ALEIYE

让 | 大 | 数 | 据 | 更 | 简 | 单

ALEIYE 安全运维大数据解决方案

北京数介科技有限公司

目录

一、 背景

中小银行现在的传统运维方式存在弊端，主要体现在：

- **以管理工具为主要依托**

  管理内容庞杂，难以实现信息的关联处理

- **以人工处理为主要手段**

  运维效率低下，人员素质限制工作开展的效率及质量

- **以问题故障为主要对象**

  运维工作被动，不利于优化网络架构及资源配置

因此亟需建立统一的智能化管理平台，通过资产信息管理、自动数据采集、科学数据分析达到故障分析，趋势分析和安全分析三位一体，达到网络安全的运维自动化，智能化。

二、 名词解释

名词	解释
ITS	银行自建的设备 IT 设备管理系统，作为系统的重要资产信息来源。
端口	本文档中端口对应网络设备的 port 的属性，也有称作为接口。
流量使用率	当前流量 / 带宽
双线热备	同一业务两条专线连接，带宽相同。在双线热备的情况下，需要将两条专线的流量进行合并，防止两条线的总量达到带宽的上限。保证其中

	一条线路出现故障时，另外一条线路能够满足业务的正常运行。
双线冷备	同一业务两条专线连接，带宽分别为 2M 单独线路跑，但是另一条线冷备份。当主线出现故障时，备应该会存在流量情况。

三、 功能

1. 权限管理

需要有工作组的概念，不同工作组的人员或者不同的工作人具有对资产、操作权限、操作类型等有不同的权限。

2. 基础配置

系统的基本配置功能。

3. 资产管理

资产管理对象分为设备和线路，设备分为网络设备、安全设备、服务器和其他设备四类，当设备为网络设备（交换机、路由器、防火墙）时则在一台设备上会连接多条线路；设备及线路的信息在页面中以树状图的形式切换进行展现；

1) 数据接入

数据来源	**采集方式**

<table>
<tr><td>ITS</td><td>数据库对接。采用 jdbc 的连接方式，每天凌晨读取数据库，将 ITS 中的资产信息自动同步到平台，用户也可实时地进行 ITS 信息同步。
要求：用户可通过界面配置数据库连接及获取的检索语句。</td></tr>
<tr><td>字段</td><td>现有字段：
<table>
<tr><td>id</td><td>hostname</td><td>master</td><td>mastergroup</td><td>info</td></tr>
<tr><td>标识</td><td>计算机名称</td><td>管理员 A</td><td>用户人组</td><td>用途</td></tr>
<tr><td>opstype</td><td>datatype</td><td>ietype</td><td>hardbrand</td><td>hardtype</td></tr>
<tr><td>操作系统类型</td><td>数据类型</td><td>ie 版本</td><td>硬件型号</td><td>硬件类型</td></tr>
<tr><td>ipaddress</td><td>maxaddress</td><td>cabinetno</td><td>howmuchu</td><td>positionu</td></tr>
<tr><td>ip 地址</td><td>mac 地址</td><td>机柜编码</td><td>cpu 数</td><td>位置</td></tr>
<tr><td>startdate</td><td>enddate</td><td>powernum</td><td>fiberinfo</td><td>jijia</td></tr>
<tr><td>上线日志</td><td>保修期限</td><td>电源数量</td><td>光纤</td><td>机架</td></tr>
<tr><td>mapipaddress</td><td>other</td><td>areacode</td><td>thirdcom</td><td>systemcode</td></tr>
<tr><td>映射 ip 地址（用;分割）</td><td>其他</td><td>区域编码</td><td>第三方公司</td><td>系统编码</td></tr>
<tr><td>masterB</td><td>relationdep</td><td>txname</td><td>txsoftware</td><td>txlevel</td></tr>
<tr><td>管理员 B</td><td>相关部门</td><td>设备名称</td><td>软件版本</td><td>运行等级</td></tr>
<tr><td>txbackup</td><td>zjjtype</td><td>cpunum</td><td>cpuhe</td><td>memory</td></tr>
<tr><td>运行备份方式</td><td></td><td>cpu 数量</td><td>cpu 核数</td><td>内存</td></tr>
<tr><td>powerapprove</td><td>hardcom</td><td>jumpline</td><td>jumpprint</td><td>dns</td></tr>
<tr><td>电源</td><td></td><td>跳线点</td><td></td><td></td></tr>
</table>
红色标记为网络设备分析使用到的字段</td></tr>
<tr><td>读取设备配置信息</td><td>SNMP 或执行读取配置脚本的方式自动讲配置中的设备信息读取到平台。
网络设备品牌分两种：cisco 和锐捷,读取配置的命令相同，但是解析方式不同。
show run
要求：用户需要通过在 ITS 或人工录入的方式指定设备的品牌，类型和型号并可以指定采集脚本进行采集设备及接口的基本信息。</td></tr>
<tr><td>字段</td><td>不同类型的网络设备读取的字段有所不同.</td></tr>
</table>

交换机配置信息如下：

hostname	portname	protdesc	porttype	Boards
设备名称	端口名称	端口描述	接口类型	板卡
vlan	vlanname			
vlan 编号	vlan 名称	版本	配置最后变更时间	

