紫光集团 核心企业 | H3C 数字化解决方案领导者

H3C资料体系介绍、主网络设备高危操作和常见故障信息收集

2023.8

引入

子曰：“工欲善其事，必先利其器“。

此课程可以帮助大家更好地了解H3C的资料体系建设以及常用工具，可以很好地解决售后工程师在项目开局、优化、维护过程中设备参数或技术资料查找困难，缺少一件称心如意工具等难题。大家处理交换机、路由器、无线、安全、解决方案、云计算、业务软件等产品问题时，都可以参考此课程内容。

此课程针对一线遇到各类主网络故障问题所需要收集的信息进行讲解，减少信息收集环节无谓的损耗，提升问题的处理效率。

H3C常用工具、资料介绍

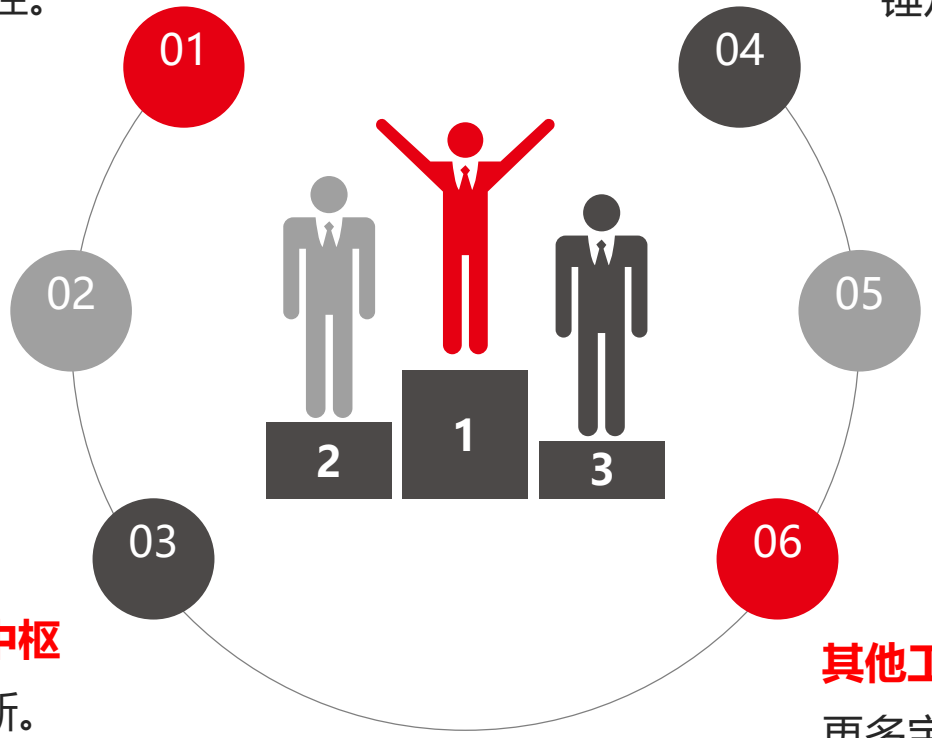
紫光集团 核心企业 | H3C 数字化解决方案领导者

新华三官网

公司最权威途径。

标杆的神器

一锤定音，百宝箱。



知了社区

网络工程师的开放论坛、宝藏社区。

HCL华三云实验室

随时随地搭实验环境，模拟现网故障，快速定位根因。

iService服务数字中枢

智慧巡检、智能诊断。

其他工具及实用资料

更多宝藏等待您的挖掘，也期待各位的分享。

1

PART 01

新华三官网

新华三官网

A、文档中心包含安装（硬件/软件）、配置、命令、维护、技术白皮书等模块，是产品最权威、最系统的资料！

*官网链接：www.h3c.com/cn/

新华三官网

B、**软件下载**：现场开局推荐升级到iservice的推荐版本或者官网最新版本，版本说明书中可以查看当前版本的**版本信息、硬件特性变更、软件特性及命令行变更、操作变更、解决问题列表、升级指导**等。

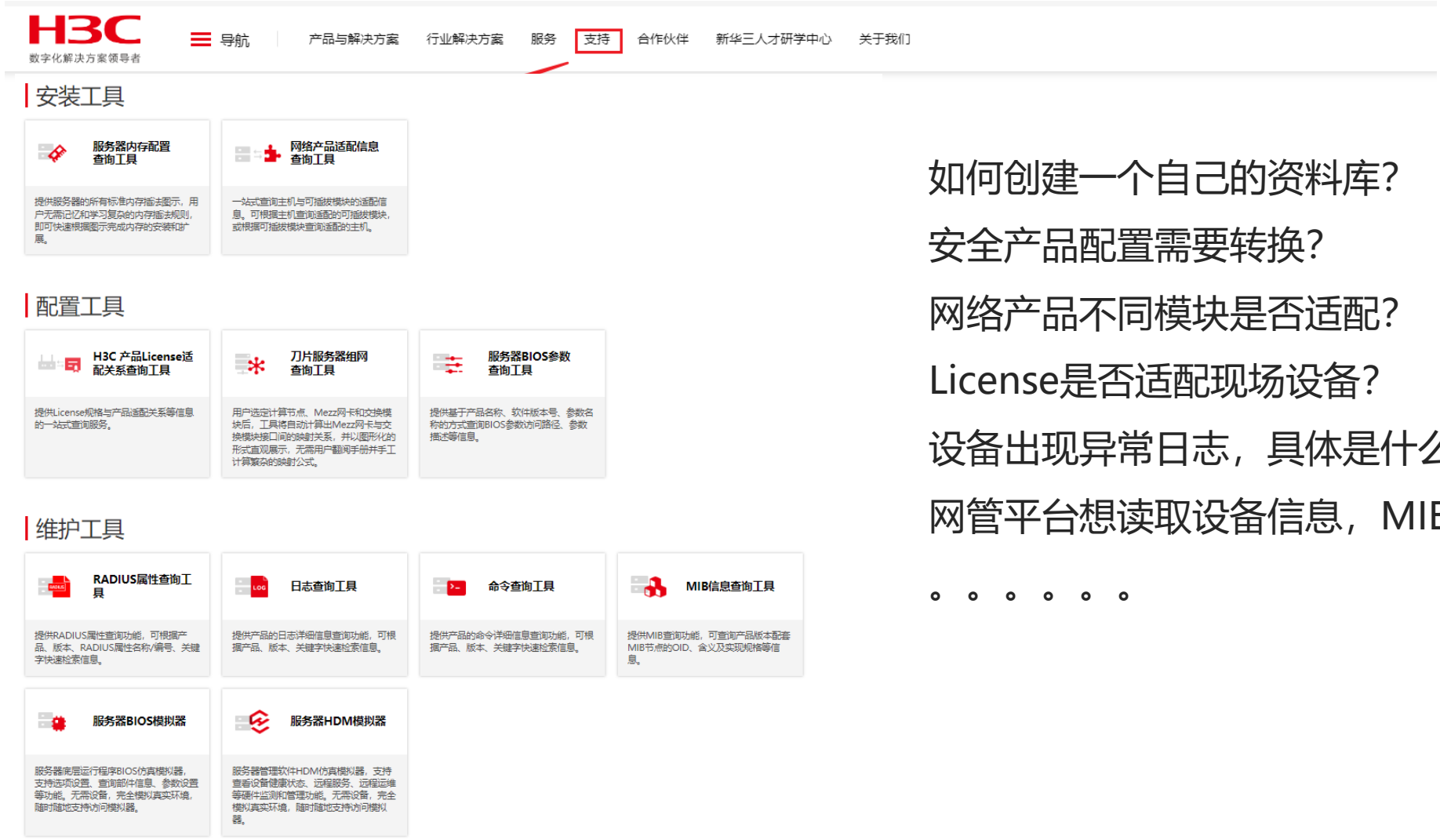
新华三官网

C、H3C官网授权相关业务介绍：自主实现license授权激活、设备授权迁移以及卸载。

若不熟悉授权流程，可以在相应的设备文档资料中找到“license使用指南链接”，里面有详细的授权安装流程（左图以交换机12500X-AF举例）；查看“license支持情况说明”可确认当前设备支持哪些类型授权。

新华三官网

D、**工具专区**：个人资料库、规划设计工具、安装工具、配置工具、维护工具。



如何创建一个自己的资料库？

安全产品配置需要转换？

网络产品不同模块是否适配？

License是否适配现场设备？

设备出现异常日志，具体是什么含义，该如何操作？

网管平台想读取设备信息，MIB信息如何确定？

。。。。。。

2

PART 02

知了社区

知了社区

遇到现网难题时，可先在知了社区快速提问、知识库中搜索解决方法，根叔云图提供排查思路。

想提高个人技能水平，通过资料中心、知了学堂连线大咖，紧跟技术热点。

对设备有新的功能需求或不满，可以在H3C产品改进计划提出相关合理诉求。

zhiliao.h3c.com

知了社区

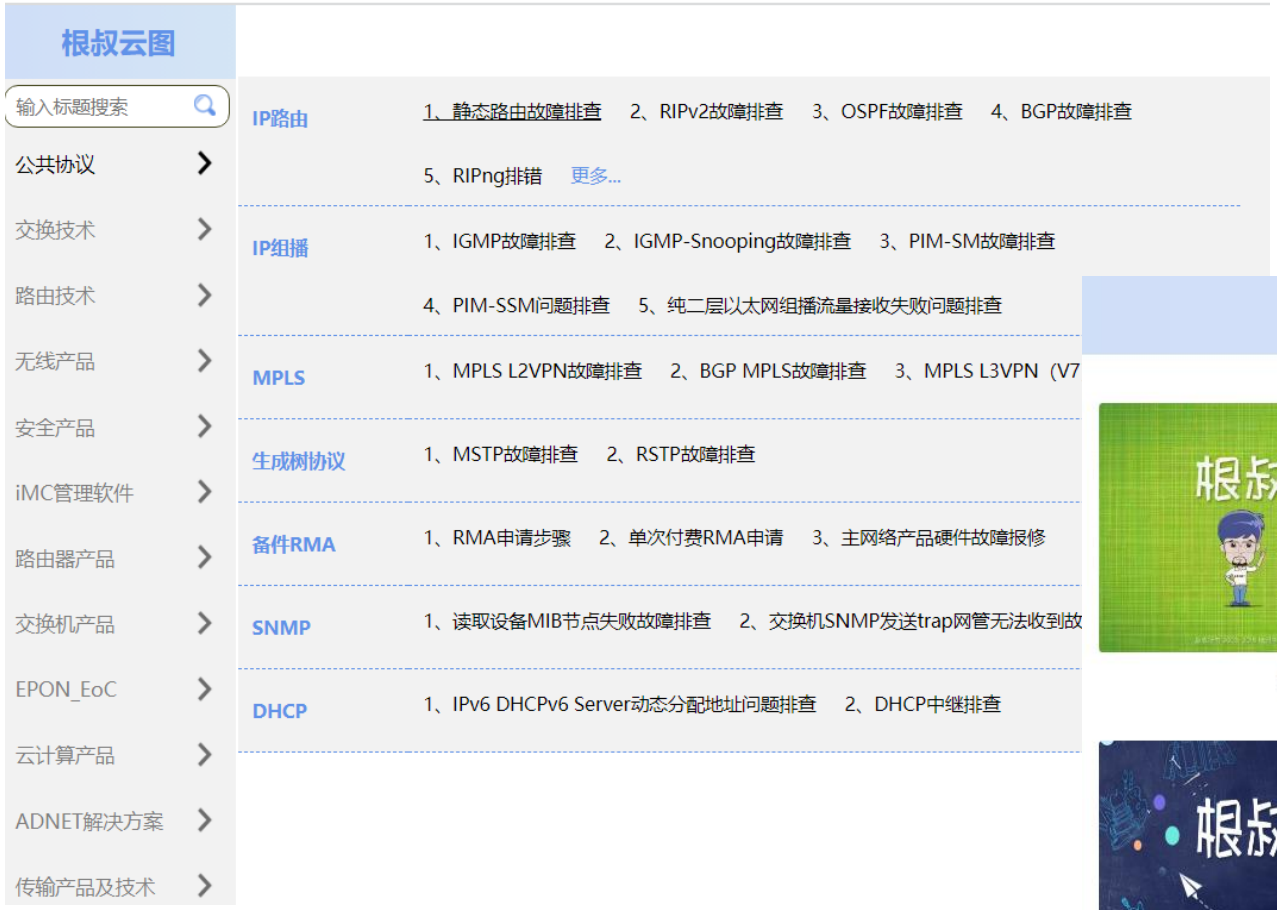
高级搜索定位更准确:

“知识库”---大量工程师踩过坑的经验案例，官网都没有的典型配置，H3C权威发布的技术公告和漏洞说明:

知识库内容均经过原厂二线审核，值得信赖~

知了社区

根叔云图：故障排查图形化，按图索骥觅真知



根叔的种子：短视频传播数字化服务之道

知了社区

技术专题路径：资料中心—产品选择—xx技术专题

- 通过分析渠道问题及当前资料，发现部分资料在特定场景无法满足客户需求，对此梳理常见场景并开发场景化、模块化资料，以解决客户问题
- https://zhiliao.h3c.com/topic/huati/5043

启动规划

- **2021年3月**
- 确定资料以专题形式呈现
- 梳理各产品TOP 5场景模块
- 制定开发计划

推出三期专题

- **2021年Q2-Q4**
- 推出三期共19篇资料专题
- 多渠道推广：通过APP、知了话题广场、渠道管理部、渠道技术交流群推广
- 累计阅读量10000+

持续改进

- **2022年至今**
- 继续分析TOP场景模块，持续推出场景化资料
- 更新老旧资料
- 加强推广，提高阅读量
- 定点推送：筛查问题模块Top10工程师，定点推送资料

3

PART 03

iService服务数字中枢

iService服务数字中枢

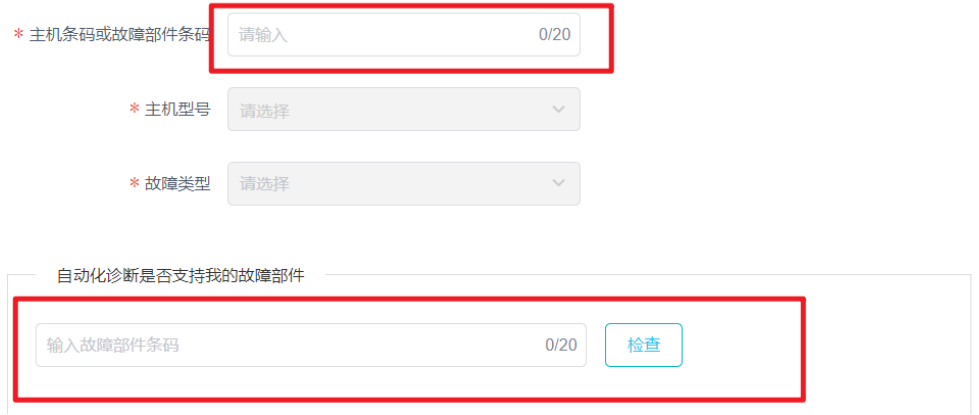
A、iservice硬件自动化诊断工具：部分模块的硬件故障问题可实现自助走备件流程，无需通过400建单

1、首先通过五位工程师账号登录iservice.h3c.com

2、在云端工具中选择硬件自动化诊断工具

3、点击右上角新建，新建工单

4、先根据序列号自主检查设备是否支持自动化诊断，如支持再进行后续流程



iService服务数字中枢

A、iservice硬件自动化诊断工具（举例）

以S6520交换机设备为例，在“自动化诊断是否支持我的部件”检查项中，输入故障件条码，点击检查，查询结果提示：自动化诊断工具已支持该部件。将序列号填入主机条码的方框中选择主机型号，以及故障类型，可知该设备仅支持“交换机无法正常启动”“console无输出或输出异常”“电源”“温度告警”“主机无法上电”“风扇”相关故障类型，其他故障问题仍需通过致电400人工进行故障判断。

支持自动化诊断的硬件故障类型：

- 光模块
- 无线
- 安全
- 路由器
- 交换机
  - console无输出或输出乱码
  - 主机无法上电
  - 交换机无法正常启动
  - 温度告警
  - 电源
  - 风扇
  - POE供电故障
  - 电源（包含主机不上电）
  - 光模块故障

iService服务数字中枢

B、版本推荐工具

推荐版本获取方式：使用五位工程师账号登录iservice.h3c.com→云端工具→版本推荐工具，搜索对应的产品线、产品型号

云端工具 > 版本推荐工具

交换机产品线 | 路由器产品线 | 安全产品线 | 无线产品线 | 业软产品线 | 云与智能产品线 | ADNET | 服务器产品线 | 存储产品线

版本推荐表使用说明：

1、产品版本推荐版本适用于：设备基本特性及传统组网版本使用推荐，如设备涉及新特性如DRNI、特殊特性、方案组网、FOA和重大项目，请与总部单独确认推荐版本；
2、本推荐表推荐版本基本为正式版本，对于特殊局点、特殊组网开局或特性应用测试需要使用受限版本，请单独与总部确认版本；
3、部分产品编码不同使用的版本分支不同，部分编码不能直接升级到新的分支版本，任何版本使用前都需要通过版本说明书确认产品与版本的适配关系；
不同软件版本硬件适配有区别，请注意查看版本说明书确认适配关系和支持版本（如框式设备特定版本后才支持某些单板）
4、部分产品如果现有分支不支持某些功能，需要升级到新分支来支持新特性，请与总部单独确认推荐版本；
5、由于补丁更新频率较版本更新频繁，且部分补丁受限一些局点使用，本推荐表的中补丁仅当前稳定补丁，如FTP中最新补丁与表格不同或特殊局点使用，请与总部确认；绿色为季度补丁，受众面更广；
6、本表格更新周期为每月初进行更新。
推荐表更新时间：2023.02.06

产品组：请选择产品组　产品系列：请输入要查询的产品系列　查询　重置

产品组	产品系列	当前版本	推荐版本	推荐补丁	运营商推荐版本	运营商推荐补丁	官网下载路径	FTP下载路径	版本使用说明
			CMW710-R1005P21	H12	CMW710-R1005P21	H14	S125X:https://www.h3c.com/cn/Service/Document_Software/Software_Download/Switches/Catalog/H3C_S12500/H3C_S12500X/?CHID=173047&v=612	S125X：/New_Internal_Versions(新内部版本归档)/01-IP网络产品/11-数据中心交换机/01.12500-X系列/	适配EA&EB&EC系列业务

