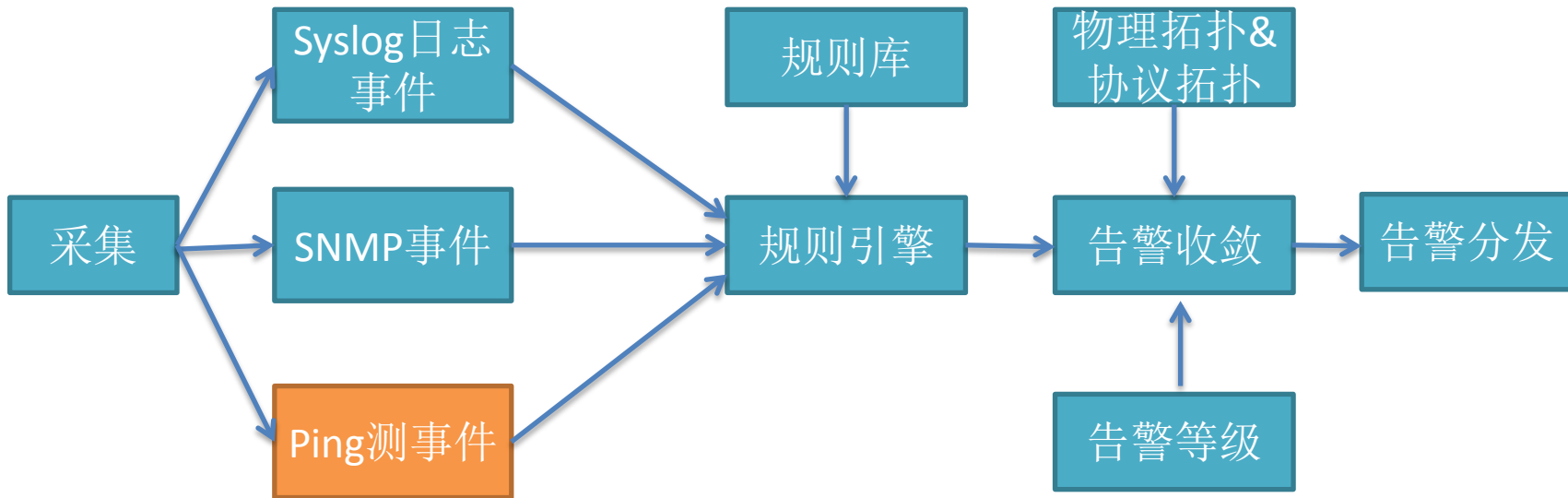
相对值

同比值

类比值



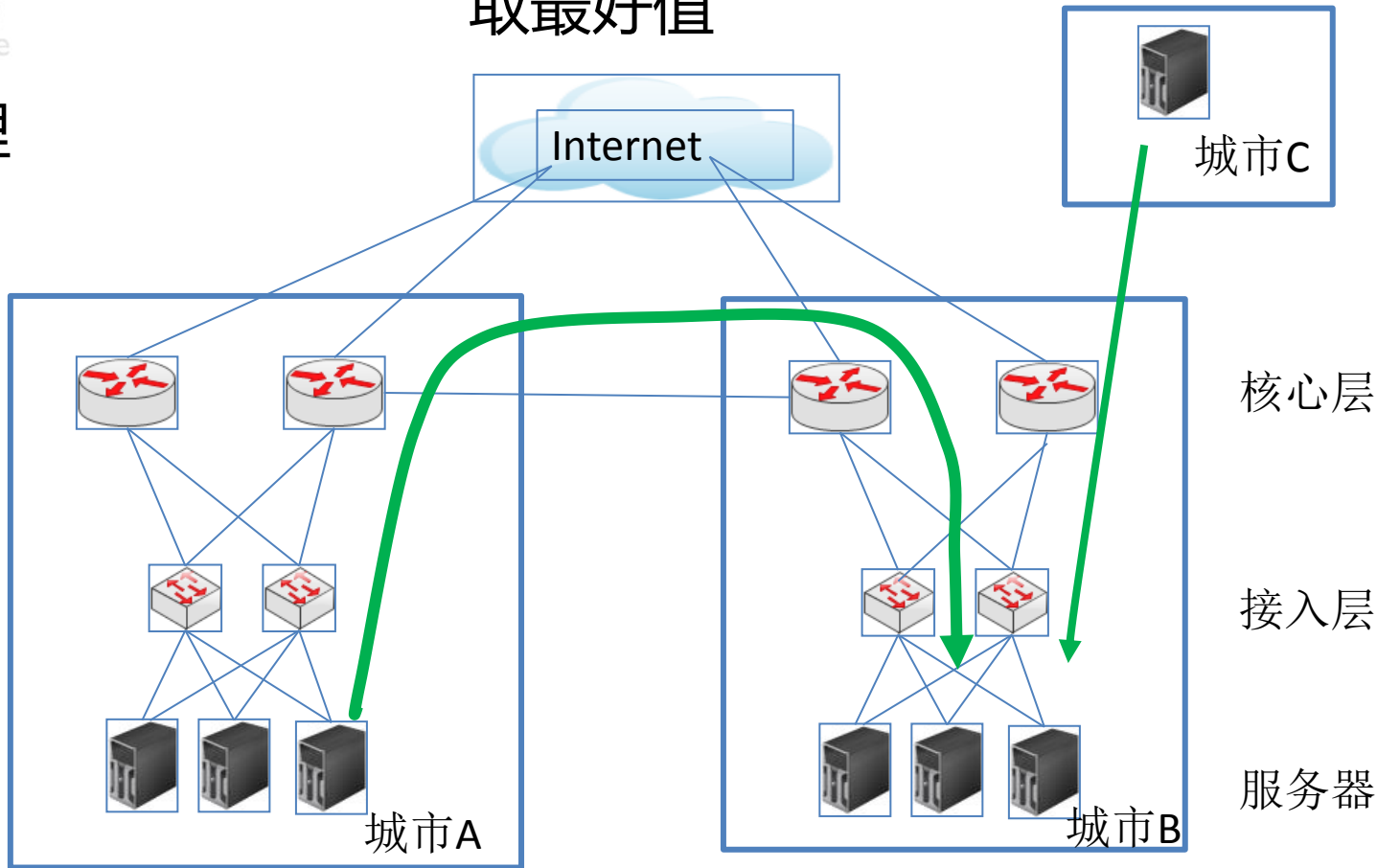
总体思路



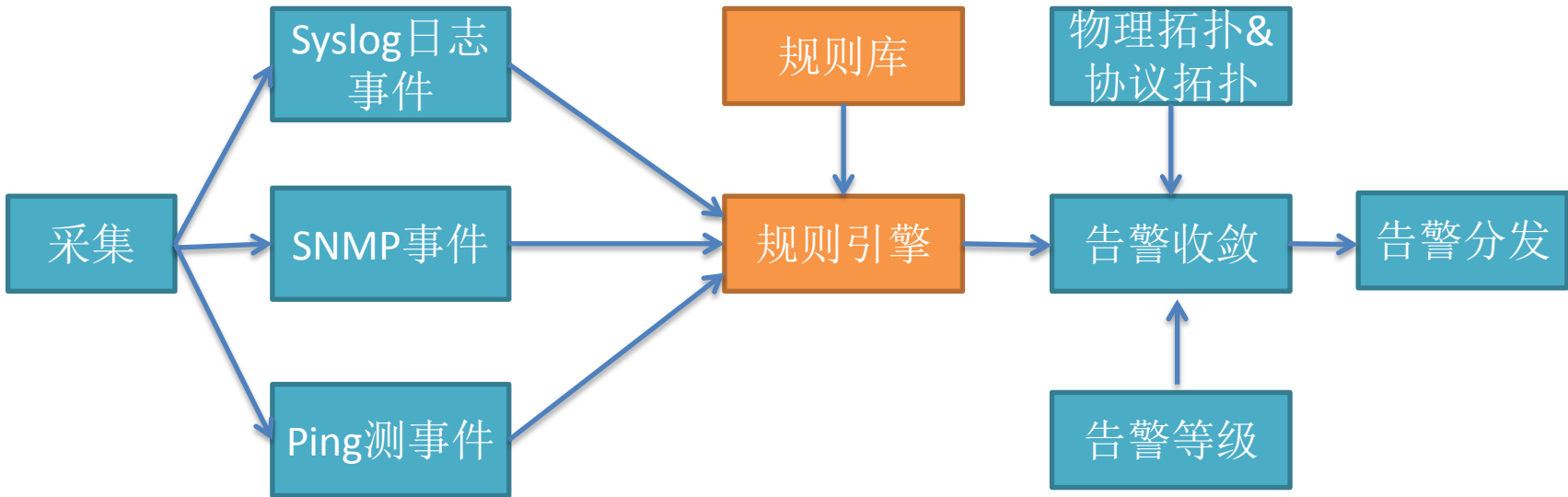
多个ping测源 取最好值



Ping处理



总体思路



规则引擎

