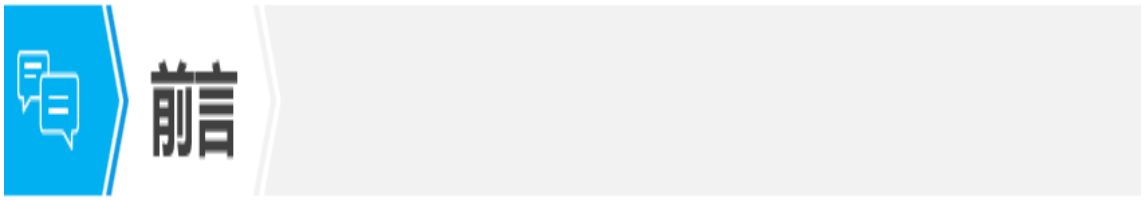
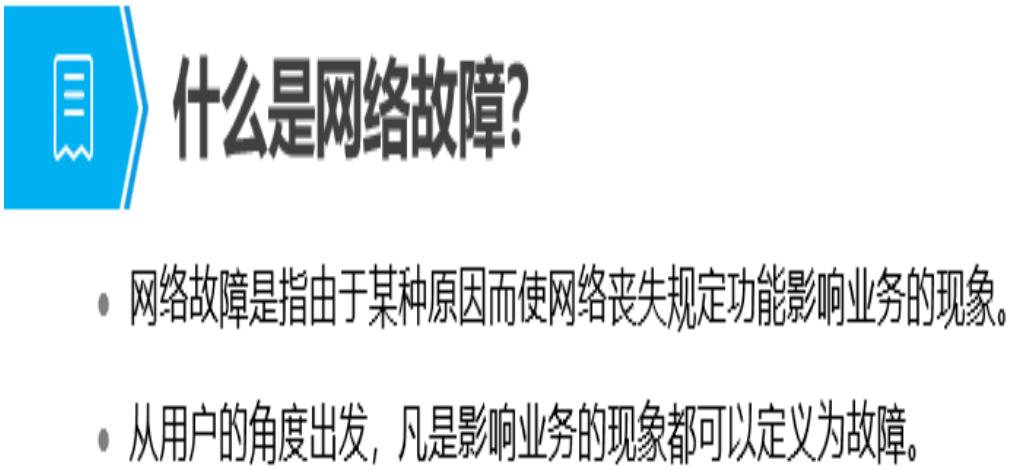
网络故障排除综述





- 网络故障是指由于某种原因而使网络丧失规定功能影响业务的现象。
- 从用户的角度出发，凡是影响业务的现象都可以定义为

故障。因而故障不一定只是设备问题，也有可能是系统或兼容性等问题。

网络故障的分类

现象 / 分类	告警	环路	业务不通	业务中断	业务瞬断	丢包	协议异常	协议震荡	路由异常
硬件类	√			√		√			
配置类		√	√				√		√
网络类		√	√	√	√	√	√	√	√
性能问题	√				√	√		√	√
软件类							√		√
对接类		√	√				√		
其他	√		√	√	√	√			

