

基于生成树及网桥协议防护的气象网络优化

马 园, 邸永强, 曹 波*

陕西省气象信息中心系统网络科, 陕西 西安

收稿日期: 2025年4月23日; 录用日期: 2025年5月22日; 发布日期: 2025年5月30日

摘 要

在网络规模持续扩张、架构愈发复杂的当下, 网络环路引发的故障严重威胁着网络的稳定运行与高效传输。本文对一次典型的网络环路故障展开深度分析, 在定位和解决故障的过程中, 借助实际案例全面阐述了MSTP协议与BPDU防护机制的综合运用, 并给出了避免网络环路的多融合处理方法。

关键词

网络环路, 多生成树协议(MSTP), BPDU防护, 根防护

Based on Spanning Tree and Bridge Protocol Protection Meteorological Network Optimization

Yuan Ma, Yongqiang Di, Bo Cao*

System & Network Division of Shaanxi Meteorological Information Center, Xi'an Shaanxi

Received: Apr. 23rd, 2025; accepted: May 22nd, 2025; published: May 30th, 2025

Abstract

In the current context of continuously expanding network scale and increasingly complex architecture, network loop-induced failures pose a serious threat to the stable operation and efficient transmission of networks. This paper conducts an in-depth analysis of a typical network loop failure. During the process of locating and resolving the fault, the comprehensive application of the MSTP protocol and BPDU protection mechanism is thoroughly explained through an actual case. Additionally, a multi-integrated approach to avoiding network loops is presented.

*通讯作者。

文章引用: 马园, 邸永强, 曹波. 基于生成树及网桥协议防护的气象网络优化[J]. 计算机科学与应用, 2025, 15(5): 718-722. DOI: 10.12677/csa.2025.155143

Keywords

Network Loop, Multiple Spanning Tree Protocol (MSTP), BPDU Protection, Root Protection

Copyright © 2025 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
<http://creativecommons.org/licenses/by/4.0/>



1. 引言

随着气象业务快速发展和信息化水平的不断提高，省局网络规模持续扩大，网络应用也在不断地增加。保障省局气象网络平稳运行是办公和业务稳定运行的基本需求，也是网络运维人员的重要职责。在日常运维过程中，我们发现引起网络故障的原因有很多，其中网络环路是一种较为常见的问题。近期，省局发生的一次网络故障，就是由于省局下属某单位网络环路引发了局部故障，进而导致应用层出现了各种异常表现形式。

2. 网络故障实例分析

2.1. 故障现象

部分主机网络出现闪断，网速忽快忽慢，且即使连通网络，网速也慢，访问办公网站困难，严重影响办公效率。现场查看发现该单位所属 10.172.*网段部分电脑无法 ping 通网管，即使可以 ping 通网关，延迟也很高且丢包严重，网速很慢。该现象反复出现。

2.2. 用户拓扑结构

某单位网络结构是由核心层和接入层组成，接入层交换机通过双链路上联核心交换机。为了提高网络稳定性，采用了冗余设计，接入交换机采用 IRF 技术，两台物理交换机虚拟为一台设备。由于历史原因，该单位内部各办公室网络布线接入点数量偏少，为了适应业务发展，将打印机、复印机和无线路由等设备接入网络，因此在接入交换机下又级联了部分不可管理交换机，下连各终端设备，实现单位内部网络互通互联。如图 1 所示为该单位的网络拓扑图：