路由器配置信息如下：

hostname	portname	protdesc	IPaddress	Boards
设备名称	端口名称	端口描述	接口 IP	板卡
vlan	vlanname			
vlan 编号	vlan 名称	版本	配置最后变更时间	

防火墙配置信息如下：

hostname	portname	protdesc	porttype	Boards
设备名称	端口名称	端口描述	接口类型	板卡
vlan	vlanname			IPaddress
vlan 编号	vlan 名称	版本	配置最后变更时间	接口 IP

人工录入	人工录入设备，管理设备属性。 人工可将设备录入平台，并可以对现有的设备进行属性管理。 **要求**：不受设备结构化设计限制，任意添加设备属性。手工录入字段如果和 ITS 或配置信息读取的字段冲突，那么将以 ITS 或自动读取到的配置信息为主。
字段	1、自定义添加 只需要给出字段中文名、英文名和值即可。 2、批量更新 用户需先将最新的自定义属性批量导出，在此基础上进行修改，然后以文件上传的形式导入平台；导出的文件系统需有标识，从而在批量更新时能够判断文件是最新的； 网络拓扑业务需要设备接口属性中必须添加以下字段用于网络拓扑的分析，因此以

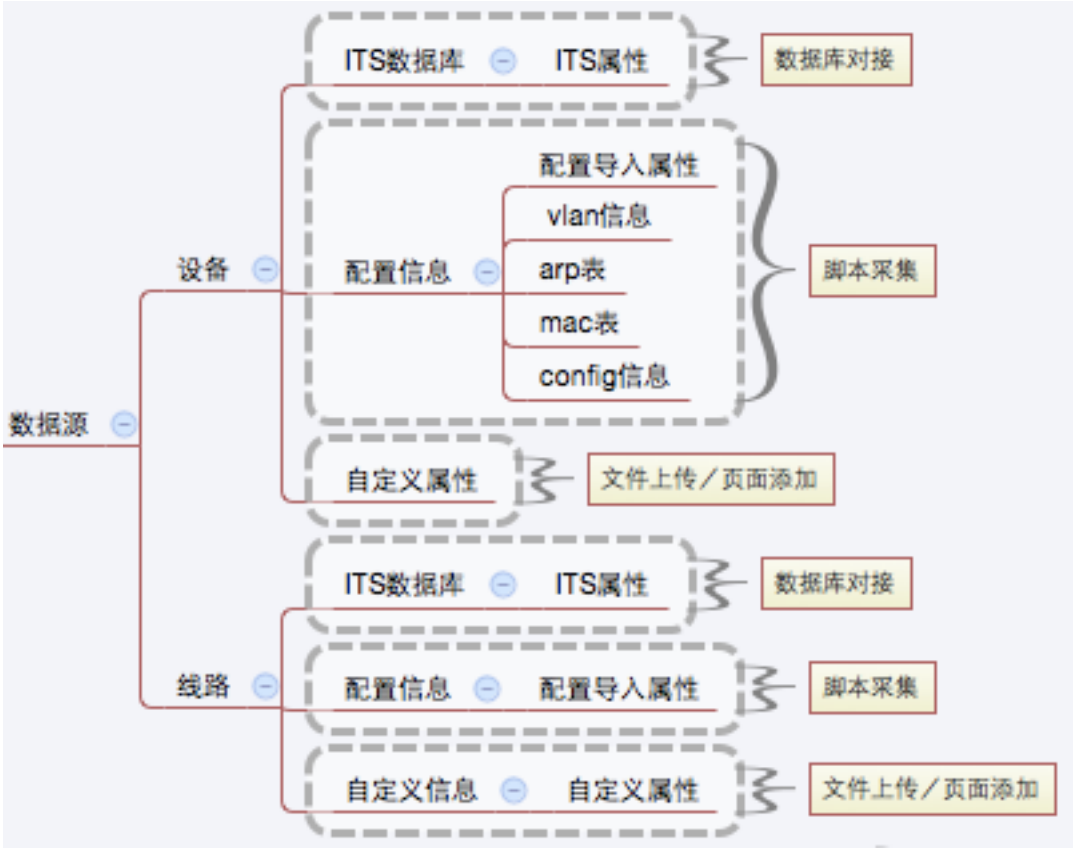
下字段为线路自定义属性中必填属性；

字段	描述
对端描述 to_desc	如果是网络设备，填写对端管理管理 IP。如果是对端服务器则有系统通过设备关联章节的说明自动发现。
设备级别 level	交换机：核心、汇聚核心、接入 路由器：骨干、区域、汇聚 级别类型不仅限于以上几种类型。