iService服务数字中枢

C、通过标杆与iservice进行巡检

1、登录标杆，在设备管理中添加需要巡检的相关设备

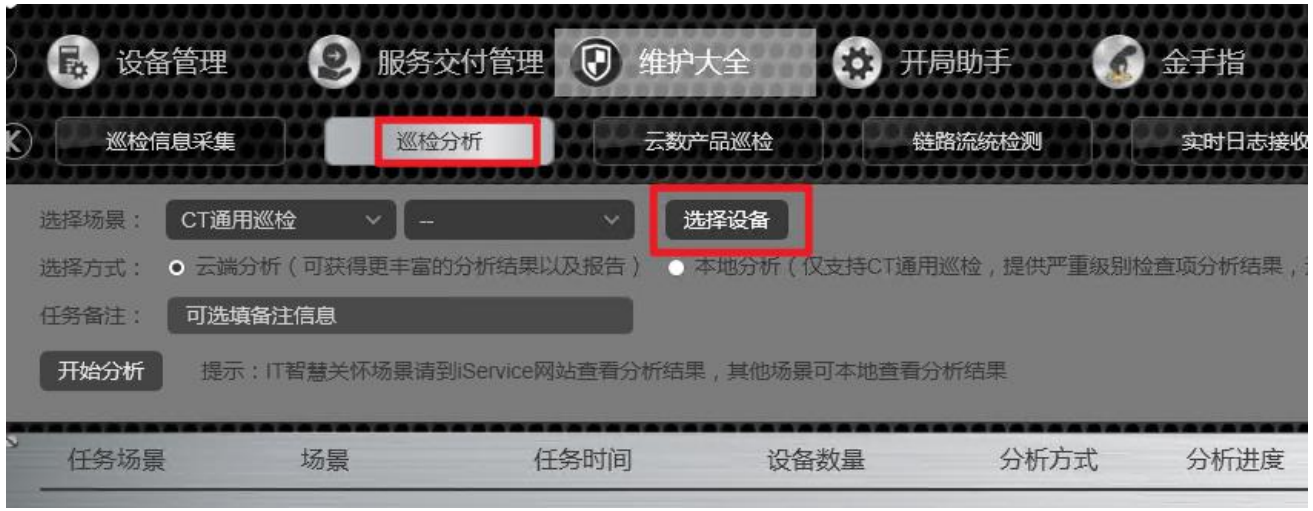
2、维护大全——巡检信息采集——选择设备，选择已添加的设备

选择采集后需填入设备相关局点信息，再次点击采集可选择采集完自动完成分析，也可不选择，后续进行手动分析

iService服务数字中枢

C、通过标杆与iservice进行巡检

3、巡检分析中选择相应的设备，注意必须是已经进行过采集的设备



iService服务数字中枢

C、通过标杆与iservice进行巡检

4、可登录iservice：我的工作台——资料采集上传中查看巡检相关结果

iService服务数字中枢

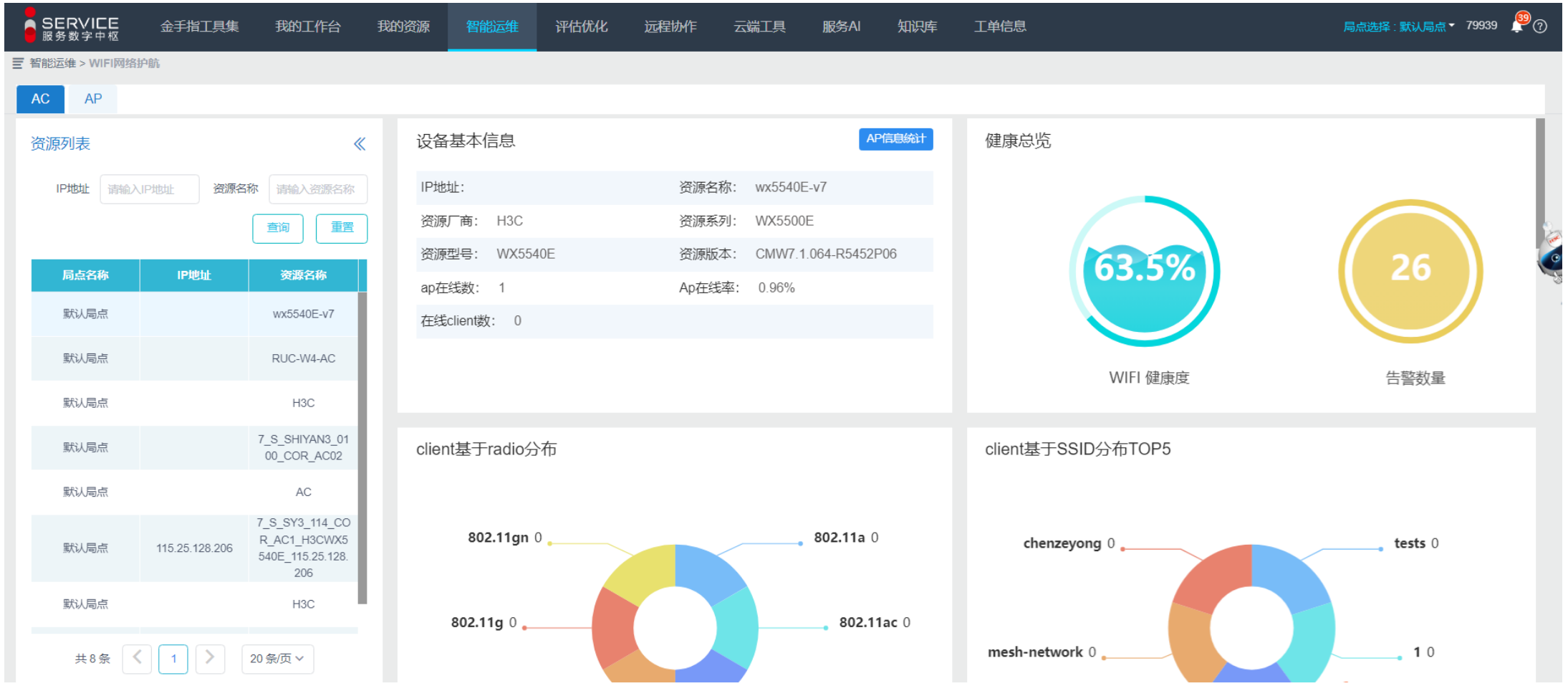
D、云端工具--CT网上问题智能诊断系统

上传设备的诊断信息，平台对设备的告警汇总、硬件、软件、配置、安全、容量、维保进行评估。

iService服务数字中枢

E、智能运维—WIFI网络护航

查看设备基本信息、无线终端分布情况，并根据无线网优规范、日常问题处理经验，按照项目局点对配置进行规范化检查。



iService服务数字中枢

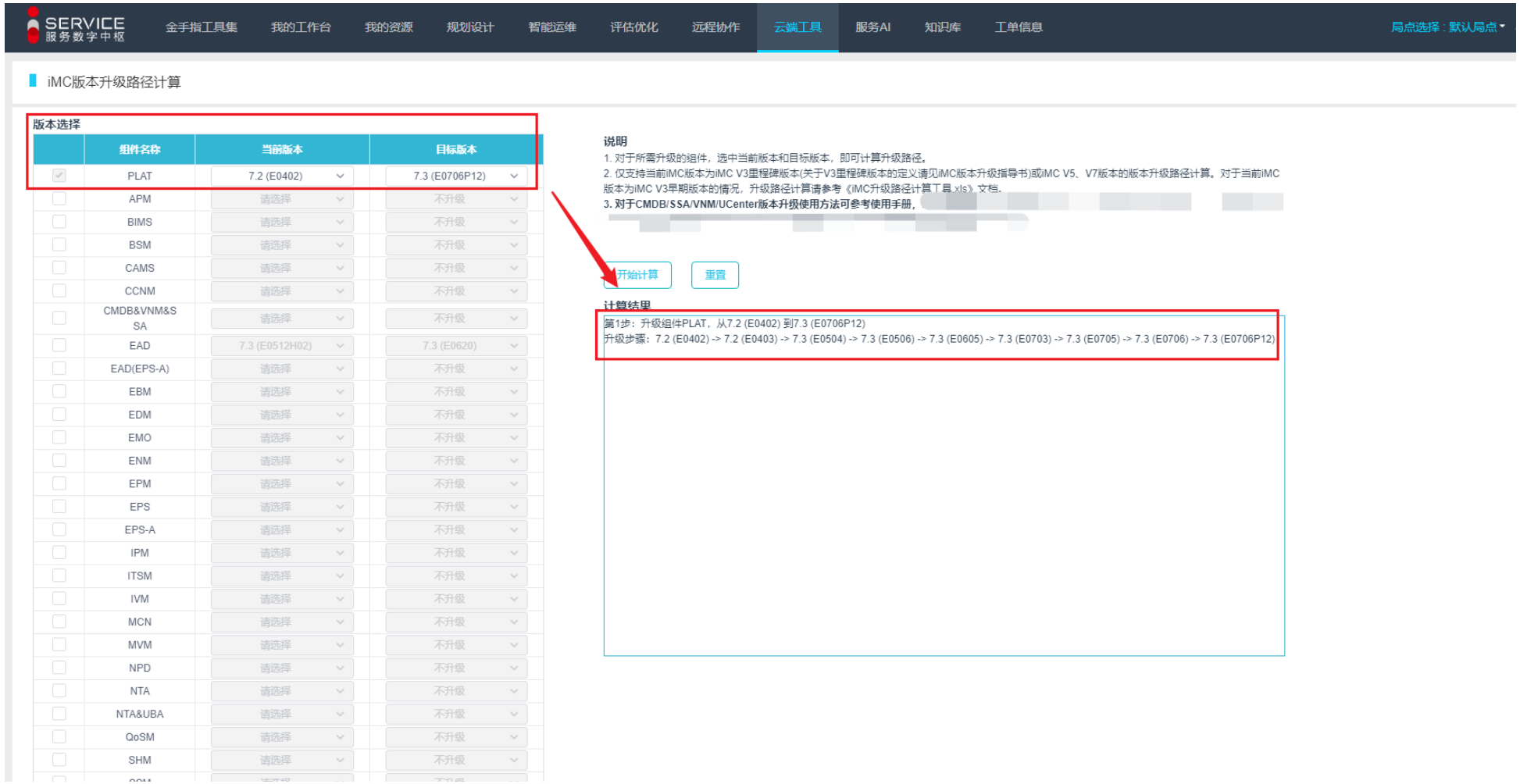
F、云端工具--硬件资源计算

开局安装iMC非常实用，根据业务量给出服务器的硬件资源要求。

iService服务数字中枢

G、云端工具-iMC版本升级路径计算

iMC平台及组件升级路径自动计算，减少自己查询资料流程。



iService服务数字中枢

H、知识库—资料检索

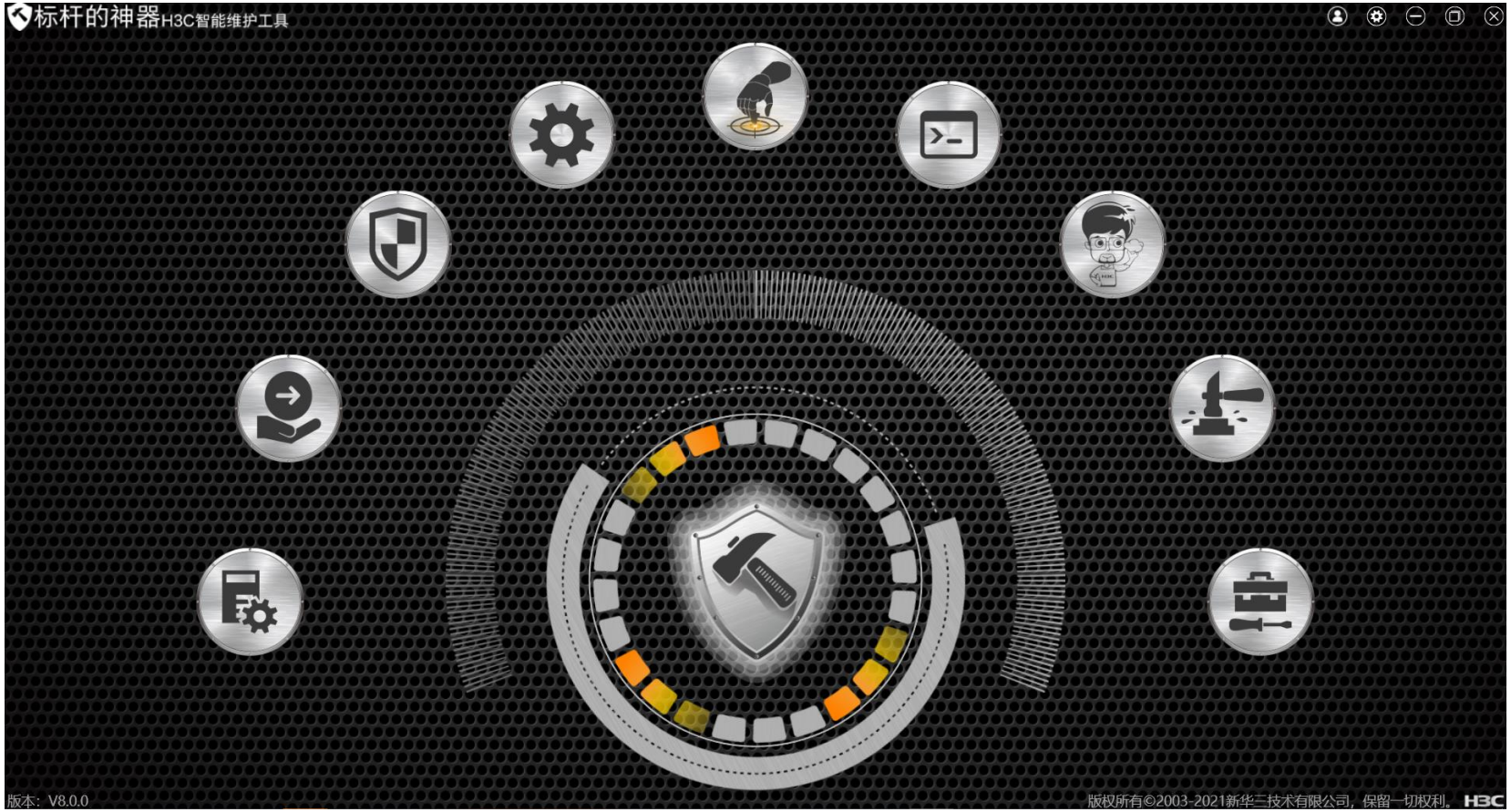
H3C官网+轻松配+知了社区，搜索一网打尽。

4

PART 04

标杆的神器

标杆的神器



维护大全、根叔云图、工具宝箱、开局助手、上岗证、一锤定音...工具多样、功能强大、应有尽有！

标杆的神器

工具宝箱众多智能维护工具!