- 网络故障可以分为硬件类、配置类、网络类、性能问题、软件类、对接类以及其他故障。不同的网络故障所引起的异常现象如表所示。

PDIOI与网络故障排除

- Operate:
  - 日常维护
  - 故障排除

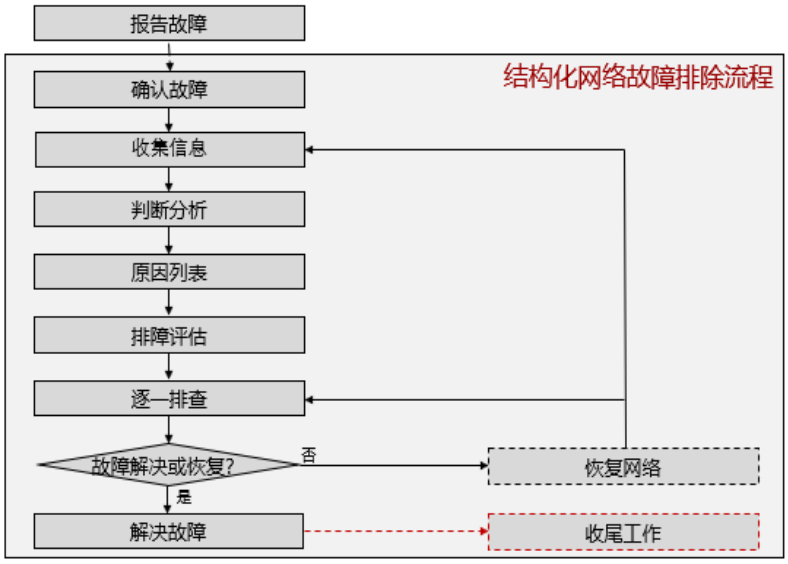
- 网络故障排除是 PDIOI 中维护阶段（Operate）的重要工作。
- 日常维护的目的是预防故障发生；故障处理是指在故障发生之后，采取措施，使系统尽快恢复正常。
- 故障处理是事件驱动的工作任务，通常会比较突然地出现，对工程师的技术能力也提出了更高的要求。
- 尽管良好的日常维护可以规避大量的突发故障，但是由于网络运行受到多方面条件限制，再好的日常维护也不可能完全避免突发故障的发生。因此网络维护人员具备关键的技术，并掌握故障处理流程和方法是非常必要的。

问题的提出

- 凭直觉或个人经验采取网络故障排除措施：
  - 难于进行团队协作。
  - 没有故障排除工作的文档总结。
  - 无法保证故障排除工作的连续性。

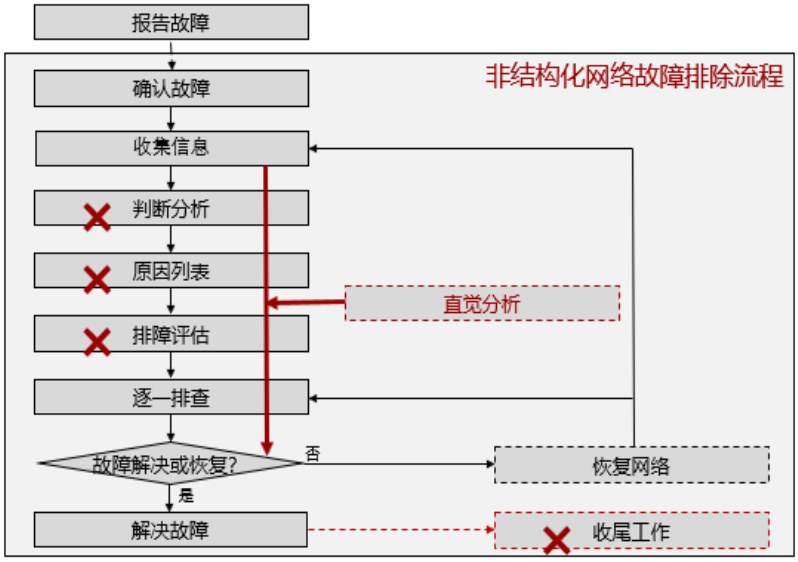
- 只是凭直觉或个人经验采取网络故障排除措施，虽然最终也可能找出解决方案，但很难将排障工作转交给其他人，不利于团队协作。已经实施过的排障结果也可能遗忘或丢失。甚至过了一段时间，该人员再次检测与排除同样的故障时都有可能无法继续下去。

结构化的网络故障排除流程



- 结构化的网络故障排除流程由报告故障触发，是合理地一步一步地找出故障原因，并解决故障的总体流程。基本步骤是确认故障、收集信息、判断分析、原因列表、排障评估、逐一排查、解决故障，其基本思想是系统地将故障的所有可能原因缩减或隔离成几个小的子集，从而使排障的复杂度迅速下降。
- 排除了故障之后，还需要进行收尾工作，如输出故障处理报告，向相关部门汇报、通告故障处理情况等。

非结构化的网络故障排除流程



- 如果采取非结构化的网络故障排除流程，就只是凭直觉在这些步骤之间重复执行，虽然最终也可能找到解决故障的方法，但没有办法保证效率。
- 在复杂的网络环境中，有可能会由于非结构化的网络故障排除流程而导致新的故障，从而使网络故障的排除变得更加困难。

报告故障

- 周一上午你接到一名公司员工的故障申报电话，内容是“无法通过PC访问互联网，希望尽快解决问题。”

- 接到这个电话，你需要做什么?

