



# 恒景科技 iRecovery产品介绍



# iRecovery (网络故障自愈系统)

# 网络维护难题



如何快速定位网络故障源?



如何快速排除网络故障?



如何实现网络故障自动愈合?

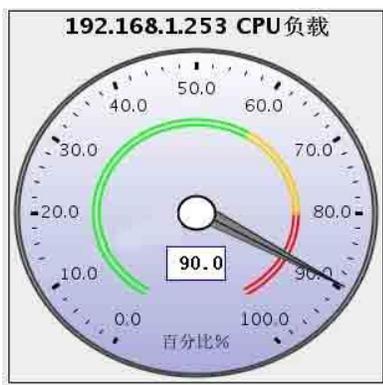


如何对故障历史数据追溯分析

# 网络自愈解决方案



# 多种网络恢复方式—手动自愈型



1. 人工发现网络故障
2. 通过网络自动愈合系统获取有效信息
3. 根据提示信息判断故障源
4. 选择愈合手段, 实施成功
5. 排除故障, 网络恢复

手工屏蔽操作窗口

被屏蔽对象: 192.168.1.122

可选操作项:

- 交换机屏蔽该IP对应MAC地址
- 路由器屏蔽该IP地址(ARP法)
- 屏蔽该IP对应交换机端口(脚本法)
- 屏蔽该IP对应交换机端口(SNMP法)
- 屏蔽该IP对应路由器端口(脚本法)
- 屏蔽该IP对应路由器端口(SNMP法)

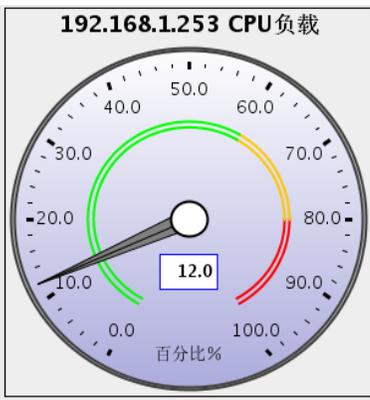
确认 取消

消息窗口

将在交换机(172.31.1.123)上屏蔽 192.168.1.122所对应的MAC地址 0011.096f.b779, 是否确认? [确认] [取消]

消息窗口

屏蔽192.168.1.122成功!!



# 多种网络恢复方式—无人值守自愈型

iRecovery以策略为中心基于事前管理，自动综合相关历史、实时数据，动态检测网络性能异常，捕捉故障征兆，防患于未然。按照“发现故障—分析原因—自动排除故障”的模式，完全实现无人值守型的网络故障自动愈合。

- 按照需求自定义策略。
- 支持自动屏蔽（多种屏蔽措施）故障源或报警。
- 支持对网络设备的端口、流量、负载等做阈值告警
- 对各项自愈记录或报警有详细记录。
- 支持白名单功能。可排除免监测IP或端口。

自愈措施信息	
自愈措施:	交换机屏蔽物理端口(SNMP法)
自愈对象最大数目:	交换机屏蔽物理端口(SNMP法)
被排除IP:	交换机屏蔽物理端口(脚本法)
被排除交换机端口:	交换机屏蔽IP对应MAC地址
被排除路由器端口:	路由器屏蔽物理端口(SNMP法)
巡视周期(秒):	路由器屏蔽物理端口(脚本法)
屏蔽时长(秒):	路由器屏蔽IP(ARP法)
短信发送周期(秒):	重新启动路由器
工作状态:	重新启动交换机
	ARP阻断IP
	生成报警记录
	短信报警