负载分析业务中需设备接口中必须有一下字段：

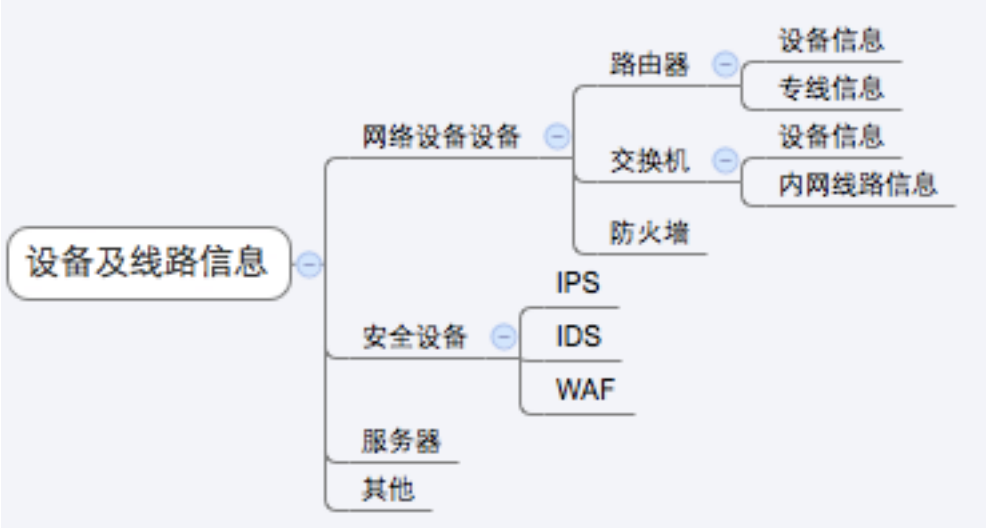
运营商、带宽、专线号

设备及线路信息来源一览图：



2) 资产信息管理

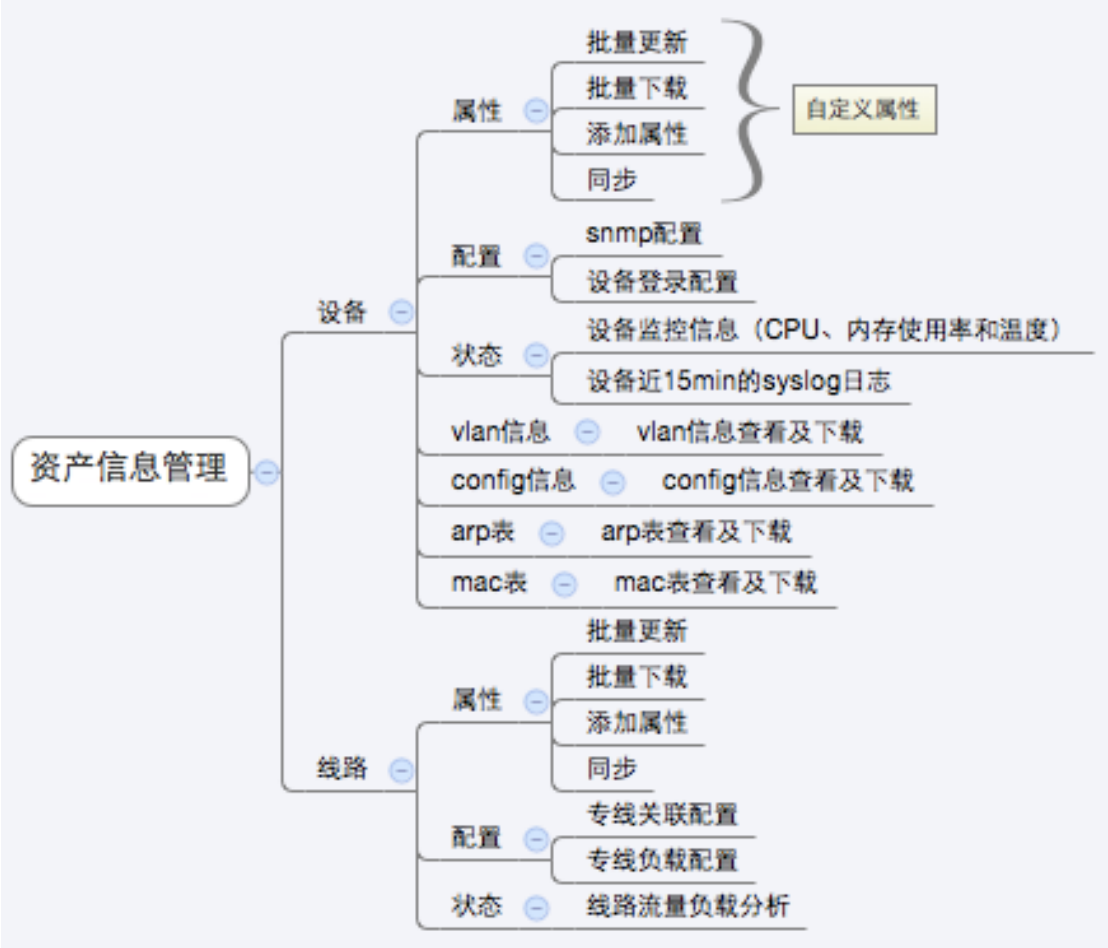
树形图：将所有设备和线路信息通过树形图进行展示，树形图分为网络设备、安全设备、服务器和其他四大类；分类如下图：



在具体设备的分类下用户可进行输入设备或线路 IP 搜索，从而快速查找设备，例如，在网络设备分类下的路由器设备，当输入 127.0.0.1 进行搜索时可快速查找到该路由器设备及该设备的资产信息。

通过点击左侧树形图进行交互，当点击某一台设备时可查看该设备的信息，包括属性、配置、状态、vlan 信息、config、mac 表和 arp 表；点击线路时可查看具体一条线路的信息，包括属性、配置和状态；