报告故障 - 主动沟通确认

故障报告者	姓名、所在的部门、职位级别、所负责的工作内容、使用电脑的位置（楼层、房间、无线接入还是有线接入）、在使用电脑访问什么网站时发现的问题。
故障频率	故障是突发的、偶尔的、还是频繁的。
用户操作	出现故障之前和之后，用户对自己的终端做了哪些操作，如是否更改了IP地址和DNS、是否安装了桌面防火墙软件、安全控制软件等。

- 在电话里询问用户上面的内容，并记录在排障报告中。

- 网络故障排除通常是从用户报告故障开始的，而用户报告故障主动提供的信息经常是模糊、笼统的，所以需要进行主动沟通、确认。

报告故障 - 预先推测

- 思考:
  - 为什么需要了解用户的职位级别、工作内容等信息?
- 答案:
  - 在企业环境中，不同级别的用户可能会有不同的网络访问权限。即使相同级别的用户，可能也只有权限使用自己工作内容相关的网络服务。

为什么要确认故障

- 用户的描述可能是含糊不清的，报告的故障也不一定是真实的故障点，所以需要有经验的工程师进行确认故障的工作。

- 以图中所示的一个最简单网络环境为例，用户可能会报告说：“服务器出故障了，因为现在我无法访问它”，而真实的情况可能是某条链路的故障而导致服务器无法访问。

确认故障

- 确认故障的四个要素：
  - 主体；
  - 表现；
  - 时间；
  - 位置。
- 对故障现象进行准确的描述。
- 确认该故障是否属于自己的负责范围。

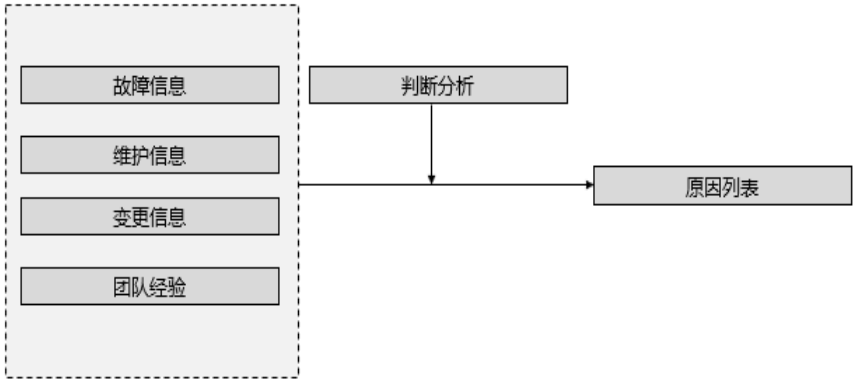
- 确认故障需要了解这些信息，确定故障现象：
- 故障的主体：哪个网络业务出现了故障；
- 故障的表现：故障的现象是什么样的；
- 故障的时间：用户是什么时间发现的故障，以及专业人员推测的故障出现的真实时间；
- 故障的位置：哪个网络组件出现了故障；
- 应对故障现象进行准确描述。
- 最后应确认该故障是否属于自己的负责范围，即自己是否被赋予了相应的权限来处理该故障。