# 功能特性

1 无干扰式部署

2 全方位数据采集

3 设备信息、流量查询

4 精准定位故障源

5 网络故障自动处理

6 地址准入管理

7 强大的外部接口

# 1 无干扰式部署

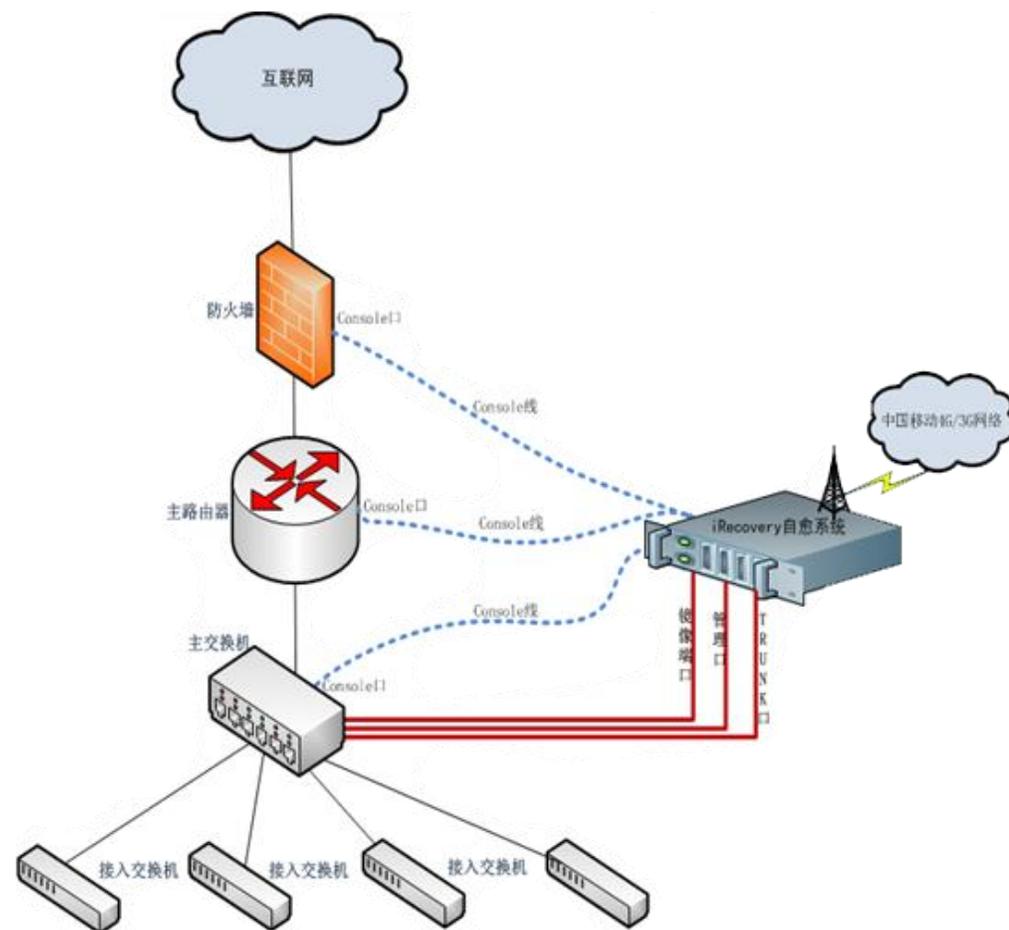
a. 纯旁路部署, 对当前网络零影响

b. 所有重要的设备均采用Console线连接

c. 中国移动4G网络提供备用链路

d. Trunk端口可通达网内任何一个子网

e. 镜像端口采集流量, “流量重现”



## 2 全方位数据采集

协议支持

*SNMP Netflow Netstream  
IPAccounting XFlow Syslog ...*

 Ruijie 锐捷  
Networks

 H3C

 HUAWEI

 DPtech

 JUNIPER  
NETWORKS

 CISCO ...

设备  
无关性

详细信息

*CPU Memory SrcIP SrcMAC  
DesIP DesMACPPS BPS ...*

# 3 设备信息、流量等查询

设备性能

流量信息

报警信息

SYSLOG

序号	端口名称	端口描述	总数	每秒平均值	端口类型	开始时间
1	Gi1/13	to_...	3.21G bytes	200.7M bps	互连 上连	2017-05-23 16:18:47
2	Gi8/11	to_...				
3	Gi8/22	to_...				
4	Gi8/1	to_...				
5	Gi8/20	to_...				
6	Gi8/18	[[mac=31]]				
7	Gi8/21	[[mac=43]]				
8	Gi8/4	[[mac=1]]				
9	Gi8/19	to_...				
10	Gi8/17	[[mac=1]]				
11	Gi8/16	[[mac=61]]				
12	Gi8/13	[[mac=26]]				
13	Gi8/15	[[mac=45]]				
14	Gi8/23	to_...				
15	Gi8/25	to_...				
16	Gi8/27	to_...				
17	Gi8/10	to_5F...				
18	Gi8/9	to_...				
19	Gi8/7	to_sec...				
20	Gi8/8	to_ir...				