标杆的神器

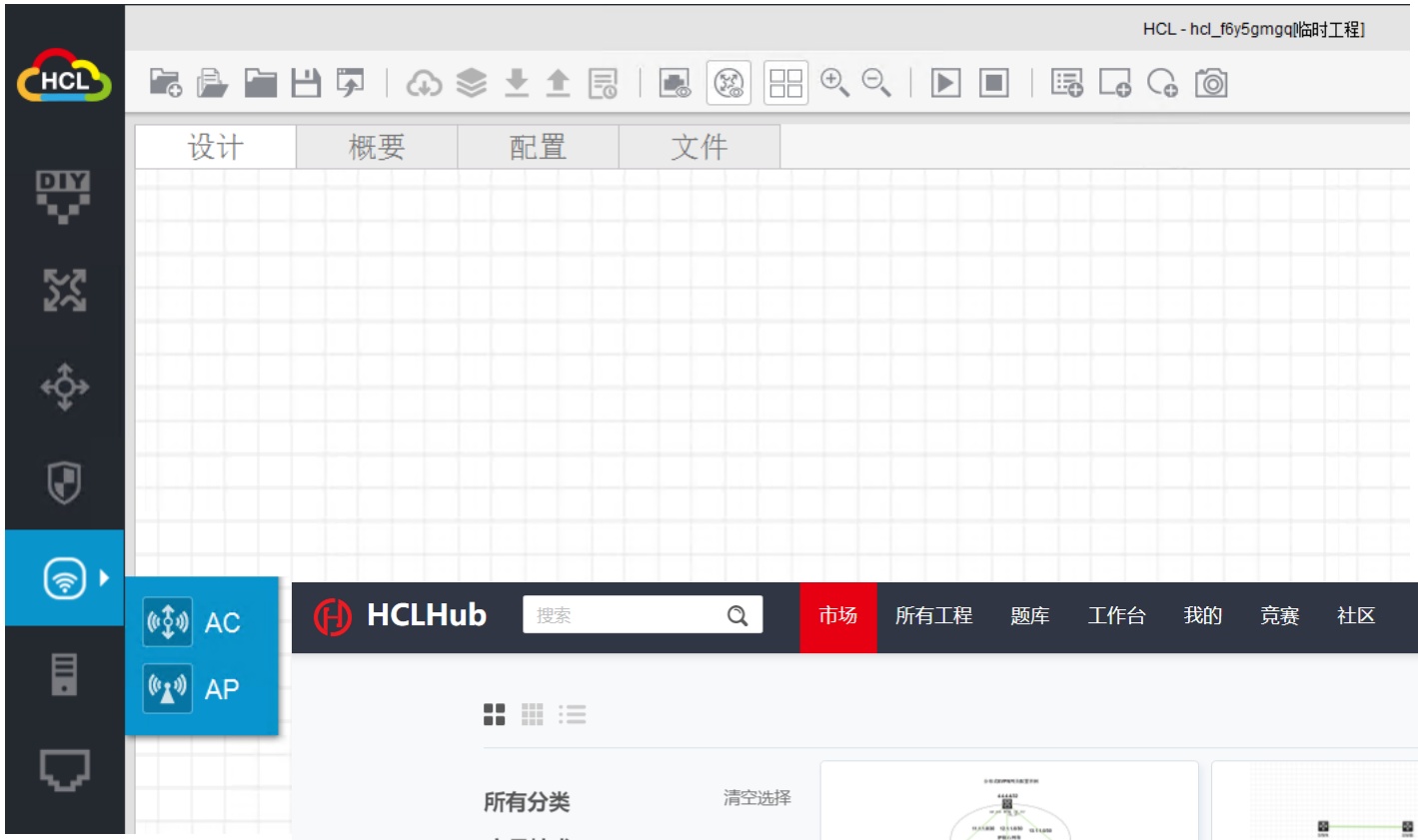
工具宝箱众多智能维护工具!

5

PART 05

HCL华三云实验室

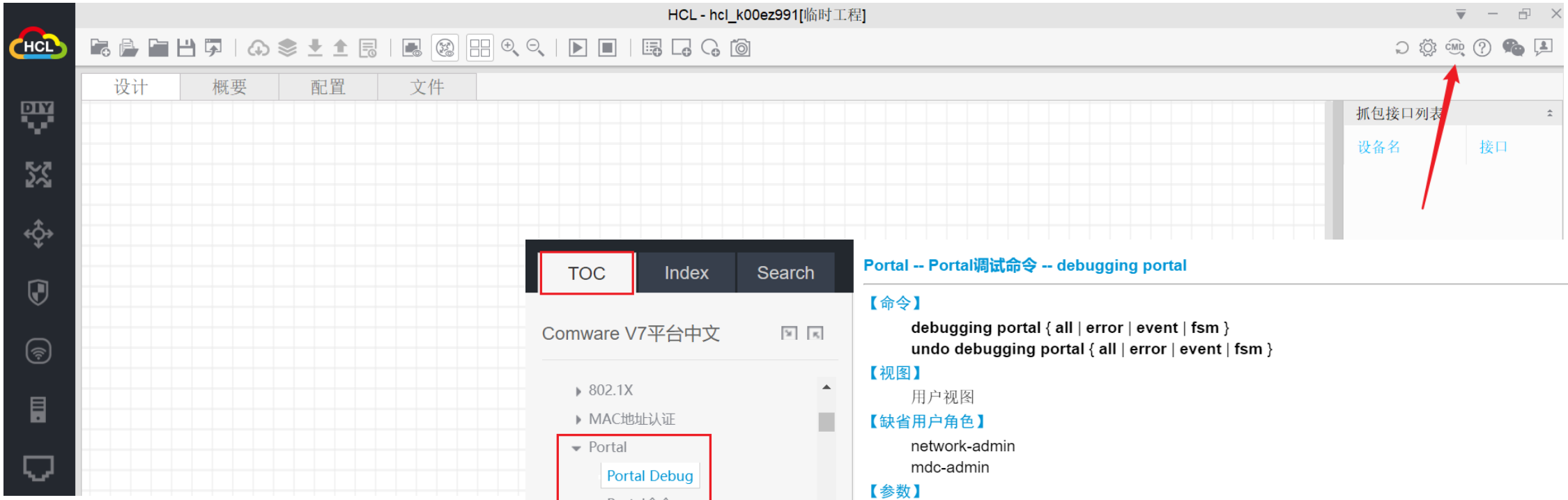
HCL华三云实验室



可模拟**路由器、交换机、防火墙、无线**等网络设备的基础功能，助您轻松搭建虚拟网络环境，完成配置、测试、调试等功能。

http://hclhub.h3c.com/提供海量工程文件。

HCL华三云实验室



CMD这个隐秘模块帮助你了解各种协议的具体报文交互过程。

Portal -- Portal调试命令 -- debugging portal

【命令】

debugging portal { **all** | **error** | **event** | **fsm** }
undo debugging portal { **all** | **error** | **event** | **fsm** }

【视图】

用户视图

【缺省用户角色】

network-admin
mdc-admin

【参数】

all：表示所有Portal调试信息开关。
error：表示错误调试信息开关。
event：表示事件调试信息开关。
fsm：表示状态机调试信息开关。

【描述】

debugging portal命令用来打开Portal调试信息开关。**undo debugging portal**命令用来关闭Portal调试信息开关缺省情况下，Portal调试信息开关处于关闭状态。

表1-1 debugging portal error命令输出信息描述表

字段	描述
Failed to create the detection timer for portal server *server-name*.	创建Portal服务器探测定时器失败，Portal服务器名称为*server-name*
User (IP:*user-ip*) will log off because of no IP address	由于未能成功被DHCP服务器分配IP地址，用户将被

6

PART 06

其他工具及实用资料

新华三大讲堂（learning.h3c.com）

包括**课程、专题&项目、知识城邦、我的学习、圈子**等模块。不定期推出新产品、新技术等相关知识。

新华三服务APP介绍

新华三服务APP是一款针对星级渠道工程师的软件工具集。工程师不仅可以快速获取技术支持、高效处理技术问题，还可以第一时间获取厂商服务信息。

下载链接：https://www.h3c.com/cn/Service/Online_Help/H3CService/

一键接入400

直接扫描条码，飞速接入400合作伙伴专线，帮助您及时解决各类技术难题。

问题单查询

查询您的所有问题单，如有需求可直接点击进入对应专家座席继续交流咨询。

维保信息查询、服务业务指南、产品手册、常用案例、典型配置、技术公告、渠道大讲堂、根叔的种子...更多功能等你体验！

新华三服务公众号

关注“新华三服务”公众号，可以实现400一键接入、在线提单、维保查询等自助服务，可以查看轻松开局、技术专题、案例库等资料和最新服务动态。

跟吉吉学路由

交换那些事

冬冬说无线

业软“祺”谈

。。。

实用资料

1. 无线产品一本通--V7和V9通用版本
https://www.h3c.com/cn/Service/Document_Software/Document_Center/Home/Wlan/00-Public/Doc_Sets/Doc_Packages/H3C_V7_OneNote/01/?CHID=846476

2. 星级渠道重大项目交维检查操作指导
https://zhiliao.h3c.com/TechDoc/details/981

第二章-主网络设备高危操作

1

PART 01

主网络产品高危操作手册

交换机

登录官网（www.h3c.com）
路径：首页--支持--文档中心—交换机：选择对应型号交换机，搜索“高危操作手册”

H3C交换机高危操作手册(Comware V7)-6W100

路由器

登录官网（www.h3c.com）
路径：首页--支持--文档中心—路由器：选择对应型号路由器，搜索“高危操作手册”

H3C 中低端路由器 高危操作手册(V7)-6W100

H3C 高端路由器 高危操作手册-6W101

无线控制器

登录官网（www.h3c.com）
路径：首页--支持--文档中心—无线：选择对应型号无线控制器，搜索“高危操作手册”

H3C无线局域网产品高危操作手册-6W100

安全产品

登录官网（www.h3c.com）
路径：首页--支持--文档中心—安全：选择对应型号安全产品，搜索“高危操作手册”

H3C 安全产品 高危操作手册(V7)-6W103

主机硬件高危操作

操作大类	操作小类	误操作可能引起的后果
整机类操作	严禁随意按下设备上的Reset按钮。	当按下设备上的Reset按钮时，设备将被强行执行硬件复位，该操作仅能由有资质的维护人员在系统出现严重故障的情况下执行。
	严禁堵塞设备入风口、出风口等风道。	可能因为风道堵塞导致设备散热不良，设备有烧毁风险。
	基于X86架构的设备，严谨直接拔出、直接断电。	有系统崩溃风险。
单板类操作	严禁在不戴防静电腕带的情况下拔插单板。	人体静电对单板上的电子器件具有很大的危害，维护人员在不戴防静电腕带的情况下拔插单板，很容易使单板遭受静电危害，从而损坏单板或使单板运行不稳定。
	取拿单板时，严禁用手直接接触单板元器件和印制电路板。	使单板遭受静电危害，从而损坏单板或使单板运行不稳定。
	存放单板时，请使用防静电屏蔽袋，请勿将其随意搁置。	使单板遭受静电危害，从而损坏单板或使单板运行不稳定。
	单板软件加载下载过程中，禁止掉电或热插拔单板	损坏单板。
电源类操作	更换电源模块前，需先将待更换电源模块的断路器断开。	可能损坏设备或造成人身伤害。
	严禁随意操作机柜配电框内的电源开关。	只有在升级、扩容、更换部件或系统发生重大故障的情况下，维护人员才能按照操作规程操作各类电源开关，随意操作电源开关将导致设备停止运行、业务中断等重大事故。
光模块操作	严禁在工作状态操作光纤时，用眼睛直视光模块的光发射口和与其相连的光纤连接器的光纤出口。 严禁在拆卸光模块的过程中，用手直接触摸模块的金手指部分。	光接口发出的激光束具有很高的能量，直视或使用非衰减的光学仪器直接查看光纤内部的激光束，会伤害眼睛。 损坏光模块。
线缆类操作	严禁随意拔插机柜内部的网线。 请使用设备随机提供的保护地线连接交换机到机房的接地排。	机柜内部的网线连接主要用于实现主机与维护终端之间的通信等功能，随意拔插网线将可能导致维护终端无法登录路由器等。 其他保护地线不能保证接地效果，容易导致交换机损坏。

硬件高危操作（续）

无线接入点硬件高危操作

操作大类	操作小类	误操作可能引起的后果
安装类	天花板不能为金属材质。	会对射频信号产生干扰。
	面板设备在安装时需要在周围预留一定的通风散热空间。	否则可能会导致设备过热。
	无线终结者电口不建议直接接终端设备。	可能会导致终端设备网口烧坏。
	无线终结单元不能使用普通PoE交换机供电。	普通PoE交换机需要PD检测才能上电，无线终结单元无法正常供电，如果PoE交换机配置了强制供电，则会损坏终结单元设备。
光模块操作	严禁在工作状态操作光纤时，用眼睛直视光模块的光发射口和与其相连的光纤连接器的光纤出口。	光接口发出的激光束具有很高的能量，直视或使用非衰减的光学仪器直接查看光纤内部的激光束，会伤害眼睛。
线缆操作	室外设备在安装后必须将未使用的接口做防水。	虽然设备接口做了一定的防水，但是室外恶劣环境会造成接口防水老化脆弱，需要使用专业防水材料加强保护。
	不使用的外置天线接口需要安装射频负载。	未安装射频负载可能会产生射频信号干扰。
	室外设备在连接射频接口或者以太口后需要做防水。	设备接口本身不防水，如果没有做防水会导致设备进水损坏。
	室外设备必须可靠接地，消除静电感应。	设备未接地可能会导致设备被雷击损坏。
	室外设备的射频口在连接射频线缆时需要安装防雷器，并将设备可靠接地。	没有安装防雷器可能会导致设备被雷击损坏。
电源类操作	电源适配器或PoE供电需满足设备最大功率的要求。	如不能满足设备最大功率会导致设备不能满载运行。