收集信息

- 需要收集哪些信息。
- 如何收集这些信息。
- 是否需要授权。
- 收集信息阶段的风险评估。

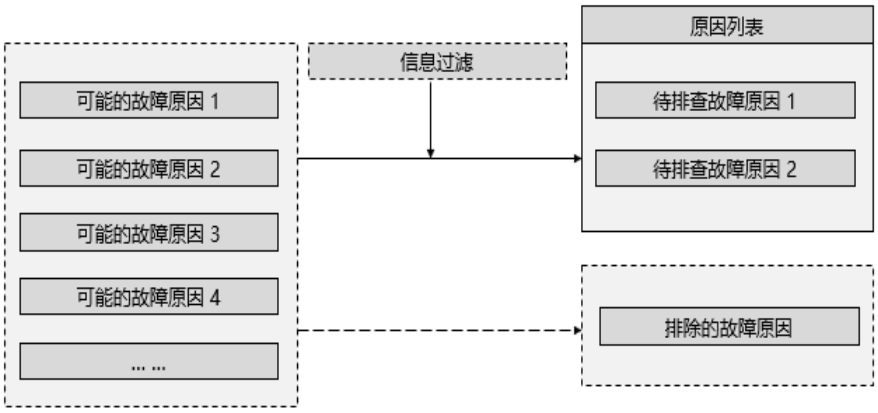
- 需要收集哪些信息：收集信息阶段主要是收集与故障相关的信息，如文档、网络变更情况等。
- 如何收集这些信息：是使用设备自身的操作命令，还是需要使用到额外的信息收集工具，如抓包工具、网管软件等。
- 是否需要授权：在对信息安全要求较高的网络环境中，对信息的收集是需要得到授权的，有时需要签署书面的授权文件。
- 收集信息阶段的风险评估：有些收集信息的操作，如对路由器或交换机执行“debug”命令，会导致设备的 CPU 占用率过高，严重的情况下甚至会使设备停止响应用户的操作指令，从而引入额外的故障现象。所以在收集信息的时候应评估这些风险，平衡引入新故障的风险与解决现有故障的紧迫性之间的关系，并明确的告知用户这些风险，由用户来决定是否进行风险较大的信息收集工作。

判断分析

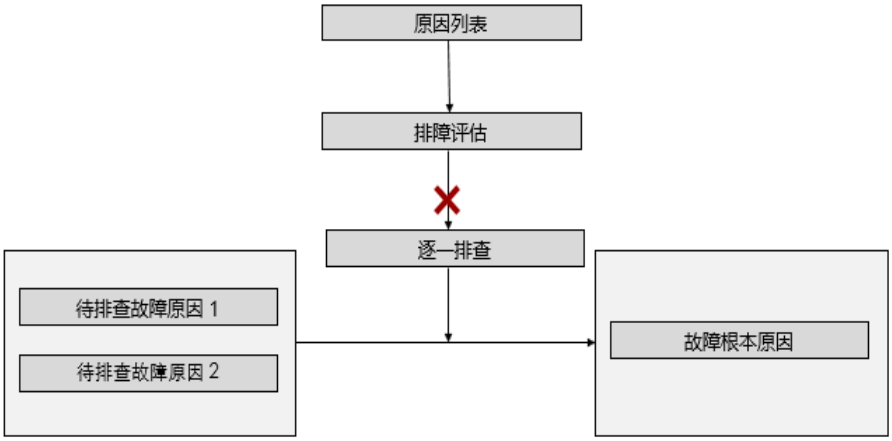


- 判断分析阶段是对收集到的信息进行分析整理。
- 通过对故障信息、维护信息、变更信息的汇总，结合团队经验（或个人经验）进行综合的判断和分析，得到可能导致网络故障的原因列表。