资产信息管理页面功能整理如下：



➢ 设备信息

属性

设备属性来源分为三类，分别为：自定义属性、ITS 属性和配置属性，

用户可对自定义属性进行新增、编辑和删除操作；新增自定义属性可通过页面添加和批量更新的方式；当选择为页面添加属性时则需定义字段的中文名、英文名和值，当选择批量更新时则需要先将最新的自定义属性批量导出，在此基础上进行修改然后以文件上传的形式导入 Aleiye 系统中;在此需要注意的是：批量导出时可导出该用户所管理的所有设备的自定义属性，用户若只需要修改当前设备的自定义属性则在导出文件中只修改该部分属性即可；批量导入时系统需判断该文件为最新文件，负责将提示“该文件不是最新文件，请下载最新自定义属性

后再进行更新”；

ITS 属性内容包括英文名、中文名和值，例如：positionu 位置 和平里机房；系统默认为每天凌晨更新一次 ITS 数据库信息，当用户需要实时修改 ITS 属性时则需要修改 ITS 数据库信息后，点击同步可进行实时更新；

配置属性内容包括英文名和值，例如：interface GigabitEthernet1/1/4；系统默认为每天凌晨更新一次配置信息；页面不支持对该部分信息进行操作。

配置

配置分为两部分，分别为 SNMP 接入配置和设备登录配置，SNMP 接入配置项为 SNMP 读写码，系统默认为“public”；设备登录配置为系统登录该台设备时所需配置项，分别为登录名、密码和 enable 密码；输入密码及 enable 密码时均为密文输入，用户输入完可通过点击验证按钮进行准确性验证；当验证失败时页面需提示错误信息，如：“设备登录密码输入错误”或“设备 enable 密码输入错误”。

配置完毕后点击保存；

状态

状态栏显示该设备的监控信息和该设备近 15 分钟的 syslog 日志；

监控信息包括设备 CPU 使用率、内存使用率和温度信息，页面默认时间为今天 0：00：00-当前时间，（时间精确到分钟）用户也可进行时间范围的自定义；用户也可进行时间粒度的选择，选项为 1min、15min、30min、1h、2h；

设备 syslog 信息显示时固定页面高度，加滚动条；

Vlan 信息、config 信息、ARP 表、MAC 表

页面默认显示昨天的相关信息，用户可自定义时间进行展示，例如：用户可选择时间为 2015/09/01；该部分信息可提供下载，当点击下载时用户需定义要下载的信息的时间范围，例如：2015/08-01—2015/09 / 01；

Vlan 信息可通过该设备的配置信息获得，在配置信息中包含 Vlan 信息，样例如下：

Vlan402 description： conncect to JGM-BJZH-R7606-1 vlan 989 and carring for sub-bjzh data ip address： 10.1.0.252 255.255.255.0 ip access-group caozuotai-control instandby 42 ip 10.1.0.254

ARP 表信息可通过“show arp”命令进行获取，样例如下：

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.250.1.51	134	f866.f283.8ebf	ARPA	Vlan1
Internet	192.250.1.42	176	f866.f283.8ebf	ARPA	Vlan1
Internet	10.4.0.22	79	f866.f283.8ebf	ARPA	Vlan1

MAC 表信息可通过“show mac add”命令获取，样例如下：

Vlan	Mac Address	Type	Ports
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU
All	0180.c200.0002	STATIC	CPU
All	0180.c200.0003	STATIC	CPU
All	0180.c200.0004	STATIC	CPU

- **线路信息**

线路资产信息分为三部分，分别为属性、配置和状态；

属性

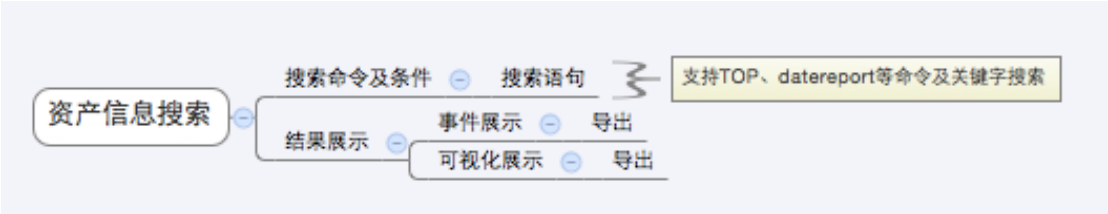
线路属性来源分为四类，分别为自定义属性、ITS 属性、配置属性和拓扑属性；自定义属性可进行新增删除修改操作，新增自定义属性的方式分别为：页面添加和批量更新；当用户需要实时修改 ITS 属性时则需要修改 ITS 数据库信息后，点击同步可进行实时更新；

配置属性页面可配置专线类型和线路负载相关配置项，专线类型分别为单线、双线冷备和双线热备；注：只有设备类型为路由器时（线路为专线）才会出现专线类型配置；

状态页面显示该线路的流量负载情况，页面默认显示时间为今天 0:00:00—当前时间，用户也可自定义时间范围进行显示；用户也可选择粒度和统计放式进行分析，粒度选项分别为 1min、5min、15min、30min、1h 和 2h。统计方式分别为求和、平均、最大和最小四种方式。