实时流量->路由器Flow流量排序->[发送流量(bps)和接收流量(bps),最近1分钟]

查询 显示最新 显示图形 流量由大到小 时间由后到前 时间由前到后 可选操作 流量追溯

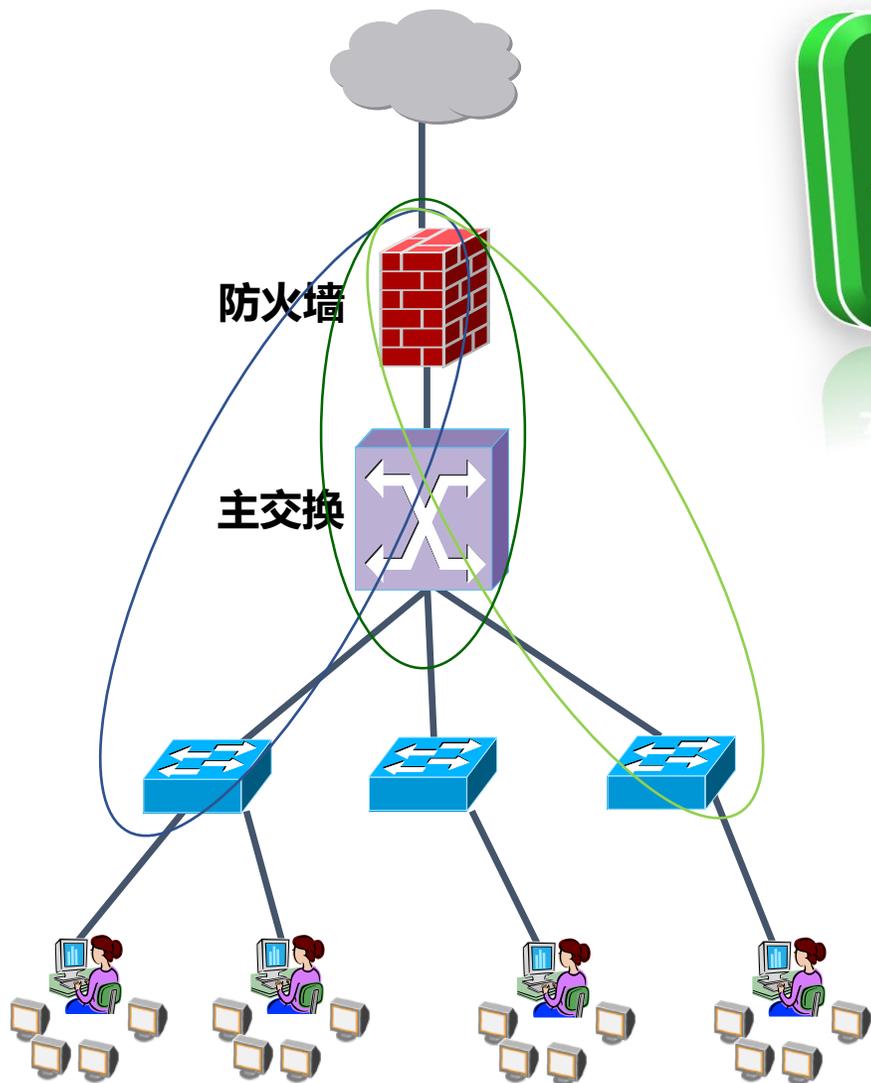
序号	IP	总数	每秒平均值
发送#1	182.1.1.44	175.81M bytes	23.44
接收#1	210.1.1.34	459.73M bytes	61.3M
发送#2	124.1.1.4	163.05M bytes	21.74
接收#2	210.1.1.34	333.83M bytes	44.51
发送#3	124.1.1.3	90.39M bytes	12.05
接收#3	210.1.1.4	196.72M bytes	26.23
发送#4	124.1.1.6	80.68M bytes	10.76
接收#4	210.1.1.26	115.77M bytes	15.44
发送#5	124.1.1.7	65.3M bytes	8.71M
接收#5	210.1.1.35	53.27M bytes	7.1M
发送#6	124.1.1.155	49.92M bytes	6.66M
接收#6	210.1.1.39	50.15M bytes	6.69M
发送#7	124.1.1.240	41.06M bytes	5.48M
接收#7	192.1.1.244	23.09M bytes	3.08M
发送#8	210.1.1.34	39.84M bytes	5.31M
接收#8	172.1.1.51	21.33M bytes	2.84M
发送#9	124.1.1.5	35.4M bytes	4.72M
接收#9	210.1.1.20	18.53M bytes	2.47M
发送#10	180.1.1.11	31.35M bytes	4.18M
接收#10	210.1.1.242	18.25M bytes	2.43M
发送#11	210.1.1.135	29.69M bytes	3.96M
接收#11	210.1.1.89	17.47M bytes	2.33M

辅助功能-镜像流量排序->设备10.0.25采集->[发送流量(bps)和接收流量(bps),最近1分钟]