原因列表



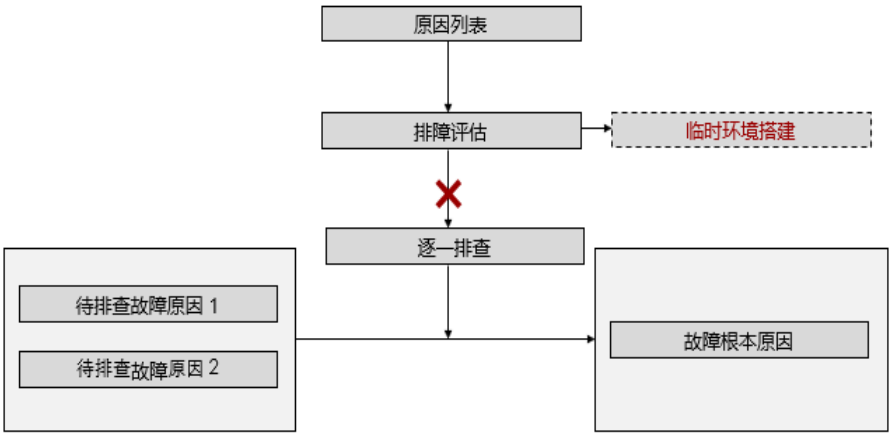
排障评估



- 需要在逐一排查前进行故障评估工作。

- 列出待排查的故障原因清单后，应该首先评估故障排除工作的复杂程度（如排除网络故障的难度和所需解决时间等），而不是马上开始进行逐一排查。

排障评估 - 临时环境搭建



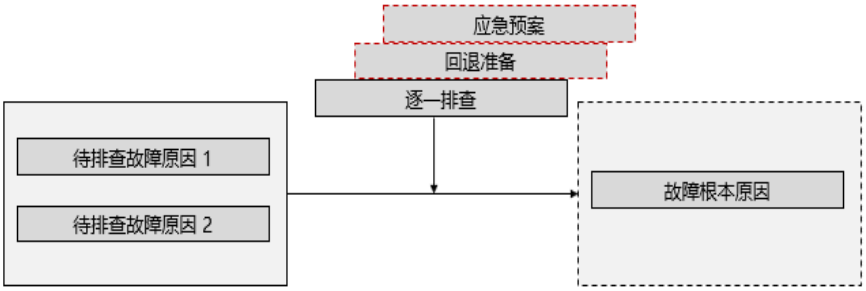
- 在故障评估阶段可能需要搭建临时的网络环境。

- 对复杂的网络故障，如果经过评估认为短时间内无法排除故障，而用户又需要马上恢复网络的可用性，这时可能需要

临时跳过故障节点，搭建替代的网络环境。

- 搭建临时网络环境的时候，应充分考虑到解决问题的迫切性与绕过某些安全限制措施的危险性，应与用户进行充分的沟通，明确必要的信息，并在得到许可的情况下才能执行。

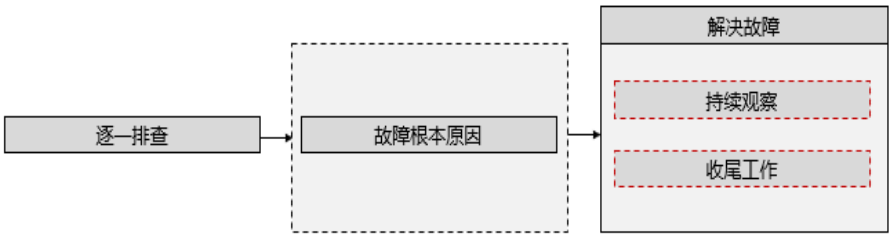
逐一排查



- 逐一排查的过程可能涉及到网络变更。

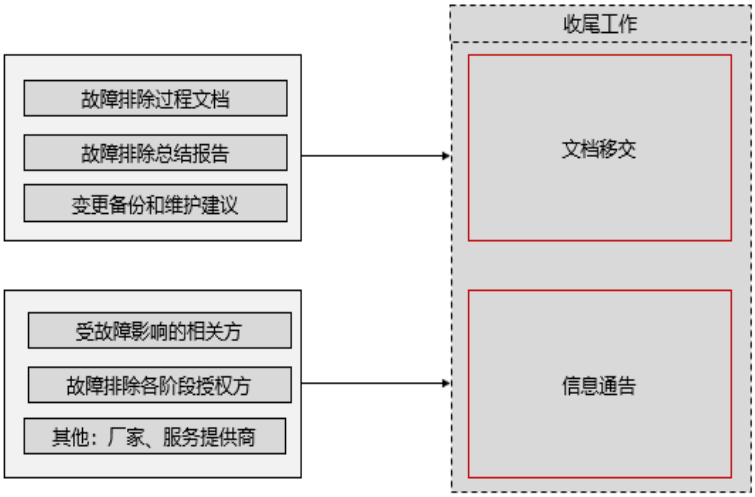
- 在逐一排查阶段同样需要平衡解决问题的迫切性与引入新故障的风险性之间的矛盾。所以，应该明确告知用户排查工作可能带来的风险，并在得到许可的情况下才能执行操作。
- 有些情况下，通过逐一排查验证推断的过程涉及到网络变更，这时必须做好完善的应急预案和回退准备。