3) 资产信息搜索

根据银行资产统计和检索的需求，资产信息搜索模块提供关键字检索和设备的信息统计功能；功能结构如下图所示：



资产信息统计：对自定义属性、配置导入属性、ITS 属性等不同来源的资产属性

（字段）可通过统计命令（支持 TOP 和 date report 命令）进行检索统计生成统计结果，并以报表形式进行页面展示。已经成型的业务报告（如周报、月报等）可通过界面定制的方式固化到首页页面上。

关键字检索：针对设备数量多，设备及线路属性复杂，无法进行快速查找，关键字检索功能提供通过关键字对设备属性进行全方位搜索。如如：描述字段、机房位置等多个属性信息中同时含有”hepingli”关键字，那么通过”hepingli”关键字就可获得所有的设备列表，方便统计设备的信息。

导出功能：对资产信息的统计详情、可视化报表以及关键字检索的结果可进行导出，系统默认导出文件为 csv 格式。

4. 负载分析

结合一期功能及改进需求和太阳风功能的替代等需求，负载分析功能分别对专线进行流量负载分析，对设备进行 CPU 使用率、内存使用率、温度负载分析；

1) 数据接入

各指标数据来源如下：

指标	类型		获取方式
流量	in	字节	snmp 获取，每一分钟获取一次。
	out		
CPU	使用率		
内存	使用量—>结合资产信息或抓取内存总量转化为使用率		
温度	摄氏度		
接口状态	up/down		Syslog 协议获取，当设备接口状态改变时发送 syslog 日志；

负载分析中各个指标在分析中会关联资产管理中的相关信息，例如流量分析

中通过 IP 地址关联资产信息的属性，例如设备名称、对端业务、线路号、带宽等属性；

2) 功能说明

- **分析功能**

针对设备内存使用率、CPU 使用率和温度以及线路的流量使用率四个指标进行实时统计分析并进行可视化展示。其中分析内容包括负载分析、超载及告警分析、预测。对展示结果可以任意调整粒度（分、时、天）和统计类型（sum、avg、max、min）。

线路流量分析功能基于一起的算法进行改进，具体如下：

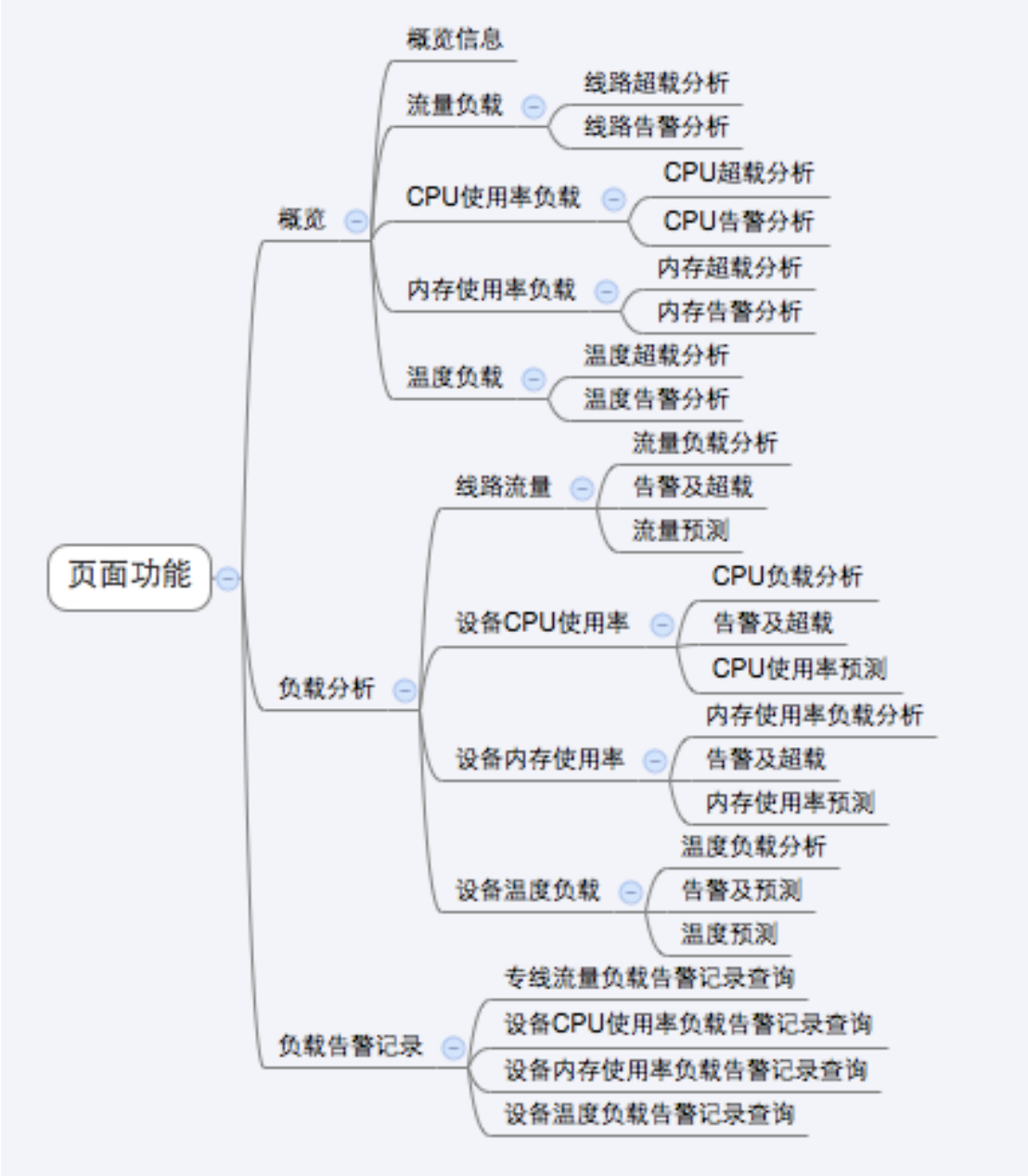
a) 预测周期增长到一个月：当数据积累到六个月或者更长时，更改预测周期为一个月。