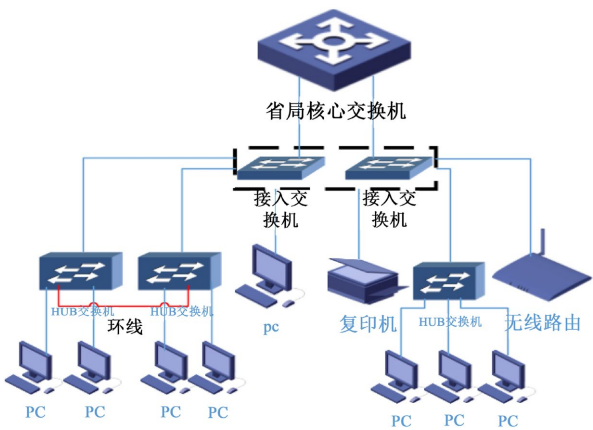


Figure 1. Network topology diagram
图 1. 网络拓扑图

2.3. 故障排查和原因分析

对网络中断的电脑进行检查,打开单位内部 OA 系统,发现速度非常慢, ping 网关时断时通,网络丢包严重。继续通过接入交换机排查,通过管理口登陆交换机后,在全局模式下使用“display counters rate outbound interface”命令查看,发现有端口广播报文平均发送速率明显高于正常值,记录异常端口,此时怀疑下连网络存在环路。继续使用“STP enable”指令启用生成树协议,阻断网络环路,恢复网络运行。开启 STP 协议后,继续在交换机上输入“display stp brief”命令,查看命令输出结果,发现记录的端口显示为“disable”(禁用状态),此时该单位反馈网络恢复正常。找到端口对应的办公室,检查物理连线,发现存在接线错误,存在两台不可管理交换机互联的情况(见图 1 中的红色连线)。经了解,用户错误地将连接在不可管理交换机上的一根网线当作电脑端线路接入了新增加的交换机中。拔除多余网线后,登录交换机查看端口显示为“forwarding”,进入转发状态,该办公室网络环路消除后,网络应用也恢复正常。综上所述,此次故障是由于不可管理交换机环路导致的网络故障,进而引发了网络广播风暴,导致网络卡顿、网速慢等一系列故障。

3. 网络环路原理

网络环路主要分为两类,一类是常见的二层网络的交换环路,这也是本次网络故障的原因[1]。二层网络交换环路通常是存在冗余链路,会造成报文多帧复制,数据量以 2 的 N 次方指数级增长,形成局域网内部广播风暴,同时 MAC 地址表不断自动更新学习,造成数据包丢失,导致网络拥堵和中断。还有一类是三层网络的路由环路,是由于数据包在网络中循环转发而无法到达目的地,导致数据包无限循环转发,从而引发网络故障,这种故障主要是由于路由器配置不当引起的。

4. 网络环路故障预防

本次故障确定由网络环路原因造成后,定位到连接错误的网线,将其断开,网络恢复正常。并在接入层交换机上启用了生成树协议,防止局部环路造成整网故障。由于该单位接入核心的方式采用了双机虚拟化冗余模式,虽然提高了网络抗风险能力,但是比起单一链路来说,冗余链路的存在就有可能会发生网络环路。为了避免后续仍出现网络环路问题,减少广播风暴和生成树重置,采取了以下三种方式融合来优化网络配置。

4.1. 启用多生成树协议(MSTP)

STP(生成树协议)是数据链路层的通信协议,可以自动检测并阻塞可能形成环路的冗余链路,确保只有无环的路径处于活跃状态,从而避免环路的产生[2]。当任意一交换机到达根网桥有两条或者两条以上的链路时,生成树协议会根据算法将其中一条切断,保证任意两个交换机之间只有一条单一的活动链路。当网络拓扑发生变化时,STP 树也会自动发生相应改变,避免广播风暴,MAC 地址表的震荡。STP 树的生成过程包括:比较桥 ID 选举根桥,确定根桥和指定端口,阻塞备用端口。如图 2 所示为 STP 树生成过程:

STP 通过构造一颗无环树来消除交换网络中的环路,但是收敛速度慢,通常需要 30~50 秒完成拓扑收敛。不能提供负载均衡,所有流量都是通过一棵树在传输。

RSTP(快速生成树协议)是 STP 的改进,通过优化端口角色和状态,减少了对定时器的依赖,加快收敛速度。但是仍然是单树结构。

MSTP(多生成树协议)是生成树协议的扩展,兼容 STP 和 RSTP,结合了 STP 的稳定性和 RSTP 的快速收敛性。核心优势在于能够快速响应网络拓扑图变化,收敛速度通常在 1~5 秒内完成。支持多实例生