命令行高危操作

模块	命令行	描述	高危提示
登录设备	**authentication-mode**	设置用户登录设备时的认证方式	当认证方式设置为none时，用户不需要输入用户名和密码，就可以使用该用户线登录设备，存在安全隐患，请谨慎配置。 如果设置认证方式为password或scheme，但是没有配置认证密码或者认证用户，会影响下次登录设备 。
FTP和TFTP	**delete**	彻底删除FTP服务器上的文件	执行本命令前，请确认指定文件不会再被使用，以免误删有用文件。
FTP和TFTP	**rmdir**	彻底删除FTP服务器上的目录	执行本命令前，请确认指定目录不会再被使用，以免误删有用目录。
文件系统管理	**delete** [**/unreserved**] *file*	删除设备上的文件	**delete /unreserved** *file*命令用来永久删除文件，系统会将该文件从设备上彻底删除。被删除的文件不再存在，不能恢复。
文件系统管理	**format**	格式化文件系统	格式化操作将导致文件系统中的所有文件丢失，并且不可恢复；尤其需要注意的是，如果文件系统中有启动配置文件，格式化该文件系统，将丢失启动配置文件。
文件系统管理	**reset recycle-bin**	清除回收站中的文件	回收站中的文件可以通过**undelete**命令恢复，如果将文件从回收站中删除，将永远无法恢复文件。执行本命令前，请确认回收站的文件都是无效文件，不会再被使用。
文件系统管理	**rmdir**	删除设备上的文件夹	在删除文件夹前，必须先永久删除或者暂时删除文件夹中的所有文件和子文件夹。如果文件只是暂时删除，那么执行rmdir会导致这些文件从回收站中彻底删除。执行本操作前，请先确认该文件夹及其中的内容不会再被使用。

命令行高危操作（续）

模块	命令行	描述	高危提示
配置文件管理	**configuration replace file**	执行配置回滚操作。	配置回滚是在不重启设备的情况下，将当前的配置回退到指定配置文件中的配置状态，回滚前的配置将会丢失。配置回滚过程中，可能会导致业务中断，请谨慎使用。
配置文件管理	**reset saved-configuration**	删除设备存储介质中保存的下次启动配置文件	执行该命令会将配置文件彻底删除，请谨慎使用。
设备管理	**clock datetime**	配置设备的系统时间	执行本命令会修改设备的系统时间，会影响和系统时间相关特性的执行（例如定时执行任务功能），以及和其他设备的协同操作（例如日志上报和统计），请谨慎执行。
设备管理	**reboot**	重启设备	重新启动可能会导致业务中断，请谨慎使用。 使用force参数时，系统在重启时不会做任何保护性措施。重启后，可能导致文件系统损坏，请谨慎使用该参数。建议在系统故障或无法正常重启时，才使用该参数。
设备管理	**restore factory-default**	将设备恢复到出厂状态	使用本命令会将设备恢复到出厂状态，请谨慎使用。
IRF	**undo port group interface**	来取消IRF端口和IRF物理端口的绑定关系	配置本命令后，会导致设备从IRF中分离，影响设备和IRF的流量转发，请谨慎使用。
IRF	**irf mac-address persistent**	配置IRF的桥MAC地址的保留时间	桥MAC变化可能导致流量短时间中断，请谨慎配置。
IRF	**irf member renumber**	配置设备的成员编号	在IRF中以设备编号标志设备，配置IRF端口和优先级也是根据设备编号来配置的，所以，修改设备成员编号可能导致设备配置发生变化或者丢失，请慎重处理。
IRF	**undo irf member stack enable**	关闭指定设备的IRF功能	关闭设备的IRF功能后，会将指定成员设备从IRF中隔离出来。
接口公共配置	**default**	恢复当前接口的缺省配置	接口下的某些配置恢复到缺省情况后，会对设备上当前运行的业务产生影响。建议您在执行该命令前，完全了解其对网络产生的影响。
接口公共配置	**shutdown**	关闭接口	执行本命令会导致使用该接口建立的链路中断，不能通信，请谨慎使用

命令行高危操作（续）

模块	命令行	描述	高危提示
以太网接口	**port link-mode**	切换以太网接口的工作模式	接口模式切换后，除了**shutdown**和**combo enable**命令，该以太网接口下的其它所有命令都将恢复到新模式下的缺省情况。
ARP	**reset arp**	清除ARP表项	执行本命令会清除设备上已有的ARP表项，可能会导致外部流量无法及时发给局域网中的用户。
DHCP	**dhcp snooping deny**	开启DHCP Snooping报文阻断功能	在接口上开启本功能后，DHCP Snooping会上丢弃该接口收到的所有DHCP请求方向报文，这会使连接该接口的DHCP客户端无法申请到IP地址。所以，本功能只能在不存在DHCP客户端的接口上开启。
静态路由	**delete static-routes all**	删除所有静态路由	删除全部静态路由可能导致网络不通，报文转发失败，请谨慎使用。
ARP攻击防御	**arp scan**	开启ARP自动扫描功能	扫描操作可能比较耗时，且会占用较大的设备资源和网络负载。可以通过<Ctrl_C>来终止扫描（在终止扫描时，对于已经收到的邻居应答，会建立该邻居的动态ARP表项）。
Portal	**portal authorization strict-checking**	开启Portal授权信息的严格检查模式	接口或者无线服务模板上开启Portal授权信息的严格检查模式后，当服务器给用户下发的授权ACL、User Profile在设备上不存在或者设备下发ACL、User Profile失败时，设备将强制该用户下线。 可同时开启对授权ACL和授权User Profile的严格检查模式。若同时开启了对授权ACL和对授权User Profile的严格检查模式，则只要其中任意一个授权属性未通过严格授权检查，则用户就会下线。
Portal	**portal user-dhcp-only**	开启仅允许通过DHCP方式获取IP地址的客户端上线的功能	配置本命令后，配置静态IP地址的Portal认证用户不能上线。 在AC+Fit AP组网中，仅当AC作DHCP服务器时，本命令才生效。 在IPv6网络中，配置本命令后，无线客户端仍会使用临时IPv6地址进行Portal认证，从而导致认证失败，所以必须关闭临时IPv6地址。

命令行高危操作（续）

模块	命令行	描述	高危提示
SSH	**ssh server port**	配置SSH服务的端口号	如果修改端口号前SSH服务是开启的，则修改端口号后系统会自动重启SSH服务，正在访问的用户将被断开，用户需要重新建立SSH连接后才可以继续访问。 如果使用1～1024之间的知名端口号，有可能会导致其他服务启动失败。
AP管理	**undo wlan detect-anomaly enable**	关闭重启业务异常AC功能	关闭该功能，设备在发生业务异常时无法通过自动重启立即恢复，只能通过手动重启设备进行恢复。因此，如无特殊需要，请不要关闭该功能。
AP管理	**undo wlan enable**	关闭WLAN功能	请在确定不需要WLAN相关功能后再关闭WLAN功能。 关闭无线功能，会导致当前上线AP全部掉线，请谨慎使用。
应用层检测引擎	**inspect bypass**	关闭应用层检测引擎功能	关闭应用层检测引擎功能后，系统将不会对接收到的报文进行DPI深度安全处理。可能导致其他基于DPI功能的业务出现中断。例如，安全策略无法对应用进行访问控制、七层负载均衡业务无法基于应用进行负载分担等。
应用层检测引擎	**inspect activate**	激活DPI各业务模块的策略和规则配置	执行此命令会暂时中断DPI业务的处理，可能导致其他基于DPI功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制、七层负载均衡业务无法基于应用进行负载分担等。

2

PART 02

高危操作举例

防火墙高危操作

1 **任意视图下执行undo security-policy ip**

工程师小A在设备上创建了一个安全域名字叫ip，想执行操作将这个安全域删除，于是他在系统模式下执行undo sec ip，直接删除了全部的安全策略，导致全网中断。

[FW]undo security-policy ip

注意

1. 命令不要缩写。
2. 升级版本，新版本增加了提示

[FW]undo security-policy ip

This command will delete all rules from the current policy. Continue anyway? [Y/N]:

防火墙高危操作

紫光集团 核心企业 | H3C 数字化解决方案领导者

2 **执行undo acl basic/advanced xxxx**

工程师小B在设备上创建了一个抓包用的acl，抓包完成之后执行删除的时候，一时手抖删错了，删除了包过滤策略中正在使用的acl，恰好现场使用了唯一一条包过滤策略，调用了这个acl，导致现场网络中断20分钟。

[FW]undo acl basic/advanced xxxx

注意

1. 删除ACL之前确认这个acl是否正在被使用。
2. 已有需求跟踪，建议研发增加二次提醒。

防火墙高危操作

3 使用域间策略的情况下，没有配置security-policy disable

客户升级F5000-C版本之后，没有进行策略转换，依然使用的是域间策略（包括对象策略和包过滤策略），设备上也没有关闭安全策略，在点开web界面新建了一个策略后网络中断，因为安全策略优先级较高，新版本web界面新增的就是安全策略，导致域间策略放通的业务全部中断。

注意

1. 建议全部使用安全策略，已发布相关技术公告建议全网使用安全策略。
2. 现场使用包过滤策略或者对象策略且一时半会无法变更时，建议通过security-policy disable命令关闭安全策略。

防火墙高危操作

4 在已有安全策略的rule下面增加service

某运维人员，想单独只放通某些地址一个端口的业务，其直接在已有的安全策略中增加了一个service，结果导致这条策略放通的其他端口的业务中断。这是因为单独在某一条策略中放通某个service相当于收紧了策略的端口，需要谨慎操作。

注意

1. 建议尽量不对已存在的策略进行操作，可以新建一条明细策略放通具体端口。
2. 已有需求跟踪，建议增加service时进行二次提示。

防火墙高危操作

5 攻击防范阈值调低

攻击防范策略用于检测某个安全域过来的流量是否有异常，设备上有缺省的flood攻击阈值，如果现场的业务特殊，或者人为将攻击阈值调低之后，可能会导致正常交互报文被攻击防范模块丢弃，从而业务受影响。

注意

1. 不建议轻易调低攻击防范阈值，根据业务情况调整阈值。
2. 低版本缺省阈值为1000，建议升级，缺省阈值有优化。

高危操作--debug

6 使用完debugging之后不关闭

工程师小D，远程定位客户问题时，新建了一个acl 3090，并开启debugging ip packet acl 3090，定位结束之后，没有及时关闭debugging并删除新建的acl，两周之后，客户做测试时在acl 3090中配置了rule permit ip，配完后现场业务出现异常，部分单核出现告警，关闭debugging之后业务恢复正常。

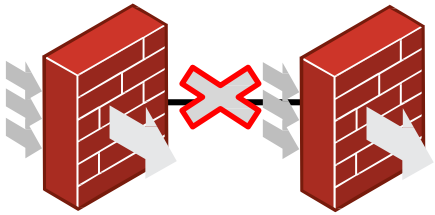
注意

1. 升级设备版本，新版本每一次退出命令行时，会自动执行一次undo debugging all。
2. 定期使用金手指进行巡检，巡检工具检查项当中可以检查到debugging开关是否打开。
3. 养成良好习惯，每次在给客户定位完问题之后，需及时删除增加的定位配置，并关闭debugging开关。

高危操作--拆堆叠配置保存

7 **拆堆叠状态下保存配置**

Comware V7平台防火墙堆叠部署情况下，部分客户会要求尽可能减少业务中断时间，此时运维人员就会选择拆堆叠升级，在拆堆叠升级过程中，有一个风险点需要注意，拆堆叠状态下 如 果 执行了配置保存，此时，slot1会丢失slot2相关的配置，同理slot2也会丢失slot1相关配置。