b) 预测对比线：历史预测结果保留，在视图界面进行可对比。

设备的 CPU 使用率、内存使用率和温度均以现有算法（流量分析算法）进行分析；

- **页面展示**

负载分析功能分为概览、负载分析、负载告警记录三个模块。如下图所示；



a) 概览模块展示该用户所在组管理的设备及线路数量，以及对其按设备类型、对端业务、运营商、带宽类型进行统计；以各个指标为纬度，将所有设备的超载次数和告警次数进行 top10 排名统计；

b) 负载分析模块交互直接与树形图关联，点击树形图进行设备及线路的切换可直接查看监控分析功能。通过与资产信息关联，显示该设备的如下信息：设备 IP、设备名称、设备类型、设备品牌、所属区域、设备等级。

c) 负载告警记录模块提供各指标的权限内所有设备的告警信息，用户可按时间

范围进行查询；

- **告警功能**

超载告警：流量使用率、CPU 使用率和内存使用率分析时系统为一分钟采集一次，在固定时间段内的点为一个固定值（总次数），当超载次数达到总次数的一定比值时需要进行告警，告警阈值可提供用户自定义；设备的温度异常分析结合实际应用场景，当温度持续超过超载阈（用户可自定义）值达到一定时间（用户可自定义）时系统进行告警；

无日志告警:设备及线路的各个监控指标均采用 SNMP 协议进行数据采集，当系统无法采集到数据达到一定时间（用户可自定义）时则系统进行告警；

注：设备的告警配置均由管理员进行设定，线路的告警（流量告警）在管理员权限下配置完后，在用户权限下可进行修改（线路的资产信息管理中配置页面），并且告警配置以用户配置为准；

5. 设备关联

设备关联是为了将设备间的连接关系（网络拓扑）体现出来，作为故障定位的基础。设备连接分为两类：网络设备（交换机）与服务器的连接、网络设备之间的连接。

1) 数据接入

数据类型	数据获取方式	期望获取结果	字段信息
服务器 IP 地址登记表	ITS 中服务器 ip 地址登记表（wf_biz_base）。每天凌晨自动通过 jdbc 的方式导入平台。	server 与 IP 的对应关系	设备资产中 ITS 的字段描述。mapipaddress 与 maxaddress 是多对一的关系
ARP 表	凌晨 ping 所有已知的服务	ip 与 mac 的对应关	Address：ip 地址

	器和网络设备，过去本地的 arp 表即可。 交换机的 arp 表同样导入到平台。	系（通过对端信息排查错误源）	Hardware Addr:mac 地址 ip 与 mac 一对一
mac 表	每天凌晨通过连接网络设备，通过命令（show mac）的方式进行获取，并导入平台。	mac 与接口的对应关系（ping 命令后抓表）	mac：mac 地址 port：接口信息 一个 port 存在多个 mac 地址

2) 分析功能

i. 服务器与交换机的连接分析方法

a) 扫描所有的的接入层网络设备,获得所有接口类型是 access 的接口。

mac	mac 地址，加 s 表示多个 mac 地址
ip	IP 地址，叫 s 表示多个 ip 地址
port	接口
info	服务器用途
devid	设备 ID

b) 通过 mac 表过滤出 access 接口的所有 mac 地址。并得到 mac 地址接口的一对一的对应关系表—>A(devid,mac,port)

c) 获取 ARP 表，获得 ip 与 mac 的对应关系表—>B(ip,mac)。

d) 合并 A、B 表获得 ip 与 port 的对应关系表→C（devid,ip,port）

e) 通过 IP 地址登记表（wf_biz_base）表获得 IP 与 server 的对应关系→D(ip,info)

f) 合并 C、D 获得 info 与 port 的关系→E(devid ,port,ip,info)

最终 E 表就是网络设备(devid)与服务之间的连接关系。

ii. 网络设备间的分析方法

a) 由核心出发，获取所有是启动并且接口类型为 trunk 的接口列表 A（devid，port）。

b) 获取核心的 MAC 地址表，通过列表 A 可知道所有接入到核心层的每个接口与下层连接的网络设备和服务器的对应表 B(devid,port,macs)

c) 获取 ARP 表，得到 ip 与 mac 的对应关系 C（ip,mac）

d) 获取 ip 地址登记表中获取设备列表 D（ip,hardtype）

e) C 表与 D 表通过 IP 做交集，并且过滤设备类型是服务器的情况获得 E 表（ip，mac），仅仅保留网络设备的 ip（管理地址 IP）地址和 mac 情况

f) B 表和 E 表通过 mac 进行关联获得 F 表（devid，port，ips）

g) 通过 ip 地址登记表获取下一层（汇聚层或接入层）的网络设备列表 G(ip)

h) F 表与 G 表通过 ip 进行关联，得到一个 H 表（devid，port，ip）

i) 再通过二层的 mac 表即可获得二层与核心的接口对关系，形成映射表 I（devid,port,ip,对方 port）。

j) H 表即为核心交换机每个端口连接的网络设备情况。

k) 二层，三层设备递归遍历最总获得整个网络拓扑结构。

iii. 差异报告

在分析连接关系过程中（网络设备与网络设备，网络设备与服务器的所有连接关系），需要监控出连接关系的变化，并对发生变化的连接关系（每天比前一天连接方式发生了变化的连接）给出报告，每天一个报告。

