

如何诊治IP网络故障

IP网络故障定位的复杂程度，非一般运维人员所能掌握。如何让运维人员追本溯源，了解IP故障发生的机理，掌握从现象到定位的过程，并顺利排障？

文/黄斌



IP网络故障管理难表现为两点：第一，告警数量多，甚至是泛滥，每天告警工单数量很多，但一些告警定位后，又不需要作任何恢复动作，维护人员不堪重负。第二，故障发生却无任何告警，只能摸索排查，定位耗时长，非常依赖人的经验。这两种现象给故障管理工作带来非常大的困扰，本文将深入诊断其发生的根源，并给出相应的治理办法。

溯源

故障告警多

告警数量多的根源与IP网络两个特点相关，第一个特点是网络层次多，例如一个VLL（Virtual Leased Line）业务在IP网络上承载，要经过物理层、链路层、路由协议、MPLS、VLL等多层次处理，若某条物理光纤发生中断，那么物理层、链路层、IP传输层、VLL管道层将全部受到影响，这些层次也将全部发送TRAP。第二个特点是协议关联多，一般物理光纤的故障将引起路由协议的收敛，再引起MPLS LDP等协议的变化，这个过程中必然要发送大量的TRAP。

无告警

无告警的问题相对复杂。我们先回顾一下故障的定义，故障是产品或产品的一部分不能或将不能完成预期功能的事件或状态，简单地说，就是现状不符合预期。反之，如果没有“预期”，则不会有“故障”。实际上，正是IP网络上的预期无法清晰定义，才导致了“无告警”现象的发生。我们从控制平面和转发平面的原理出发，追溯无告警发生的根源。

控制平面决定源到目的地的业务路径。在传统的电路网络上，管理员静态指定主备路径，每个业务的下一跳非主即备，预期非常清晰。而在IP网络上，路由协议根据网络实际情况选择最优路径，单个路由器只知下一跳，并不掌握业务路径。因此，当链路中断产生路由收敛或者路径计算错误，导致路径发生变化时，路由器无法告警业务路径切换。

华为曾遇到过这样一个网上问题，NGN语音业务中断40多分钟而IP承载网无任何告警，排查中发现是LSP路径计算错误，其结果与ISIS路径不一致而导致业务中断。在这个案例里，建立LSP的协议并不掌握路径预期，因此无法发现LSP路径计算错误，也就无法发出



告警通知路径错误。

在转发平面上，IP网络不是同步网络，其转发机制无法定义预期，比如，业务报文要经过路由器A、B顺序转发，但是B完全不知道A是否有报文会送到，有报文送到是正常，没有也是正常，因此当A路由器故障无法转发报文时，B无法告警。

此类故障最常见的情况是路由器间的光纤劣化，光纤上发生了丢包，但路由器上无告警。对于这类故障的排查需要花费大量的时间，需要按照承载网的转发路径，逐个路由器、逐条链路去排查，最终才能发现是光纤故障导致丢包。

厘清IP网络故障管理难的根源后，排障的思路和措施就比较明确了，下文将给出华为针对告警多和无告警故障的解决之道。

排障

突出根源告警

前文提到，告警数量多的根源在于层次多、关联多，底层故障衍生出大量高层告警。如果我们能够突

出根源告警，忽略或者抑制衍生告警，就不需要针对无效告警派单处理，从而减少工作量。

从华为的网上问题库中统计发现，IP网络的故障根源大部分来自于硬件、链路的劣化。尤其是网络中的链路，如光纤、微波等，容易受到环境影响，从而导致接口闪断。接口反复UP/DOWN，将引发大量接口的告警，同时又引起IGP协议收敛，引发IGP反复告警，进而引发LSP的反复告警。即链路的告警将衍生出大量的协议告警。

针对以上情况，华为提出两种告警优化的思路：第一，在告警监控中，将告警归类为环境、硬件、软件、接口、链路管道、协议和业务等几个类别，环境、硬件类告警的处理优先级大于协议、业务类告警。高级别告警处理恢复后，其衍生的低级别协议告警会自动恢复。这种方法简单实用，可短期见效。第二，建设告警相关性系统，按协议、业务运行关系定义告警的衍生关系。在告警监控系统上，将衍生告警挂载在根源告警上显示，管理员直接处理根源告警，这种方法可以比较完善地解决告警多的问题，但建设困难且周期较长。