查询 显示最新 显示图形 流量由大到小 时间由后到前 时间由前到后 可选操作 流量追溯

序号	IP	总数	每秒平均值	开始时间
发送#1	60.2.1.7.20	76.28M bytes	10.17M bps	2017-05-23 16:28:07
接收#1	210.1.1.2.108	55.86M bytes	7.45M bps	2017-05-23 16:27:31
发送#2	124.1.1.3.95	28.42M bytes	3.79M bps	2017-05-23 16:27:43
接收#2	210.1.1.133	48.07M bytes	6.41M bps	2017-05-23 16:27:31
发送#3	60.2.1.12	11.58M bytes	1.54M bps	2017-05-23 16:28:05
接收#3	172.1.1.210	38.97M bytes	5.2M bps	2017-05-23 16:27:31
发送#4	124.1.1.143	6.19M bytes	825 Kbps	2017-05-23 16:28:08
接收#4	218.1.1.101	6.6M bytes	880 Kbps	2017-05-23 16:27:31
发送#5	14.1.1.179	5.65M bytes	753 Kbps	2017-05-23 16:28:13
接收#5	172.1.1.211	5.94M bytes	791 Kbps	2017-05-23 16:27:41
发送#6	150.1.1.173	4.79M bytes	638 Kbps	2017-05-23 16:27:44
接收#6	172.1.1.214	3.75M bytes	499 Kbps	2017-05-23 16:27:33
发送#7	124.1.1.1.63	4.5M bytes	599 Kbps	2017-05-23 16:27:40
接收#7	124.2.1.1.214	1.3M bytes	173 Kbps	2017-05-23 16:27:46
发送#8	210.1.1.54	3.73M bytes	497 Kbps	2017-05-23 16:27:31
接收#8	60.2.1.7.20	1.03M bytes	137 Kbps	2017-05-23 16:28:12
发送#9	210.1.1.203	2.87M bytes	383 Kbps	2017-05-23 16:27:31
接收#9	118.1.1.1.49	628 Kbytes	83 Kbps	2017-05-23 16:28:19
发送#10	103.1.1.3.50	2.45M bytes	326 Kbps	2017-05-23 16:27:47
接收#10	198.1.1.1.213	533 Kbytes	71 Kbps	2017-05-23 16:27:31
发送#11	210.1.1.1.133	1.85M bytes	247 Kbps	2017-05-23 16:27:31
接收#11	210.1.1.230	280 Kbytes	37 Kbps	2017-05-23 16:27:31

## 4 精准定位故障源



### 实时分析所采集的数据

支持端口流量、IP流量、发包率等查询，查询精度可支持到秒级  
支持各种排序、搜索、历史对比等操作

### 将所管理的设备捆绑管理

将相关设备捆绑进行管理，建立网络平台，二三层绑定  
确定故障目标

### 精确定位故障源

可定位至设备端口、IP地址、MAC地址



相比于传统的定位故障IP，  
本系统借助“二三联动”，  
定位故障IP的同时可定位该  
IP接入终端交换机所在端口！

# 5 网络故障自动处理

**基本信息**

站点名称: 四季青97网段路由器3\_3\_3\_14

规则链: 规则链#0

优先级: 优先级#0

执行宿主机: 10.0.10.25

规则描述:

**主触发条件信息**

主触发条件: 自定义路由器监测规则

自定义监测规则: SNMP法获取Cisco设备CPU利用率值->CPU\_5秒钟平均

计算方式: 大于

自定义主触发值: 70

主条件采样参数: 过去 60 秒

**并发触发条件信息**

并发触发条件: 单IP发送包值(pps)

并发触发值: 3000

并发条件IP流量数据源: Netflow

并发条件采样参数: 过去 60 秒

并发条件监控IP: 192.168.10.0/24;192.168.20.0/24

并发条件排除IP:

**自愈措施信息**

自愈措施: 定位交换机屏蔽IP对应物理端口

自愈对象最大数目: 3

巡视周期(秒): 120

屏蔽时长(秒): 120

短信发送周期(秒): 3600

辅助报警方式:  声音报警  邮件报警

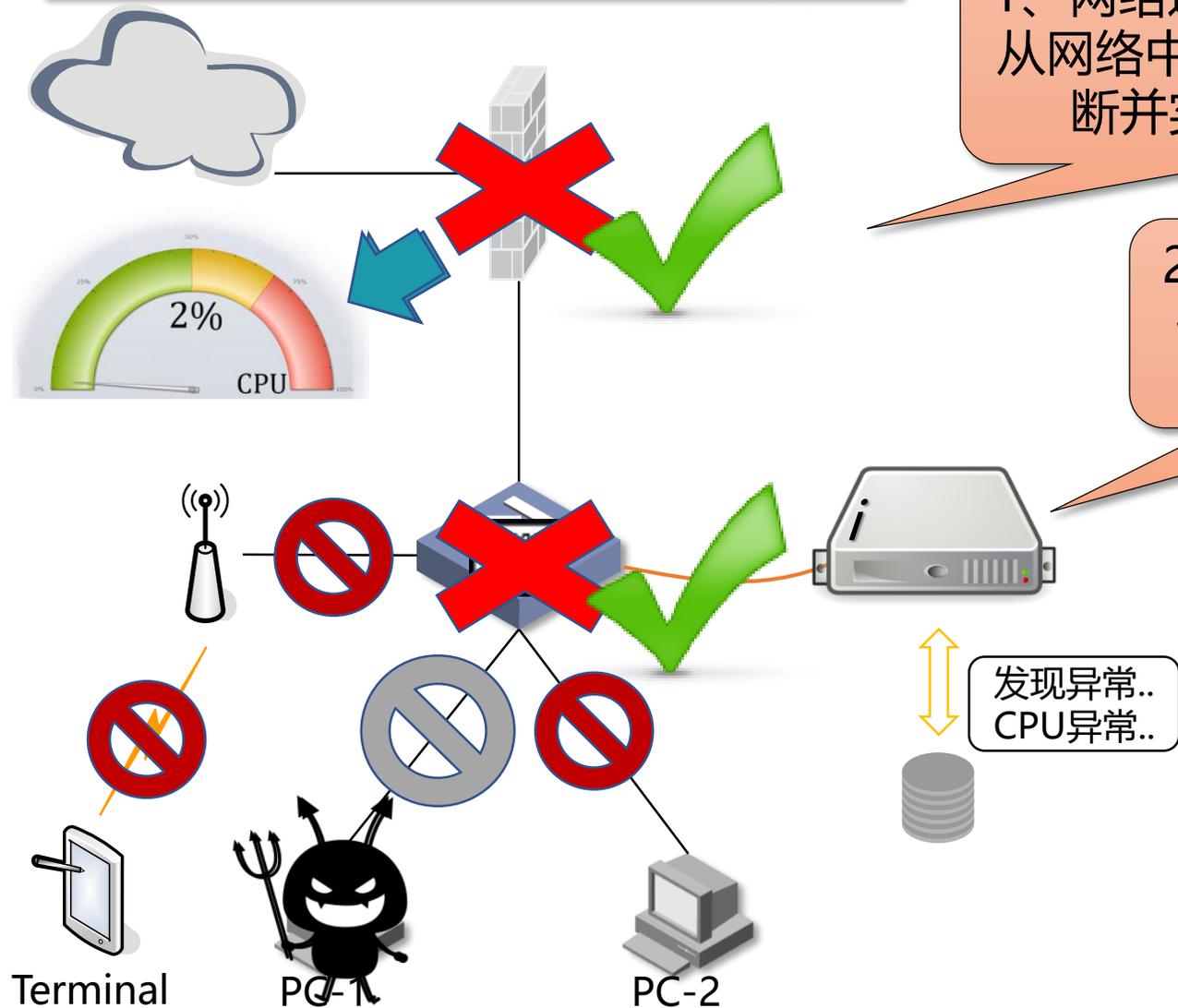
短信报警(限屏蔽成功)

授权模式: 终端授权

工作状态: 开启

- 交换机屏蔽物理端口(SNMP法)
- 交换机屏蔽物理端口(脚本法)
- 交换机屏蔽IP对应MAC地址
- 路由器屏蔽物理端口(SNMP法)
- 路由器屏蔽物理端口(脚本法)
- 路由器屏蔽IP(ARP法) s)
- 定位交换机屏蔽IP对应物理端口 s)
- 定位交换机屏蔽IP对应MAC地址
- ARP阻断IP
- 旁路式限制IP带宽
- 生成报警记录
- 短信报警
- 自定义路由器动作脚本
- 自定义交换机动作脚本
- 自定义其它设备动作脚本