成树, 可将多个 VLAN 映射到不同的生成树中, 实现 VLAN 间的流量负载均衡。网络中可以有多条冗余路径, 当某条路径发生故障时, MSTP 可以自行切换到其他线路, 确保网络连通性。

气象网络具有高实时性要求、多业务流量和高可靠性特点, 且该单位采用双机虚拟化冗余模式, 综上所述通过对比不同 STP 算法的优缺点, 结合气象网络特点, 最终采用 MSTP 对气象网络进行优化配置。当发生故障时, MSTP 的快速收敛能力确保了迅速切换到备用路径, 减少气象数据传输中断事件。省局下属有多个事业单位, 划分不同 VLAN, MSTP 可以根据 VLAN 需求将流量分配到不同的生成树实例中, 避免某些链路过载, 提高网络整体性能。

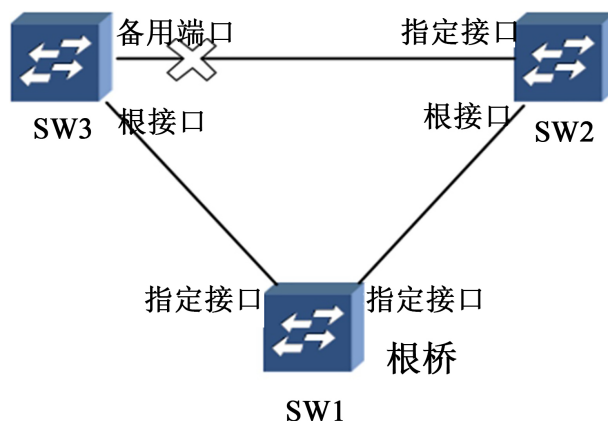


Figure 2. STP tree generation process

图 2. STP 树生成过程

4.2. 开启网桥协议(BPDU)防护

针对用户反应的网络闪断情况, 查询交换机运行日志发现有端口在短时间内不断 up 和 down, 导致网络拓扑发生变化, 进而使交换机 ARP 表格更新重置, 用户端的反映就是网络闪断。当网络中存在大量 ARP 请求时, 导致设备 CPU 占用率较高, 出现用户掉线、频繁断网、上网慢、业务中断或无法上网等现象。详情日志可见下图 3。

```
%Oct 12 13:45:44:963 2024 Leida-65.106 LLDP/6/LLDP_DELETE_NEIGHBOR: Neighbor deleted on Port GigabitEthernet1/0/23 (Ifindex 9437206), Chassis ID is 6c0b-84e2-1e60, Port ID is 6c0b-84e2-1e60.
%Oct 12 13:45:44:997 2024 Leida-65.106 LLDP/6/LLDP_CREATE_NEIGHBOR: New neighbor created on Port GigabitEthernet1/0/23 (Ifindex 9437206), Chassis ID is 6c0b-84e2-1e60, Port ID is 6c0b-84e2-1e60.
%Oct 12 13:47:53:014 2024 Leida-65.106 ARP/4/RATELIMIT: The ARP packet rate(103pps) exceeded the rate limit(100pps) on interface GigabitEthernet1/0/6 in the last 60 seconds.
%Oct 12 13:52:00:534 2024 Leida-65.106 MSTP/6/MSTP_NOTIFIED_TC: Instance 0's port Bridge-Aggregation6 was notified of a topology change.
%Oct 12 13:52:01:241 2024 Leida-65.106 MSTP/6/MSTP_NOTIFIED_TC: Instance 0's port Bridge-Aggregation6 was notified of a topology change.
%Oct 12 13:52:20:071 2024 Leida-65.106 ARP/4/RATELIMIT: -Slot=2; The ARP packet rate(117pps) exceeded the rate limit (100pps) on interface GigabitEthernet2/0/48 in the last 60 seconds.
%Oct 12 13:52:53:011 2024 Leida-65.106 ARP/4/RATELIMIT: The ARP packet rate(652pps) exceeded the rate limit(100pps) on interface Ten-GigabitEthernet1/0/52 in the last 60 seconds.
```