解决故障



- 有时解决故障后仍需要持续观察一段时间。

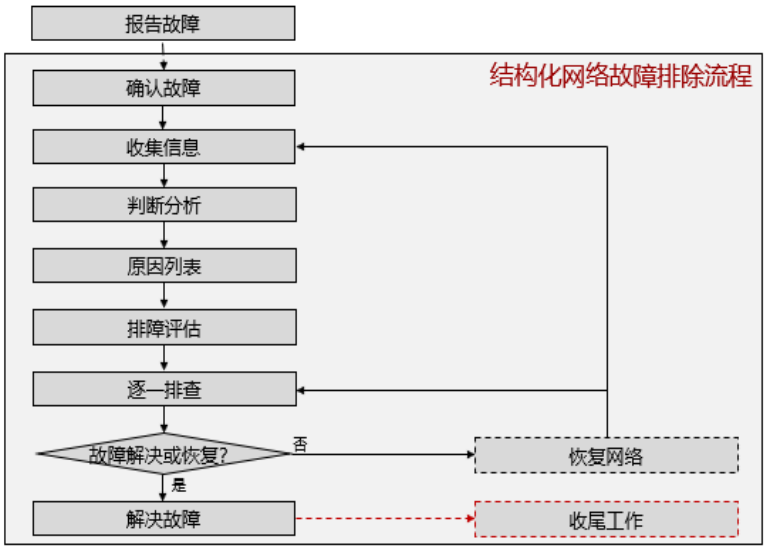
解决故障 - 收尾工作



- 故障排除之后的收尾工作同样重要。

- 收尾工作包括相关文档的整理、信息的通告等。需要对之前网络故障排除流程中所有进行了变更的配置或软件进行备份，并做好故障排除文档的整理和移交工作。为了避免同样的故障再次发生，在此阶段应该向用户提出改进建议。

回顾：结构化的网络故障排除流程



- 相对于非结构化的网络故障排除流程来说，结构化的网络故障排除流程所产生的结果是可预期的，排障过程中所造成的影响是可控的，引入新故障的风险是可评估的。

TCP/IP参考模型与网络故障排除

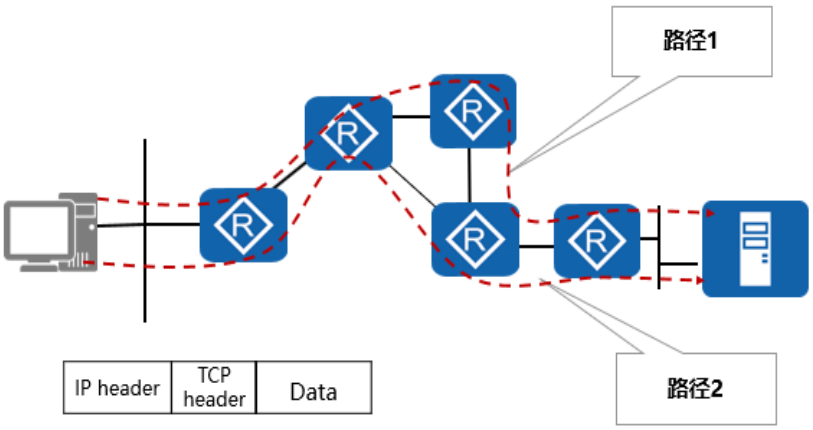
- TCP/IP参考模型是网络故障排除的理论基础，OSI参考模型的物理层和数据链路层也是需要我们关注的。

- TCP/IP 参考模型是网络故障排除的理论基础，OSI 参考模型的物理层和数据链路层（这两层对应于 TCP/IP 参考模型

的网络接口层）也是需要我们关注的。推荐的故障排除方法是从 TCP/IP 参考模型的网络接口层和网络层分别确认并测试业务流量的路径，然后采用自顶向下法或自底向上法进行故障排除。

- 在复杂的网络环境中，网络故障排除该从何着手？
- 如图所示，在一个有着财务、OA（Office Automation System，办公自动化系统）、生产、甚至更多业务系统的复杂网络环境中，网络故障排除首先需要关注的是各业务系统的数据流方向。
- 在企业环境中，网络存在的作用即是服务于业务，只需要知道受到网络故障影响的业务的流量往返路径，跟踪此路径，逐步排除即可。
- 通常情况下，网络中业务流量的路径是在网络规划阶段就已经设计好的，在网络故障排除过程中可以首先向用户询问受影响的业务流量路径是如何规划的，然后使用 ping 和 tracert 工具进行测试，验证当前的业务流量路径是否与预期的业务流量路径相一致。