解决“无告警故障”的关键在于预期和现状的对

比，我们仍从控制平面和转发平面分别阐述。

路径预期和检测

尽管IP的控制平面采用了动态协议，但其运行的基础仍然是物理链路和SPF（Shortest Path First）算法，链路规划越简单，路径预期就越清晰。如在大部分的中小型城域网设计中，网络层次少，层次之间采用主备双链路进行保护，路径非主即备。对于这种网络，只要维护好网络拓扑图，就可以满足故障处理的需要。

对于大型、复杂的网络，管理员通过物理链路的分布，已无法快速识别业务路径。在这种情况下，需要采用仿真计算的方式，将网络上的配置、拓扑等集中到仿真软件中，计算出业务的预期路径。

预期建立之后，采用OSS软件定期获取路径的现状并与预期对比的方式，若不一致即发送告警，并提示管理员网络发生了故障。中小型、简单网络可以采用TraceRt获取路径。大型、复杂网络一般都会存在ECMP（Equal-Cost MultiPath等价多路径），此类情况一般可以综合TraceRt、转发表查询等方式来详细判断业务流的路径。另一种方式是通过分析IGP的泛洪报文，掌握路径建立的详细过程，根据路由算法和配置来掌握转发路径。

转发预期和检测

在转发平面上，预期的建立和检测非常密切，按照实现方式的不同，可以分为三种情况：非业务随路检测、业务随路检测和业务分析。

第一种是非业务随路检测。简单地说，就是自行定义预期，在网络上注入OAM检测报文。由于接收方已预先掌握了检测报文的大小、时间间隔等特征，当收到的报文不符合自行定义的预期特征时，即是发生故障。

这种方式的优点是容易获取和实施，网络各层面均有OAM检测协议可以使用，如BFD、EthOAM、ICMP Ping、MPLS OAM等，缺点是OAM检测报文特征与业务流量特征不完全一致，可能会出现检测未发现问题，但实际业务却发生了问题的情况。

第二种方式是业务随路检测，直接对业务流进行度量，典型代表是ITU-T Y.1731标准中定义的丢包统计功能，其原理简单地说就是“包守恒”，体现在以下的公式：

$$\text{接收报文数量} = \text{发送报文数量}$$

具体实现上，发送方和接受方都对业务流进行计数统计，发送方定时将计数发送到接收方，由接收方进行核对，核对出错即是故障发生。

第三种是业务分析。这种方式度量业务数据，并和预定义的标准阈值进行对比，如针对IPTV业务，采用专用硬件挂载在设备端口上，直接度量网络上IPTV流量的vMOS值等业务指标。这种方式需要采用DPI等方式，对实际业务报文进行采样统计或深度解析，按照业务已经定义的预期，分析其是否出现问题。该方式的优点是真实，缺点是设备部署和维护的成本高。

这三种方式不是非此即彼的关系，需要根据业务SLA目标，综合采购、维护成本等因素进行考虑和选择。

另外，控制平面和转发平面是互相有影响的，控制平面的运行直接影响转发平面的流量分布，可能会导致设备、链路的拥塞、故障等。因此，华为将控制平面与转发平面的预期建立和现状检测进行了综合与叠加，提供“路径+流量”的IP可视化方案，提供全面的故障监控和定位能力。

针对告警多的问题，华为在与中国移动的告警优化的合作中，通过对告警定义、告警级别的梳理，使城域网的日故障工单下降了50倍，每天的告警工单数量从500余条下降到10条左右，大大降低了工单处理的工作量。针对无告警的问题，如链路误码、链路闪断、器件失效和路由错误等常见疑难故障，以往需要几小时，甚至是几天时间才能排查，通过华为IP可视化方案，内部测试已经可做到分钟级的故障定位，该方案正在一些运营商网络上进行试点运行，已经取得一定成效，为帮助运营商降低维护难度，有效缩短故障恢复时长夯实了基础。**H**

责任编辑：陈雨虹 chyhong@huawei.com