Figure 3. Access switch log

图 3. 接入交换机日志

运行 STP 协议的交换机会互相交换 STP 协议帧, 这些协议帧的荷载数据被称为 BPDU (网桥协议数据单元)。STP 的各种选举是根据交换 BPDU 消息来实现的[3]。边缘端口直接与用户终端相连, 正常是不

参与生成树计算的, 如果错误接入交换机会立即发送 BPDU 消息, 使得边缘端口变成非边缘端口, 开始参与生成树计算[2][3]。如上图所示, 端口状态发生变化后, 产生了 BPDU 消息后, 触发了生成树重新计算, G1/0/23 端口上邻居关系被删除重建, ARP 数据包速率超过限制, ARP 重置, 拓扑发生改变, 网络出现闪断情况。

在二层网络中开启生成树协议时, 为防护 MSTP 生成树的安全, 一般在边缘端口上配置 BPDU 保护功能, 避免边缘端口受到 BPDU 报文攻击导致网络拓扑改变及业务流量中断, 从而提高交换网络的可靠性和安全性。要在交换机的边缘端口上开启 BPDU 防护, 当受防护端口接收到 BPDU 信息, 受防护端口会立即做出反应, 使端口进入 shutdown 或者 errdisable 状态。

4.3. 开启根防护

受办公大楼物理布线的限制, 原有网络接入点较少。随着办公人员和各种网络设备增加, 现有网口接入点数量不足, 因此管理员未禁止用户自行接入交换机。根据 STP 协议, 生成树选举根桥时, 一般根桥交换机为局域网核心交换机, 新接入的交换机有可能拥有最低的网桥 ID 并成为根桥交换机, 从而导致网络拓扑发生改变[4]。因此, 为了杜绝用户新接入交换机成为根桥, 在接入核心交换机对应端口上配置根防护, 执行“spanning-tree guard root”命令来启用根防护, 确保核心交换机一直是根桥, 避免由于根桥选举变化导致的拓扑改变, 进而造成网络故障[5]。

采用以上技术融合对交换机进行配置后发现网络性能明显优化。对应应用效果进行分析: 主机都能连网且网速正常, 无网络闪断情况, 现场 ping 各服务, 无丢包和大的网络延迟[6]。登录接入交换机查看日志, 没有 BPDU 报错, 说明网络中没有环路, 查看交换机上联端口流量也恢复正常, 链路通信率明显降低。

5. 讨论

网络环路是常见的网络故障之一, 通过本次网络故障处理表明, 基于 MSTP 及 BPDU 防护技术可以有效消除环路对网络的影响, 根防护避免用户新接入交换机对网络拓扑的影响。多技术融合实现了整体气象网络优化。后续日常工作人员也要注意网络连接规范和标准配置, 确保网络的平稳运行[7]。

参考文献

- [1] 陶海祥, 张上, 章健. 浅谈校园网网络环路故障的处理及预防[J]. 长江信息通信, 2024, 37(5): 178-181.
- [2] 宋艳, 刘悦先, 王爽, 等. 基于交换网中的 STP 生成树协议的实验设计与验证[J]. 网络安全和信息化, 2024(3): 101-104.
- [3] 刘叶梅, 徐龙泉. 生成树协议操纵攻击及其应对安全策略研究与实现[J]. 现代计算机, 2022, 28(22): 118-120.
- [4] 谢胜盈. 交换机生成树安全[J]. 网络安全和信息化, 2018(2): 112-113.
- [5] 刘台, 赵瑞峰, 向灯, 等. 网络交换机 STP 算法研究与实现[J]. 信息与电脑(理论版), 2022, 34(15): 211-214.
- [6] 曹波, 邸永强, 王垒, 等. 基于策略路由的气象广域网优化[J]. 陕西气象, 2017(6): 35-38.
- [7] 燕东渭. 基于省市气象骨干网络的带宽管理设计[J]. 陕西气象, 2013(1): 34-36.