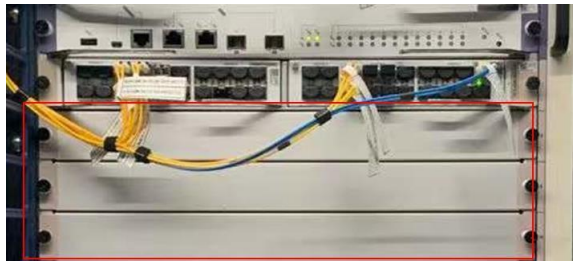
注意

1. 在拆堆叠的情况下一定不要执行save命令进行配置保存。

高危操作—未安装假面板

8 **高端安全产品空槽位未安装假面板**

高端产品安装过程中，若现场不是满插，且运维人员忘记在空槽位安装假面板的话，可能导致设备散热异常，出现温度告警，板卡存在烧坏的风险。



注意

1. 高端产品如果有槽位没有插板卡的话，需要安装假面板。

高危操作—黑白名单

9 MSG云网关系列&小贝钉钉智连系列&云AP配置白名单

【高危操作】
配置无线白名单
【操作后果】
所有已上线客户端会被强制下线。
【操作页面】
选择“安全”，进入安全配置页面。
在无线白名单区块单击<添加>按钮，如下图所示。

注意

1. 主网络设备若存在黑白名单设置，配置前应先注意配置黑白名单之后是否会对已有在线用户造成影响。

高危操作—误配置管理主机

10 D2000-G系列二代数据库审计误配置管理主机

如下界面误配置了管理主机IP地址后，导致无法登录设备：

注意

1. D2000-G系列二代数据库审计配置管理主机IP地址后只有这些地址可以管理设备，如存在误配置或忘记管理主机配置，则需登录后台修复。

第三章-主网络常见故障信息收集

1

PART 01

主网络问题处理“八问”

主网络问题处理“八问”

紫光集团 核心企业 | H3C 数字化解决方案领导者

- **现实问题**

当我们从用户那里接到一个故障时，工程师根据现象要求客户收集一堆信息，然后一线、二线用服、研发产品、研发平台一级一级反复咨询与确认，几乎每个故障都要经过多个层级的人进行处理，信息交流占据了每个人大部分的时间，反复收集信息与确认问题现象也会让用户不胜其烦。那么该如何减少这些环节无谓的损耗，提升问题的处理效率？接下来就带大家一同探讨下。

主网络问题处理“八问”

紫光集团 核心企业 | H3C 数字化解决方案领导者

- **问题处理第一问：什么业务有问题?**

在网络设备上承载的业务是多种多样的，而并不是所有用户均可以根据业务部门反馈的故障准确描述是什么类型的网络问题。这就需要详细询问客户遇到的问题，来推测可能和网络设备的哪些应用有关。

网络设备只不过是一个管道，并不关心承载的业务是搜索，还是云盘，网上商城等，网络设备**只关心是什么网络协议出了问题**。比如说是浏览网页（http协议）不可以，还是FTP下载不行，是PORTAL认证有问题，还是路由没生效？我们需要通过一系列的咨询，迅速掌握用户的业务和网络设备的什么功能有关系。

主网络问题处理“八问”

- **问题处理第二问：故障现象是什么?**

知道了是什么业务有问题，就基本知道和网络哪部分有关。比如最常见的就是某些网络链路不通。由于网络链路不通，导致了客户业务系统出现了各种各样的异常表现。我们需要再了解，是延迟大，还是丢包；是丢包还是彻底不通；是部分地址不通，还是全网不通；具体是从哪个地址到哪个地址网络互访有问题。

主网络问题处理“八问”

- **问题处理第三问：与哪个设备有关?**

  数据中心里的网络设备成千上万，当明确了故障现象后，接下来需要迅速找到故障设备。

  这时“流量统计，镜像，抓包”三大招就派上用场了。通过这些日常手段，结合业务测试或PING测试，就可以找到故障设备，这个过程决不能省，而且还要确保统计的结果准确无误。

主网络问题处理“八问”

- **问题处理第四问：用户是否操作过设备?**

有人做过统计，发现数据中心里出现的故障，70%是人为操作故障。每年运营商封网，或者节假日放假，大家会发现网上问题一下子少了很多，即使出现的也多是硬件故障。

由于每个人对各个设备，网络协议的理解程度不同，在做网络变更或者部署新的应用时，往往是故障的高发期，所以不要放过用户操作的任何细节，尤其很多时候用户认为自己的操作与故障毫无关系，就不去提。请仔细检查设备的log，history Command信息。

主网络问题处理“八问”

- **问题处理第五问：做过哪些排查?**

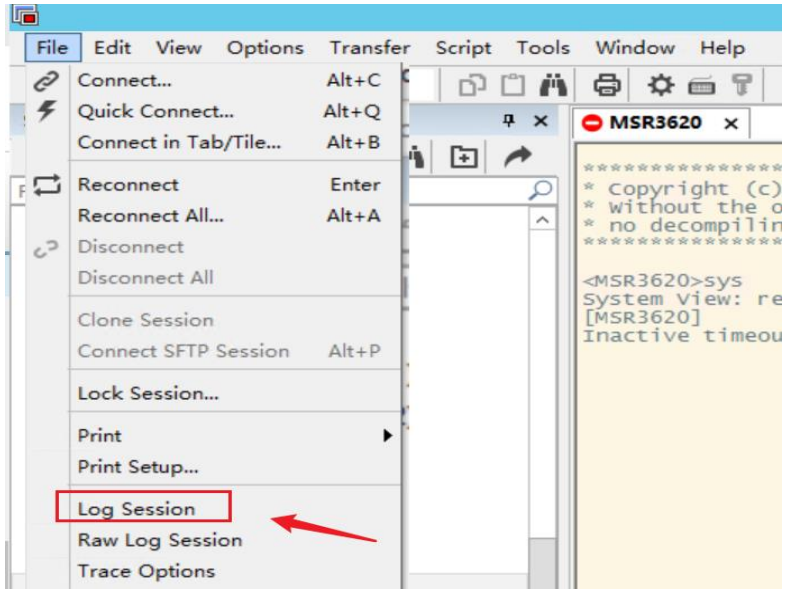
当遇到PING不通时，试着将ARP/MAC静态绑定下，看是什么结果；当遇到PBR不生效时，试着调整下PBR的配置，看是什么结果；当遇到下载速度慢时，试着换台PC测试下，看是什么结果… …，我们可以通过各种排查测试将故障现象进一步细化。

平时可以多翻翻操作手册、命令手册以及维护手册，这样遇到问题时才能得心应手。

主网络问题处理“八问”

- **问题处理第六问：操作记录呢?**

人会记错，但设备不会记错。任何时候操作设备时，都要留下操作记录，留日后自己分析，或者作为说明问题的证据。空口无凭，很难说服任何人，所以不仅要自己养成记录的好习惯，也要让用户养成记录操作记录的好习惯。



主网络问题处理“八问”

- **问题处理第七问：故障诊断呢?**

很多时候客户急于恢复业务，要求重启设备或不再配合测试，这样留给我们定位的时间很少，此时一定要采集故障时的DIAG信息。DIAG信息里包含了这台设备运行状态的各种参数，是产品经历过多年网上问题洗礼总结出的关键信息，所以通过DIAG往往能准确定位出80%网上问题。

除了DIAG，还有”LOGFILE，DIAG-FILE”都要收集，而且DIAG信息最好有故障时和正常时两份。

#导出并反馈以下信息
<H3C>logfile save
<H3C>diagnostic-logfile save
<H3C>display diagnostic-information
。。。
最后将上诉文件通过ftp或more方式回显导出。

交换机问题处理“八问”

- **问题处理第八问：H3C官网、知了社区是否有看过？标杆是否锤了？iservice CT网上问题智能诊断系统是否诊断了？**

如果问题不是那么着急，可以看看官网对硬件安装、适配关系、协议使用场景等是否有相关限制；知了社区是否有类似故障问题；此外，标杆和iservice中接口错包、设备运行异常等信息也是极有帮助的。

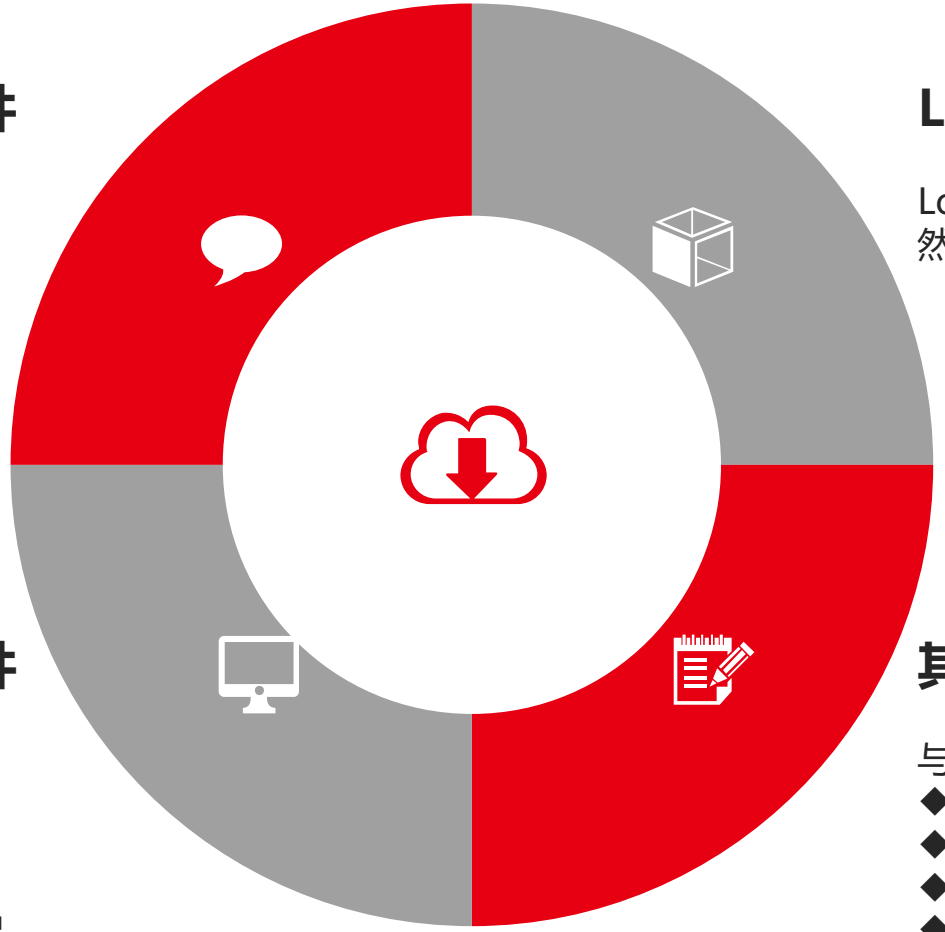
如果还是无法定位，需要将故障时间点、详细故障现象、DIAG、LOGFILE、DIAG-FILE、流统、操作记录等信息收集并反馈，有了这些详细信息，问题也许很快能找到答案，否则就要花费大量的时间去交流，影响问题处理效率。