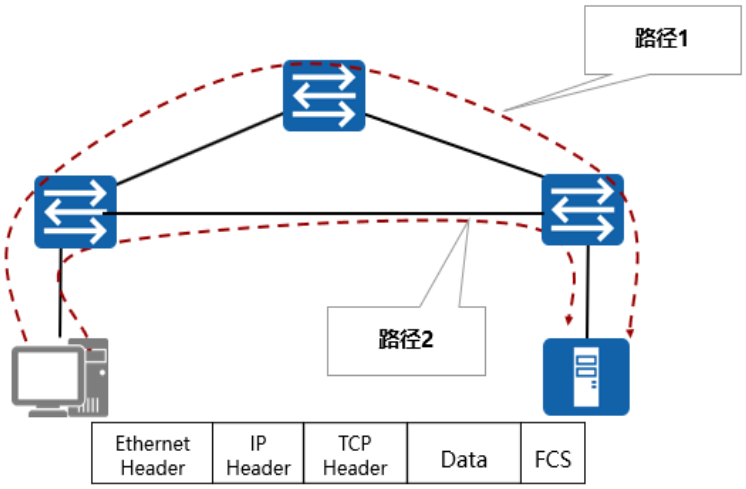
确认业务流量路径 - 网络层



- 网络层确认业务流量路径需要了解报文是如何被路由的。

- 在网络层，确认业务流量路径的工作内容是了解数据报文在网络中的可路由设备（路由器、有路由功能的交换机、防火墙等）上是如何被路由的。

确认业务流量路径 - 数据链路层



- 网络接口层确认业务流量路径需要了解数据帧是如何被交换机转发的。

- 在数据链路层，确认业务流量路径需要了解数据帧是如何被交换机转发的。要确认数据帧在交换机之间的转发路径需

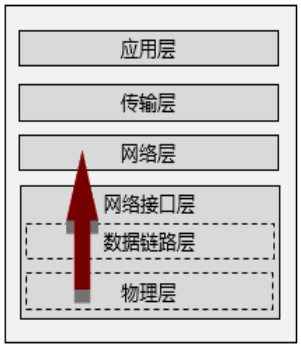
要查看交换机上的 MAC 地址表、了解生成树协议收敛的情况，有时还需要抓包工具的协助。

自顶向下法

- 如果网络层的连通性没有问题，可以使用自顶向下法进行故障排除。

- 在确认业务流量路径的过程中，同时也验证了网络层的连通性。
- 如果网络层的连通性没有问题，可以使用自顶向下法进行故障排除。即从应用层开始，对比相同应用的工作状态、检查是否存在应用层代理、应用层防火墙等导致故障现象的因素。