3) 存储需求

每天留存 config、arp 和 mac 表，原文可提供下载。

6. 故障定位

针对路由器和交换机接口的状态变化进行定义故障，当接口的状态由 down 变为 up 的间隔时长大于等于 5 秒时（间隔时长用户可根据实际情况进行自定义）则定义为该接口的一次故障事件。

1) 数据接入

网络设备（路由器和交换机）接口状态改变时发出 syslog 日志，指向平台 syslog 接收器。当设备为路由器时则接口所连接线路为专线，当设备为交换机时接口所连接线路为内网线路。

2) 分析功能

- **纵向分析**

i. **日志归并为事件**

网络设备同一接口出现故障，故障因为具备传播性，所以同时会在三层抛出日志。

层	关键字
网络层	第三层关键字（备选）
链路层	protocal
物理层	Interface

不同层短时间内（5s）出现的多条日志（syslog）应该归并为一个事件。

事件是故障分析的基本单位。

ii. **闪断和故障的判断：**

闪断是指在短时间（5~10s）内接口出现的先 down 然后又 up 的情况。这样的情况一般不会对业务产生大的影响，闪断不需要告警只需要记录。

故障是指接口出现 down 以后，短时间（5~10s）内没有出现 up 的情况。会对业务系统产生影响，甚至不可用。所以此类情况一定要告警。

iii. **无日志情况**

通过 snmp 的轮询机制，如果出现了数据无法获取的情况那么系统告警和事件级别挂钩，在和告警平台挂钩

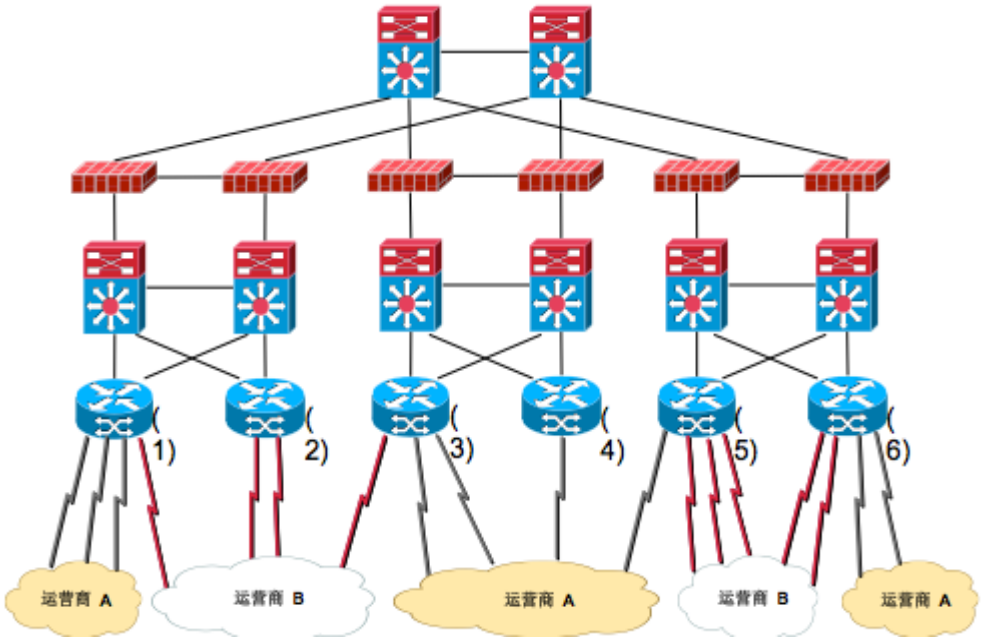
- **横向分析**

横向关联是指通过单一事件无法简单的定位出问题的关键，需要将同时出现的多个事件进行分析，找到共性或符合规则的情况

i. **同一属性故障分析**

1. 在 1 分钟内出现的所有事件，进行关键属性的分析。
2. 如果出现了所有事件存在共有属性的情况，判断运行着的拥有相同属性的线路是否仍然正常运行
3. 如果存在，说明不是该属性的问题。如果不存在，那么可以认定设备故障的根源就在于此了。