## 5 网络故障自动处理



1、网络运行中，iRecovery从网络中采集数据，分析判断并实时记录数据。

2、网内某用户异常致使网络异常，网内用户无法正常联网。

3、iRecovery发现异常状况，根据用户定义的规则屏蔽该异常用户。

4、处理该故障，网络恢复正常运行。

## 6 地址准入管理

添加IP/MAC审核表的成员可正常使用网络

如未通过IP/MAC审核,可进行限制入网或多种报警提示

IP/MAC地址管理功能,无需网络管理员在原有的网络设备上,进行IP/MAC绑定操作

序号	IP地址	MAC地址	入库时间	状态	组别	备注	采样设备
409	10.5.1.168	8c89.4d4e.4d08	2017-03-22 10:51:19	已核准	办公室	刘刚	10.5.1.1
410	10.5.1.202	f80f.4d4e.4d0c	2017-03-22 10:51:19	已核准	办公室	崔明	10.5.1.1
411	10.5.1.188	d8cb.4d4e.4d3d	2017-03-22 10:51:19	已核准	机要党委	李政	10.5.1.1
412	10.5.1.2	7427.4d4e.4d06	2017-03-23 18:27:31	已核准	办公室	黄建群(临时)	10.5.1.1
413	10.5.1.111	7427.4d4e.4d431	2017-03-23 18:27:44	已核准	办公室	杨少峰(临时)	10.5.1.1
414	10.5.1.112	7427.4d4e.4d4a6	2017-03-23 18:27:54	已核准	办公室	伊德平(临时)	10.5.1.1
415	10.5.1.1	8c89.4d4e.4d91f	2017-03-23 18:28:04	已核准	无限制	孔海	10.5.1.1
416	10.5.1.4	8c89.4d4e.4d653	2017-03-23 18:28:13	已核准	无限制	戴明	10.5.1.1
417	10.5.1.1	d43d.4d4e.4d19	2017-03-23 18:28:21	已核准	无限制	任志	10.5.1.1
418	10.5.1.8	8c89.4d4e.4d6ca	2017-03-23 18:28:30	已核准	服务中心	范	10.5.1.1
419	10.5.1.103	74e6.4d4e.4d44a	2017-03-23 18:28:40	已核准	文印处	付文	10.5.1.1
420	10.5.1.112	74e6.4d4e.4d989	2017-03-23 18:28:49	已核准	文印处	姚宁	10.5.1.1
421	10.5.1.20	5cf9.4d4e.4d53f	2017-03-23 18:28:59	已核准	文印处	曲	10.5.1.1
422	10.5.1.10	c89c.4d4e.4d0c1	2017-03-23 18:29:08	已核准	无限制	盛	10.5.1.1
423	10.5.1.11	c89c.4d4e.4d5b	2017-03-23 18:29:16	已核准	无限制	王	10.5.1.1
424	10.5.1.17	4437.4d4e.4d174	2017-03-23 18:29:25	已核准	无限制	吴	10.5.1.1
425	10.5.1.255	4437.4d4e.4d0ce	2017-03-23 18:29:33	已核准	无限制	官	10.5.1.1
426	10.5.1.3	8c89.4d4e.4d9ab	2017-03-23 18:29:41	已核准	无限制	马	10.5.1.1
427	10.5.1.7	1078.4d4e.4d7d	2017-03-23 18:30:01	已核准	无限制	刘	10.5.1.1
428	10.5.1.78	eca8.4d4e.4d29e	2017-03-23 18:30:01	已核准	无限制	左	10.5.1.1
429	10.5.1.252	4487.4d4e.4d7ca	2017-03-23 18:30:09	已核准	无限制	施	10.5.1.1
430	10.5.1.1	5453.4d4e.4d995	2017-03-23 18:32:04	已核准	电表处	杨	10.5.1.1

## 7 强大的外部接口

支持任何Linux系统下的程序接口

(Java, C, bash/tcl脚本, Linux命令行等)

可快速地实现定制化的功能模块, 以满足用户各种需求。

# iRecovery-特色功能



交互式  
短信排障



远程4G  
带外管理



旁路式  
限带宽



全自动  
拓扑发现

# 交互式短信排障

Help

【4g:拨入4g网络】  
【N4g:挂断4g网络】  
【T:查询T信息】  
【halt:关机】 【Y:恢复短信报警】 【N:24小时内不再接收短信报警】  
【reboot-s:重启自愈软件系统】 【reboot-h:重启自愈硬件系统】  
【down-设备IP地址-设备端口名称:短信关闭设备端口】 【up-设备IP地址-设备商品名称:短信开启设备端口】