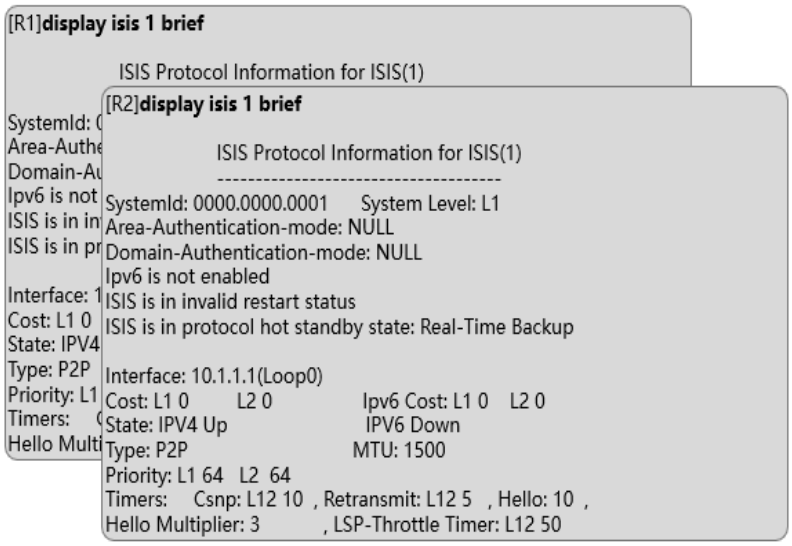
自底向上法



- 如果网络层的连通性有问题，可以使用自底向上法进行故障排除。

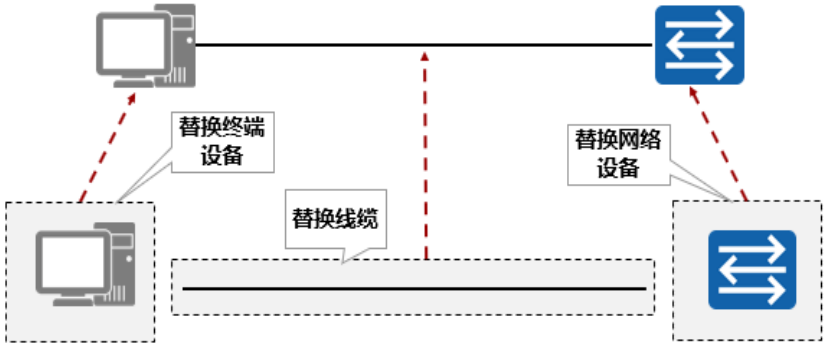
- 如果网络层的连通性有问题，说明支持网络层的下一层或网络层本身可能存在问题，这时可以使用自底向上法进行故障排除。在物理层，检查是否存在网络线缆故障等问题；在数据链路层，检查是否存在二层环路故障、链路层协议不匹配等问题；在网络层，检查是否存在路由协议配置错误、防火墙过滤等问题。

对比配置法



- 对比配置法是指对比正常状态与故障状态下的配置、软件版本、硬件型号等内容，检查两者之间的差异。
- 经验较少的网络故障排除人员在实践中会更多的使用到这种方法。

替换法



- 替换法是检查硬件问题常用的方法。

- 替换法是检查硬件问题常用的方法。在没有条件收集到

更多信息的环境下可以使用替换法隔离故障范围。

- 应用层也可以使用替换法。如财务部门的用户无法访问财务服务器，可以检查其他同部门的用户是否也存在同样问题。

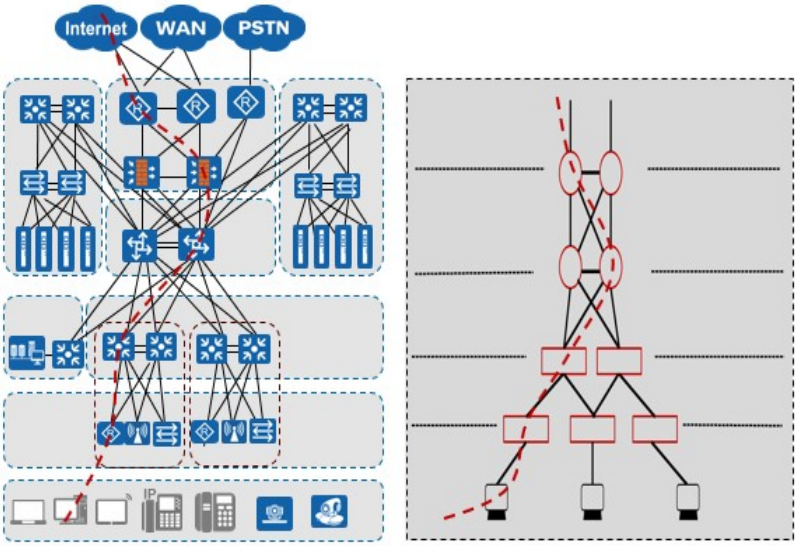
分块法

- 对网络设备的配置文件进行分块分析：

Cfg.txt

配置	内容
管理部分	路由器名称、口令、服务、日志等。
端口部分	地址、封装、cost、认证等。
路由协议部分	静态路由、RIP、OSPF、BGP、路由引入等。
策略部分	路由策略、策略路由、安全配置等。
接入部分	Telnet登录等。
其他应用部分	QoS配置等。

分段法



- 当排除大型网络环境中的网络故障时，可以基于受到故障影响的业务流量路径，使用分段法将故障的排除范围缩小。

思考题

1. 在结构化的网络故障排除流程的收尾工作中，下列哪几项是需要主要进行信息通告的相关方?

A. 受故障影响的相关方。

B. 故障排除各阶段授权方。

C. 厂家、服务提供商。

D. 对故障根源感兴趣的其他无关人员。

- 1、答案：ABC。
-