2

PART 02

主网络产品故障信息收集

基础故障信息收集



诊断文件

display diagnostic-information
命令收集
选Y保存到设备存储，选N窗口输出

Logfile文件

Logfile save
然后more显示文件或者ftp导出

Diagfile文件

diagnostic-logfile save
然后more显示文件或者ftp导出

通常中低端产品仅出现内存告警时需要收集——如果发现有记录则说明设备出现过内存门限告警

其它现场信息

与故障相关或者记录故障现象的，如：

- 故障出现的CRT操作日志
- 业务异常信息
- 硬件故障的现场照片
- 组网图
- ……

诊断文件收集

紫光集团 核心企业 | H3C 数字化解决方案领导者

尽可能收集故障时诊断

诊断文件是设备当前常用维护命令的集合，如果能采集到故障时的诊断，对大多问题的定位会有帮助。
如果故障期间因着急恢复业务进行规避动作或设备自动重启等原因而无法采集故障时诊断，那么可提供恢复后诊断文件进行协助分析。

推荐保存后FTP导出

有条件使用FTP的情况下，建议选择Y保存到设备存储后通过FTP导出。除了console口收集诊断过慢外，还有以下优势：

- 合并收集core文件
- 记录诊断收集时间
- 收集结果纯净且完整，没有前后操作记录干扰

注意诊断收集用户权限

由于诊断文件本质也是在设备上收集命令回显，因此如果当前操作用户角色权限不足，可能无法收集部分权限受控的信息，导致诊断中大量回显为空。
因此，收集诊断前请提前确认是否最高权限登录设备执行收集命令。

完成诊断收集后可以用iservice CT网上问题智能诊断系统
或标杆神器先进行一次扫描检查

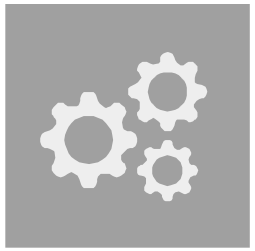
Logfile和diagfile

Logfile文件

- Logfile save命令会显示当前保存的日志文件路径和文件名，如：

```
<Sysname> logfile save
The contents in the log file buffer have been
saved to the file flash:/logfile/logfile.log.
```

- 收集时需要进入路径后根据日志文件生成时间，将包含故障发生到当前时间的logfile文件一同返回。若不好判断时间可将整个logfile文件夹一同返回。
- 如果是多主控设备或者IRF场景，建议将多个槽位存储空间里的logfile文件夹都进行检查，如果有近期生成的文件，也请一并返回。



Diagfile文件

- 中低端路由器设备在触发内存告警门限时，除了logfile中会记录日志外，会自动在diagfile中保存一份告警时的内存使用分布情况。
- 如果当前故障明确出现了内存利用率问题，则必须收集diagfile文件（注意是设备告警不是网管平台判断的告警）用于分析内存异常原因。
- 如果无法判断故障原因时，可以检查设备diagfile是否有新记录。如果diagfile没有任何信息，则大概率可以排除内存超过阈值导致故障。
- 如果是多主控设备或者IRF场景，也建议多个槽位遍历检查和收集。

其它现场关键信息

电源风扇等外部器件异常

- 收集现场照片/视频
- 反馈指示灯情况
- 进行交叉替换测试

板卡无法识别

- 收集板卡无法加载过程中命令行的日志打印
- 反馈板卡指示灯情况
- 进行交叉替换测试
- 拍摄板卡和机框连接器照片

网管告警

- 反馈告警节点或告警内容
- 告知告警触发/恢复时间
- 确认属于设备trap告警还是网管自生成告警，若为自生成告警则须告知告警机制

设备无法启动

- 收集现场设备照片
- 描述指示灯情况
- 确认Console口是否有输出
- 进行电源交叉替换测试
- ……

主控无法启动

- 反馈指示灯情况
- 收集主控板在重启过程中console口的输出信息

业务异常

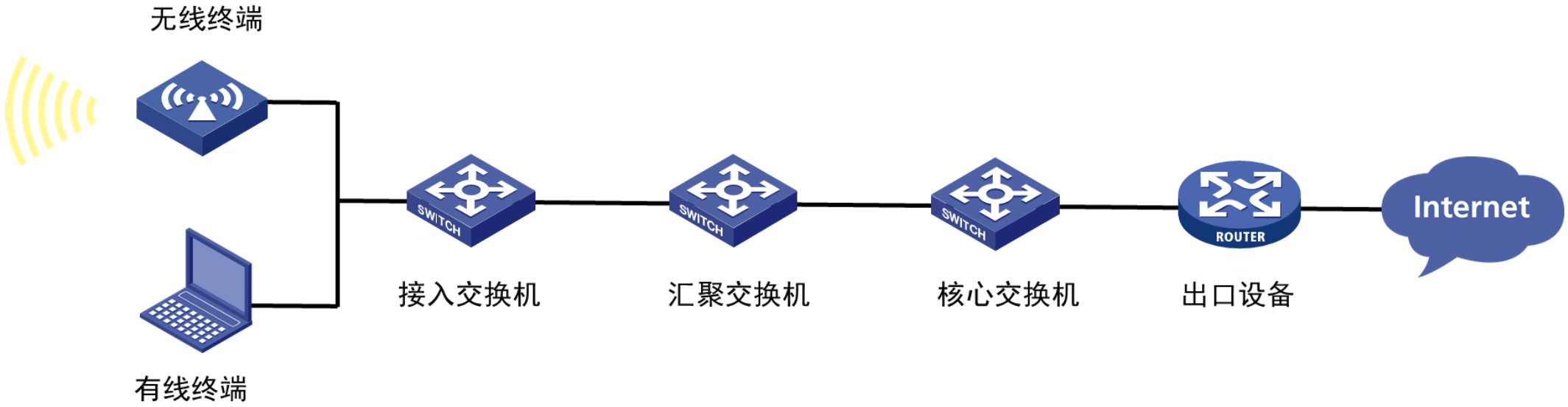
- 反馈组网拓扑
- 告知故障业务源目的地址或网段信息
- 描述流量走向

3

PART 03

主网络产品维护通用手段

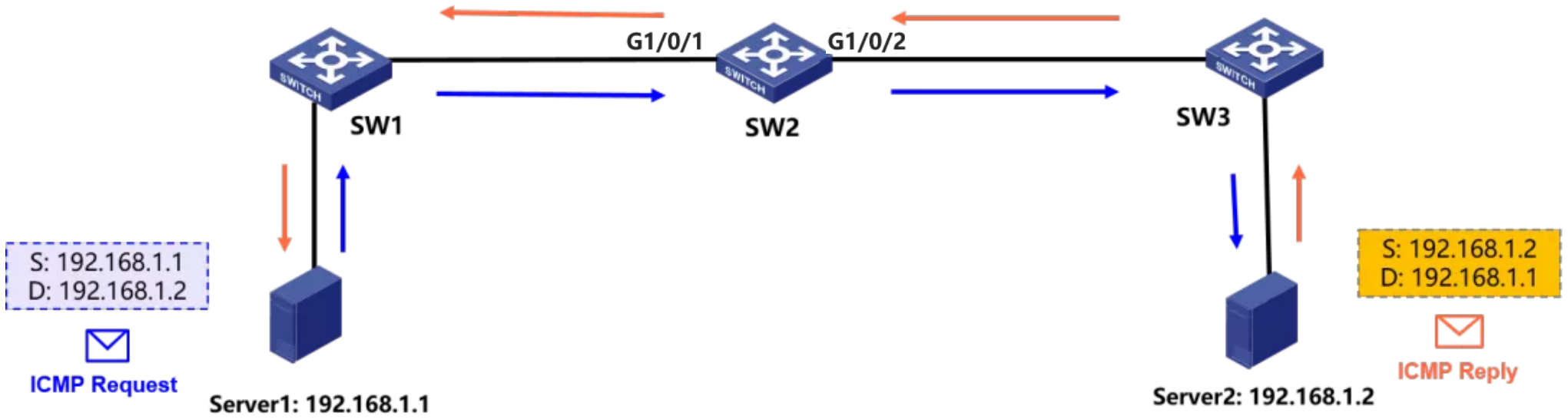
定位流量丢包位置方法



定位流量丢包位置常用方法：1、分段测试；2、流量统计；3、镜像抓包；4、debug

交换那些事儿 | 基础维护篇 - 流统

ICMP流统方法



交换那些事儿 | 基础维护篇 - 流统

ICMP流统方法

Step 1 :定义ACL匹配某一方向的流量

acl advanced 3000

rule 0 permit icmp source 192.168.1.1 0 destination 192.168.1.2 0

Step 2:定义类匹配ACL并开启计数动作

traffic classifier c1 operator and

if-match acl 3000

traffic behavior b1

accounting packet

Step 3：定义QOS策略关联类和动作

qos policy p1

classifier c1 behavior b1

Step 4：在1/0/1口和1/0/2口运用QOS策略

interface GigabitEthernet1/0/1

qos apply policy p1 inbound

interface GigabitEthernet1/0/2

qos apply policy p1 outbound

ICMP request

Step 5 :定义ACL匹配某一方向的流量

acl advanced 3001

rule 0 permit icmp source 192.168.1.2 0 destination 192.168.1.1 0

Step 6:定义类匹配ACL并开启计数动作

traffic classifier c2 operator and

if-match acl 3001

traffic behavior b2

accounting packet

Step 7：定义QOS策略关联类和动作

qos policy p2

classifier c2 behavior b2

Step 8：在1/0/1口和1/0/2口运用QOS策略

interface GigabitEthernet1/0/1

qos apply policy p2 outbound

interface GigabitEthernet1/0/2

qos apply policy p2 inbound

ICMP reply

ICMP流统方法

```
<SW2>display qos policy interface
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: p1
   Classifier: c1
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: b1
      Accounting enable:
        5 (Packets)
Interface: GigabitEthernet1/0/2
  Direction: Outbound
  Policy: p1
   Classifier: c1
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: b1
      Accounting enable:
        5 (Packets)
```

ICMP request

```
Interface: GigabitEthernet1/0/1
  Direction: Outbound
  Policy: p2
   Classifier: c2
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: b2
      Accounting enable:
        5 (Packets)
Interface: GigabitEthernet1/0/2
  Direction: Inbound
  Policy: p2
   Classifier: c2
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: b2
      Accounting enable:
        5 (Packets)
```

ICMP reply

用户视图下的reset counters interface命令清空流量统计信息

镜像抓包

镜像指通过将指定报文复制到连接监测设备的端口，使用户可以在监测设备上利用复制的报文对网络进行监控和分析。

镜像源是指被监控的对象，可以是端口、CPU或符合一定特征的数据流。镜像目的端口是连接审计服务器、个人电脑等监测设备的端口。入方向镜像是指仅复制镜像源收到的报文，出方向镜像是指仅复制发出的报文，双向镜像则是指复制收到和发出的报文。

实际运维过程中经常遇到的“抓包”操作，就可以通过镜像来实现。常用的镜像方法有:

1.本地端口镜像

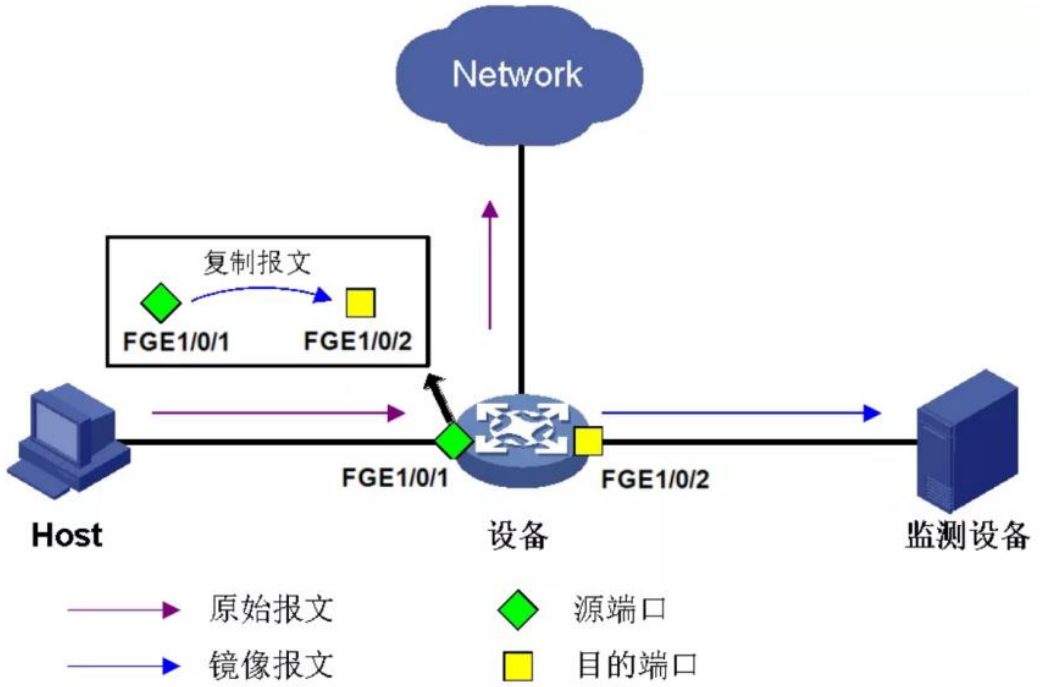
2.二层远程端口镜像

3.远程镜像VLAN实现多目的端口

4.三层远程端口镜像

5.流镜像

镜像抓包——本地端口镜像



Step 1: 创建本地镜像组1

[Device] mirroring-group 1 local

Step 2: 配置本地镜像组1的源端口为FGE1/0/1，对源端口收到的报文进行镜像，目的端口为FGE1/0/2

[Device] mirroring-group 1 mirroring-port fortygige 1/0/1 inbound

[Device] mirroring-group 1 monitor-port fortygige 1/0/2

Step 3: 在目的端口FGE1/0/2上关闭生成树协议

[Device] interface fortygige 1/0/2

[Device-FortyGigE1/0/2] undo stp enable

4

PART 04

主网络产品常见问题排查思路

交换机丢包问题排查

开始

No.1 明确故障发生时间

故障是否规律、一直异常、某个时间异常?

No.2 确认报文丢弃位置

1、分段测试；2、流量统计；3、镜像抓包；4、debug

No.3 检查logbuffer

检查接口Down/UP;
检查设备运行的动态路由协议邻居等状态是否存在变更;
检查设备是否收到大量刷新转发表项的TC报文

No.4 检查接口

display interface查看接口错包（input errors）计数是否增长
display transceiver diagnosis interface xxx查看光口收发光
确认接口是否存在超带宽、拥塞丢包:
display counters rate inbound interface
display interface xxx（看Peak input rate、Peak output rate）
display qos queue-statistics interface+端口+outbound

No.5查看转发表项

三层转发：display ip routing-table 、display fib 、display arp
二层转发：display mac-address

交换机丢包问题排查（续）

No.6检查二层环路

```
<H3C>display  mac-address mac-move
[H3C-probe]debug l2 slot 1 chip 0 mac/move_rec/show
```

No.7 STP是否正常

display stp brief查看接口转发状态
display stp abnormal-port确定接口是否被阻塞
display stp tc确认收到的tc报文是否在不停增加

No.8 检查路由是否正常

display ip routing-table查看路由是否正确，是否稳定；
[spine-probe]debug rxtx softcar show slot x检查是否有路由环路（IPV4_TTL数值是否在不停增长）

No.9 检查ARP是否正常

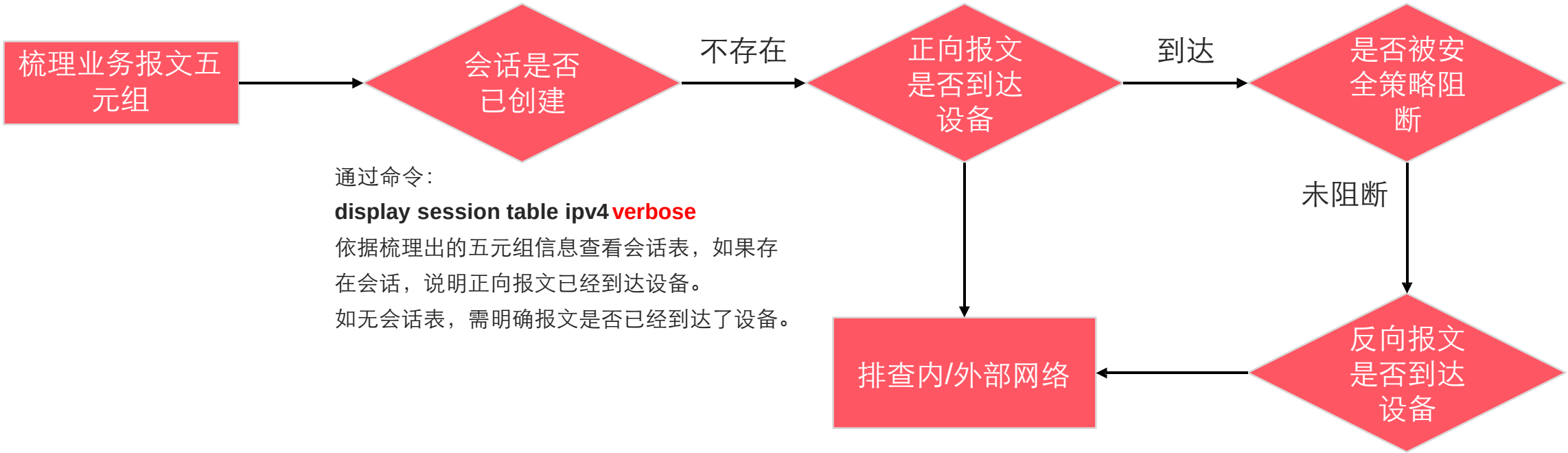
[H3C-probe]debug rxtx softcar show slot X检查ARP是否超限速（正常流量or现网攻击？）；
[S6800-probe]debug ipv4-drv show config slot x确认设备的ARP表项是否超规格；
<S6800>debugging arp packet 确认ARP学习过程；

No.10其他

框式设备确认内联口是否存在异常；
入方向报文封装是否正常；
是否存在Parity-Error告警；
检查交换机版本说明书是否存在已知问题

结束

业务过防火墙不通思路



通过命令：

display session table ipv4 verbose

依据梳理出的五元组信息查看会话表，如果存在会话，说明正向报文已经到达设备。

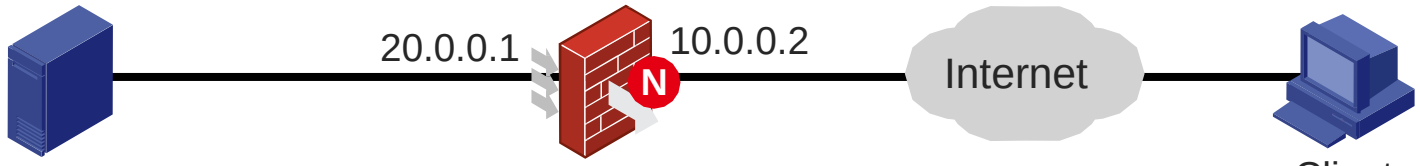
如无会话表，需明确报文是否已经到达了设备。

开启**debugging ip packet acl xxx**、**debugging ip info acl**或web页面抓包

通过**debugging security-policy packet ip** *acl*、**debugging aspf packet** *acl*命令检查ASPF策略是否阻断报文

思路与正向报文相同，只是需将debug查看的ACL修改为匹配反向流量五元组

NAT场景业务不通排查



FW NAT Server配置

NAT Server	Global IP:Port	Inside IP:Port	协议
Entry 1	10.0.0.2:80	20.0.0.2:8080	TCP

- 会话表是否创建
- 报文是否到达FW
- NAT是否正常转换
- 报文是否被策略阻断
- 反向报文排查

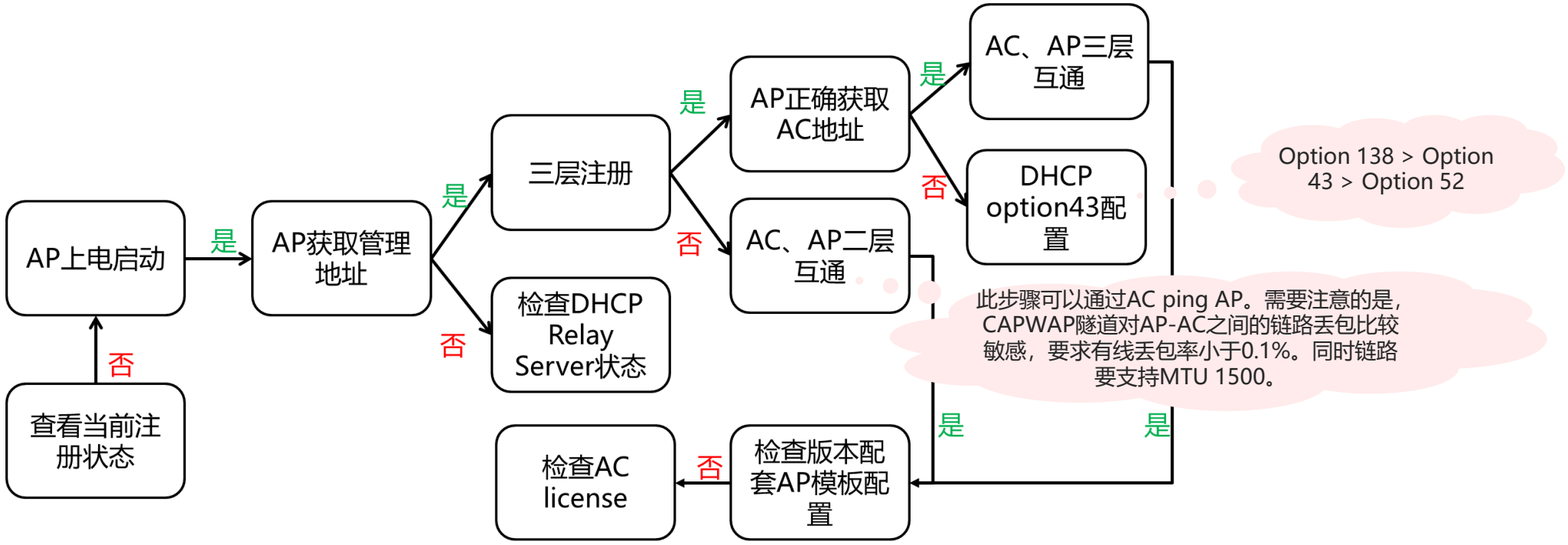
NAT转换前的五元组信息
TCP
Source IP 10.0.0.1
Dst IP、Port：10.0.0.2:80

NAT转换后的五元组信息
TCP
Source IP 10.0.0.1
Dst IP、Port：20.0.0.2:8080

acl advanced 3000
rule 0 permit tcp source 10.0.0.1 0 destination 10.0.0.20
rule 5 permit tcp source 10.0.0.1 0 destination 20.0.0.20
（NAT转换后的来回报文）
rule 10 permit tcp source 20.0.0.2 0 destination 10.0.0.10
rule 15 permit tcp source 10.0.0.2 0 destination 10.0.0.10

NAT场景下业务不通需根据NAT类型来判断查看的五元组信息，其余步骤与正常业务不通步骤相同。

无线AP注册不上排查思路



注册不上信息收集：
1、AC 诊断和AP诊断；
2、如果有配置MAP文件，收集MAP文件信息；
3、AC和AP上分别收集debug wlan capwap all。

课程总结

- **介绍H3C常用工具和资料：**新华三官网、知了社区、iService服务数字中枢、标杆的神器、HCL华三云实验室、其他；
- **介绍主网络设备高危操作：**高危操作手册、高危操作案例；
- **介绍主网络常见故障信息收集：**主网络问题处理“八问”、故障信息收集方法、主网络产品维护通用手段、主网络产品常见问题排查思路。

Thanks!

新华三集团
www.h3c.com