09:40  
down-172.31.1.235-fa0/20

09:41

已成功关闭设备172.31.1.235上的端口FA0/20

09:41

up-172.31.1.235-fa0/20

09:41

已成功开启设备172.31.1.235上的端口FA0/20

4月13日 18:54

(B办公网\_10.1.1.1地址规则-5)[IP:10.1.1.8,当前对应MAC:143d.1.1.e756]:IP与MAC绑定审批表中没有该记录

09:40

(cisco\_路由器自愈规则-5)设备192.168.0.1中镜像端口流量流量中IP:192.168.10.100接收包858(pps)大于阈值。可尝试进行以下操作[在<b>所定位的交换机192.168.0.2-[H3C\_交换机]<b>中屏蔽物理端口(目标设备=192.168.0.2;屏蔽标的=Ethernet1-0-1;屏蔽类型=INTERFACE;屏蔽手段=SNMP)].如授权此操作,请回复短信代码278132,或邮件回复\$278132\$,3小时内有效

09:40

278132

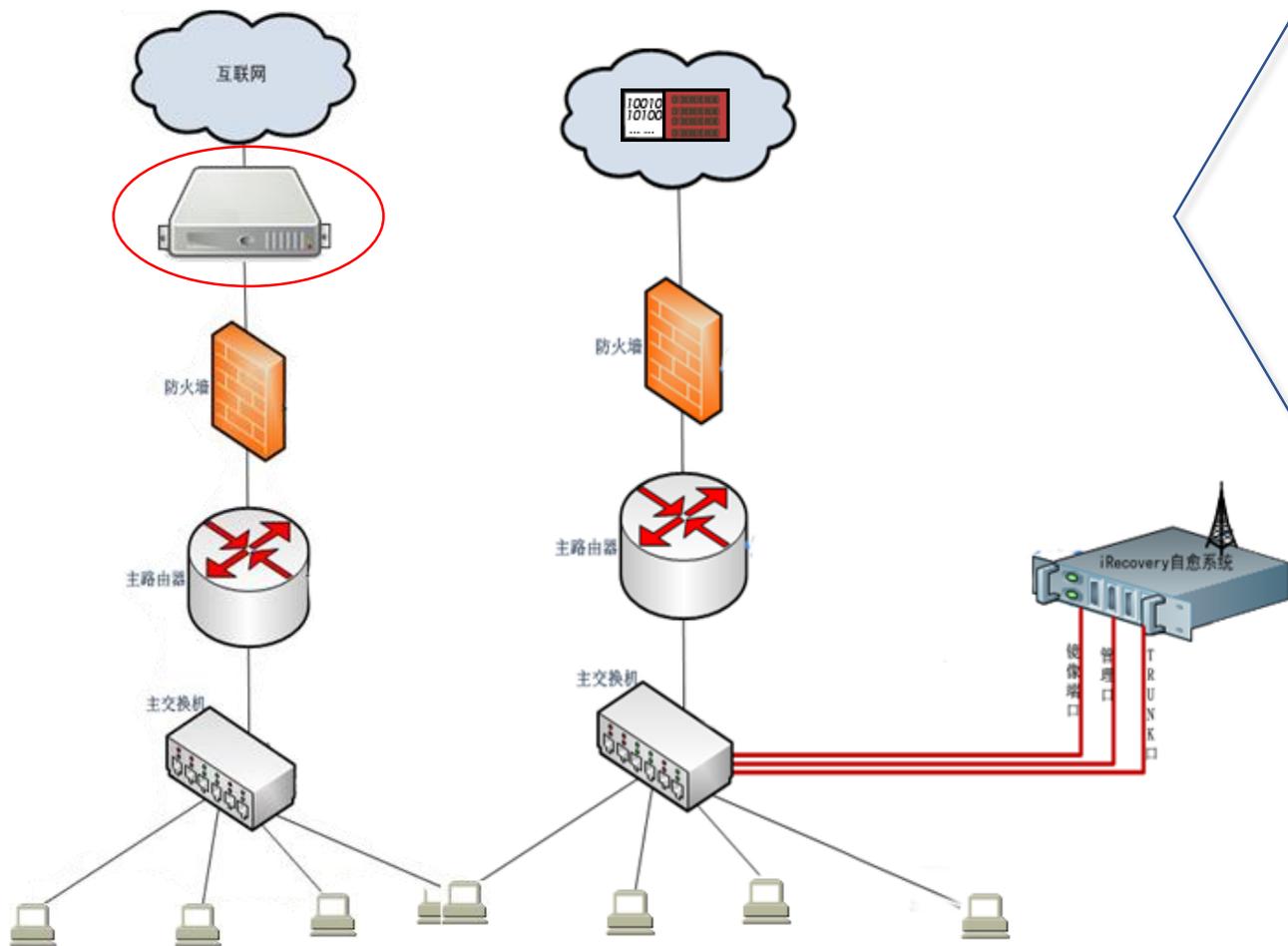
# ▶ 远程4G带外管理



授权管理员通过手机短信激活4G功能，系统即可接入中国移动4G网络。

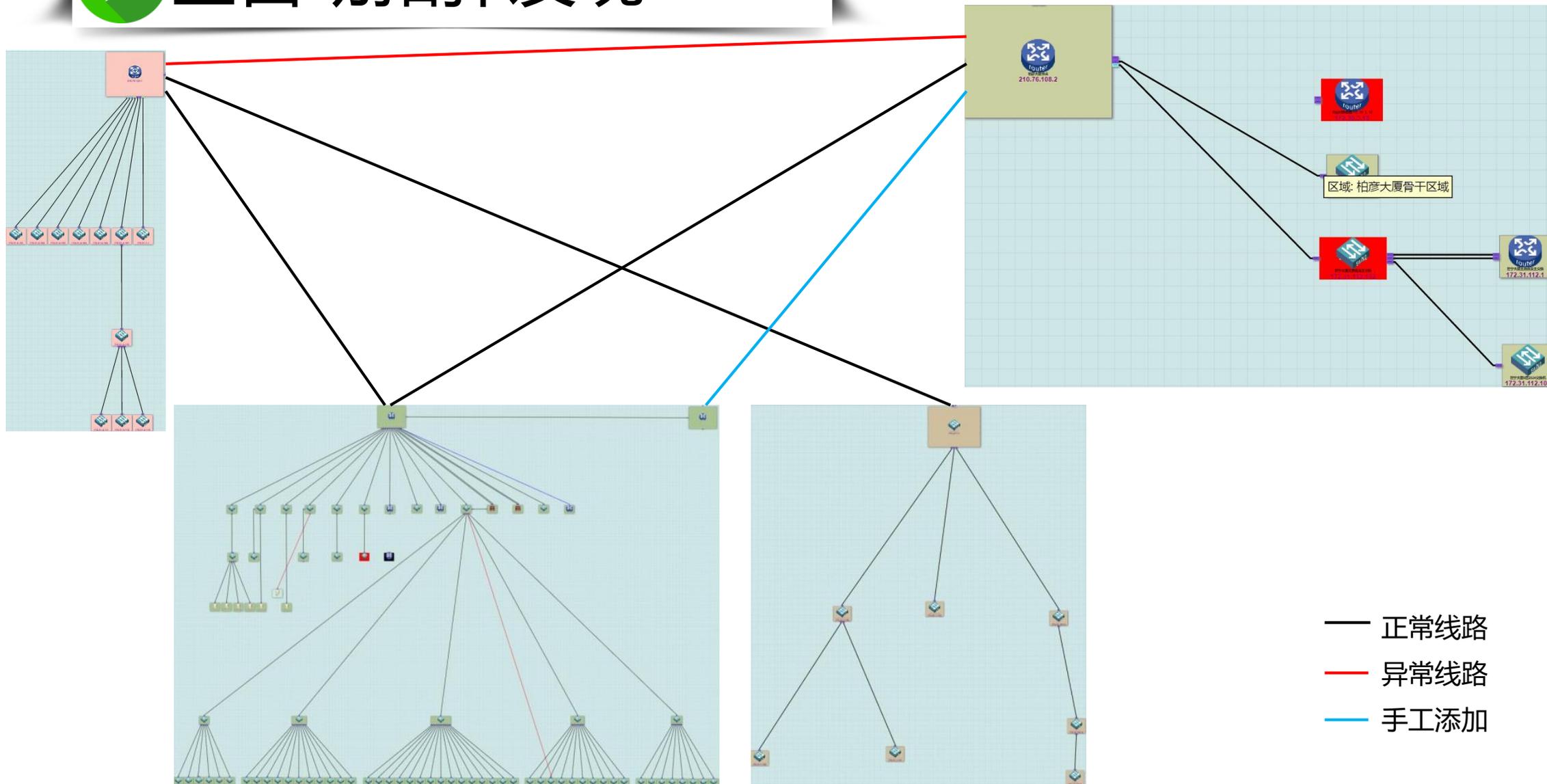
此时可借助其他第三方软件登入系统（如Teamviewer、TightVNC或VPN等），同时可以本系统作为跳板登录（Telnet、SSH或Console方式等）单位内网的设备。

# ▶ 旁路式限带宽



传统的流控设备都是串接。此种方式故障点较多，无论是上联口、下联口或设备出现故障都将影响到网络连接。

# 全自动拓扑发现





**谢谢**

**恒景科技**