端口流量超过带宽的XX%且丢包数超过阈值

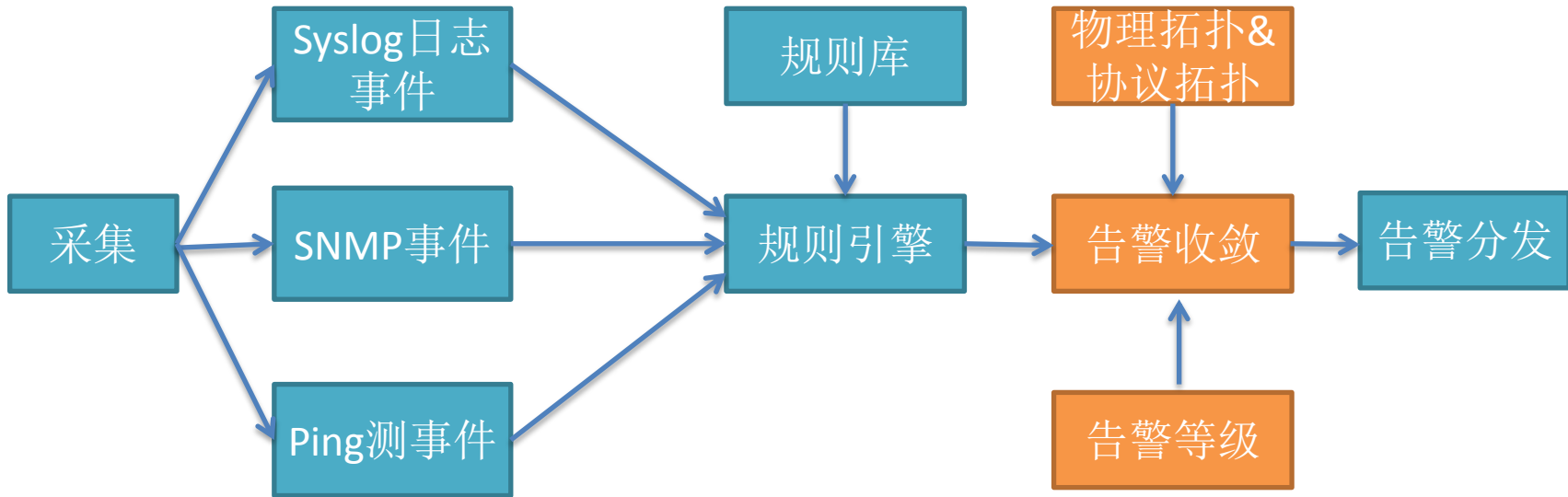
端口在1分钟内连续up,down超过n次

流量下跌超过XX%且连续n分钟低于基线

.....

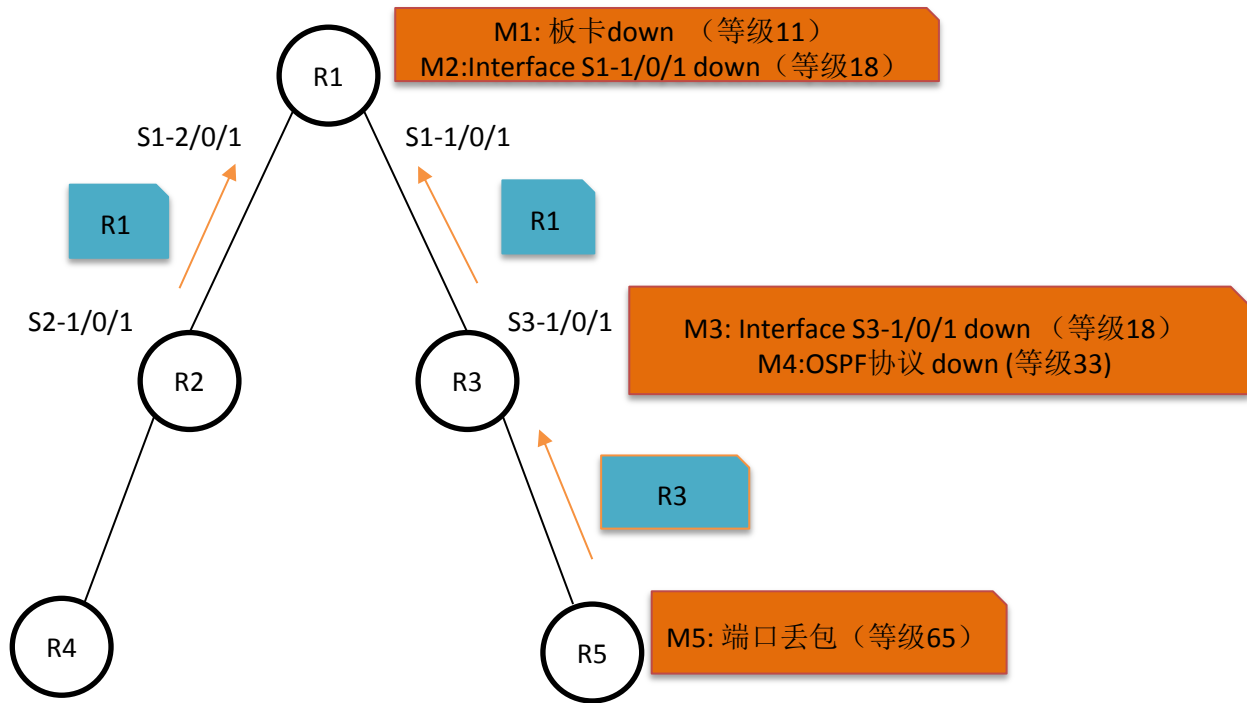


总体思路



告警收敛

- Pagerank
- 告警分级



数据量每分钟千万级

基于spark streaming流式处理，spark graphX图算法

单一的监控手段都有可能失效，要有多重手段

大数据不可怕，基础设施怕的是没有数据

既懂基础设施，又懂数据的人很稀缺，我们非常缺人

Email: Jinghang.hy@alibaba-inc.com



2016 The
Computing
Conference
THANKS