如当多个接口同时出现了 down 的信息，但是所有的属性中运营商的值都是 B，并且运营商 B 的线路没有一条在正常运行， 那么基本断定运营商 B 出现问题。



ii. 多规则冲突

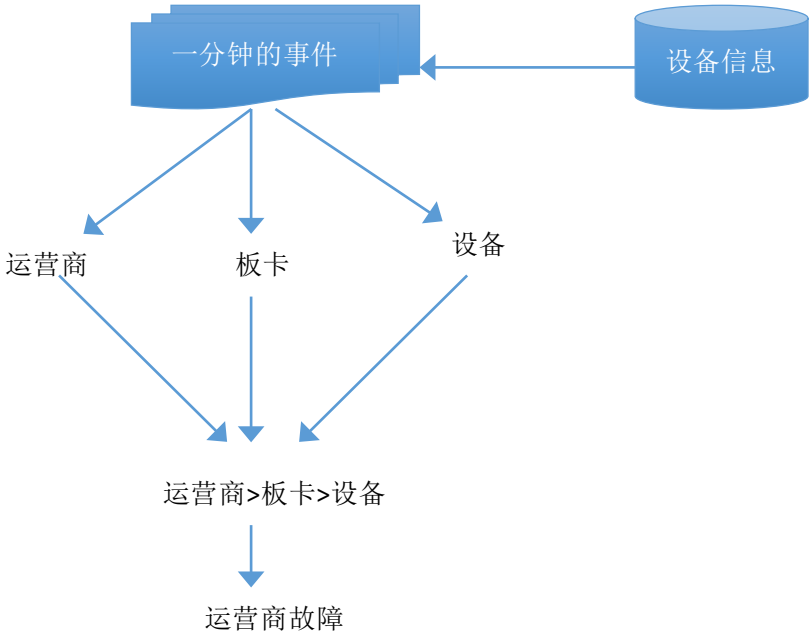
同一属性的分析存在冲突性，应该有一个二级规则用于归并和消除多个同一属性的冲突结果。如

事件： G1/0 设备 1 运营商 A

G1/1 设备 1 运营商 A

G1/2 设备 1 运营商 A

分析方法



结论：运营商 A 出现故障

故障定位结论以告警方式展现，如：

运营商 A 出现故障　起始时间~结束时间
G1/0　设备 1　运营商 A
G1/1　设备 1　运营商 A
G1/2　设备 1　运营商 A

告警信息：

影响性分析：业务的影响性

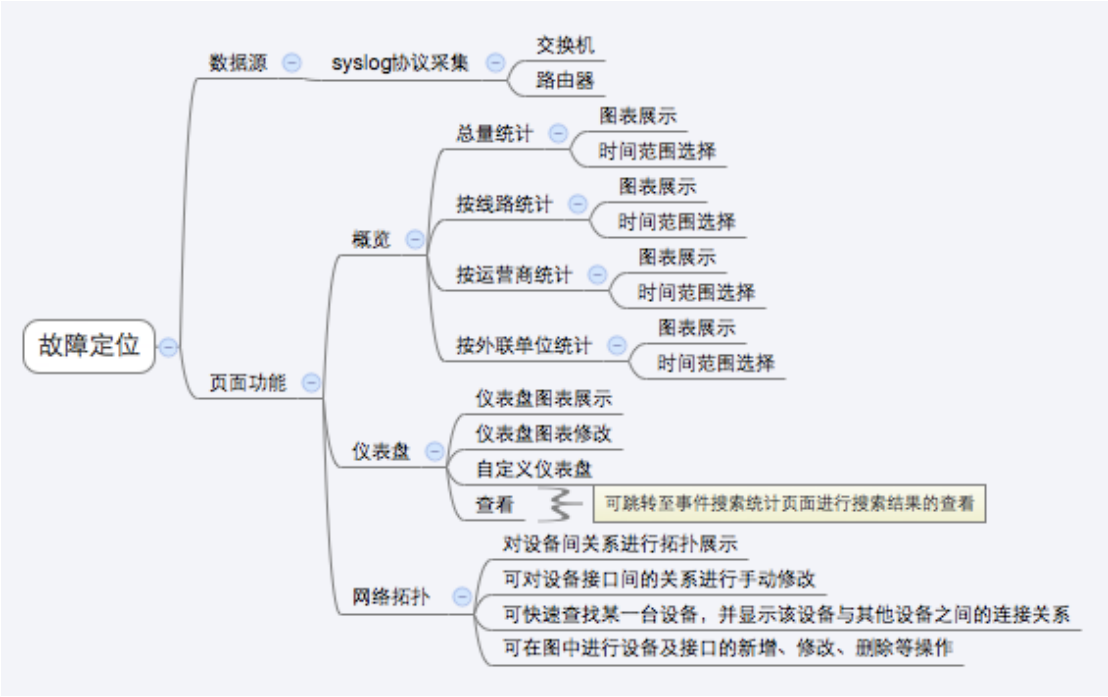
3) 页面展示

故障定位功能页面分为概览模块、仪表盘模块和网络拓扑模块三部分；如下图所示：

概览模块结合业务和用户场景，分别对线路故障按总量统计、按线路进行 top 统计、按运营商统计以及按外联单位进行统计。用户可对图表的显示时间范围进行自定义。

用户可在事件搜索统计中将搜索语句进行保存为报表，添加至仪表盘中进行显示，用户也可以在仪表盘中进行自定义仪表盘。

网络拓扑模块显示权限内所有设备及接口的连接关系，在拓扑图中用户可添加、编辑或删除设备和接口以及各接口之间的连接关系。在拓扑中可实时显示线路的状态（up / down）。



7. 事件搜索统计

事件搜索统计功能提供对接口事件日志的检索，可支持 aleiye 原语搜索语句；页面功能如下图所示：