An Investigation into the Application of Spanning Tree Protocol (STP) for Loop Prevention and Control in Switched Networks

Ping Zhang

Institute of Electronic Science, China Electronics Technology Group Corporation, Beijing 100041, China

Abstract

In the construction of enterprise campus and campus local area networks (LANs), physical redundant links are ubiquitously deployed in network design to enhance network operational reliability. However, the coexistence of multiple links is highly prone to inducing Layer 2 switching loops, which in turn trigger failures such as broadcast storms, MAC address table flapping, and frame duplication. In severe cases, such issues can lead to full network paralysis, presenting a persistent and thorny challenge in LAN operation and maintenance. As a foundational protocol for loop prevention and control at the data link layer, the Spanning Tree Protocol (STP) automatically elects root bridges, root ports, and designated ports through the exchange of Bridge Protocol Data Units (BPDUs) between switches. By logically blocking redundant ports while retaining physical backup links, STP constructs a loop-free tree topology. This paper starts by examining the formation mechanisms and hazards of loops in switched networks, expounds the operational principles of STP, and compares the differences among three generations of spanning tree technologies—STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). Drawing on engineering practice, it analyzes practical limitations in STP deployment, including slow convergence, topology flapping, and malicious BPDU attacks. Targeted strategies for configuration optimization, security hardening, and operation and maintenance management are proposed, along with reference deployment schemes for typical scenarios, providing actionable technical insights for loop risk prevention and control in LANs.

Keywords

spanning tree protocol; STP; layer 2 loop; switched network; redundant link; network operation and maintenance

生成树协议STP在交换网络环路问题中的防控应用探究

张平

中国电子科技集团有限公司电子科学研究院，中国·北京 100041

摘要

在企业园区、校园局域网建设过程中，为提升网络运行可靠性，组网设计普遍部署物理冗余链路。但多条链路并存极易产生二层交换环路，继而诱发广播风暴、MAC 地址表震荡、帧重复复制等故障，严重时可造成全网瘫痪，是局域网运维中较为棘手的常见问题。生成树协议 STP 作为数据链路层环路防控的基础协议，依靠交换机之间交互 BPDU 报文完成根桥、根端口、指定端口的自动选举，通过逻辑阻塞冗余端口，在保留物理备份链路的前提下构建无环路树形拓扑。本文从交换网络环路形成危害入手，阐述 STP 协议运行原理，对比 STP、RSTP、MSTP 三代生成树技术差异，结合工程实践分析 STP 在部署时存在的收敛缓慢、拓扑抖动、恶意 BPDU 攻击等现实短板，提出针对性配置优化、安全加固与运维管控策略，并给出典型场景下的部署参考方案，为局域网环路风险防控提供可落地的技术思路。

关键词

生成树协议；STP；二层环路；交换网络；冗余链路；网络运维

1 引言

随着局域网业务不断丰富，视频监控、办公系统、物联网终端等业务对网络连续运行能力提出更高要求。网络设计人员通常增加多条物理链路作为备份，一旦主链路断开，备用链路能够快速承接业务，避免单点故障。很多基层组网人员只考虑链路备份，却忽略二层环路风险，当两条及以上链路同时连通时，广播帧会在环路内无限循环扩散，短时间内带宽资源被广播流量占满，终端出现卡顿、掉线现象。

以往传统的环路防控手段大多依靠人工布线管控，通过减少冗余链路规避环路，这种方式牺牲了网络可靠性，一旦单条链路损坏，网络直接中断。生成树协议 STP 技术出现之后，很好地平衡了冗余备份与环路抑制两大需求，成为交换网络必不可少的基础配置。但在实际工程当中，不少运维人员仅简单开启

【作者简介】张平（1979-），男，高级工程师，从事通信系统与网络、传感器网络及IMS技术研究。

STP 默认配置，没有结合网络规模进行根桥手动规划、边缘端口设置以及安全防护，由此出现网络收敛时间过长、拓扑频繁震荡、外来设备接入引发环路等问题。基于上述工程痛点，有必要深入梳理 STP 运行逻辑，总结实践层面的优化办法，提升交换网络整体稳定性。

2 二层交换环路产生机理及带来的危害

以太网交换机本身没有路由计数机制，对于广播帧、未知单播帧采取泛洪转发模式。当两台或多台交换机之间存在两条互通链路，就构成二层物理环路。环路形成后主要产生三类典型故障。

第一，广播风暴。广播报文沿着环路不停循环转发，流量呈指数级增长，交换机 CPU 与带宽资源被大量消耗，设备负载持续走高，最终造成网络卡顿甚至断网。第二，MAC 地址表不稳定。同一个终端发出的数据帧会从不同端口到达交换机，交换机 MAC 地址表会反复刷新端口记录，地址表频繁震荡，造成单播转发异常。第三，多帧复制。目的设备会多次收到相同的数据帧，上层业务出现数据包重复，引发应用层程序报错、视频画面卡顿等现象。

环路故障具备突发性特点，往往施工布线、后期增加交换机、用户私接家用路由都可能意外形成环路，故障排查难度较大，因此必须依靠自动化协议手段进行环路预防，而不是单纯依靠人工管理布线。

表1 二层交换环路引发的主要故障及表现

故障类型	故障现象	对网络业务的影响
广播风暴	广播报文循环泛洪，网络带宽被占满	全网终端卡顿、丢包，严重时全网瘫痪
MAC 地址表震荡	同一 MAC 地址在不同端口反复学习刷新	单播流量转发错误，数据包丢失
多帧复制	接收端重复收到相同数据帧	业务程序报错、视频画面花屏、数据异常

3 STP 协议基本运行原理

STP 即生成树协议，标准定义为 IEEE 802.1D，其核心思路是利用 STA 生成树算法，把存在物理环路的网络修剪成逻辑上无环的树形网络。交换机之间依靠 BPDU 桥协议数据单元交互拓扑信息，BPDU 报文内包含桥 ID、根路径开销、端口 ID、协议计时器等关键参数，所有交换机依据报文信息完成角色选举。

第一步选举根桥。桥 ID 由桥优先级与交换机 MAC 地址组成，全网桥 ID 数值最小的交换机成为根桥，是整个生成树拓扑的逻辑核心。工程实践中不能依靠设备出厂默认值自动选举，若由接入层低端交换机意外成为根桥，会造成转发路径不合理，因此必须手动将核心交换机设置为主根桥，汇聚交换机设置为备用根桥。

第二步选举根端口。除根桥以外每一台交换机选出唯一的根端口，也就是到达根桥路径开销最小的端口，根端口状态为转发状态。

第三步选举指定端口。每一条物理链路上选出一个指定端口，负责该网段的数据转发，端口同样处于转发状态。

第四步剩余非指定端口进入阻塞状态。阻塞端口可以接收 BPDU 报文用来监控拓扑，但不会转发业务数据，以此切断逻辑环路。

当网络中某一条链路发生断开，交换机接收不到对应 BPDU 报文，STP 将重新计算拓扑，原本阻塞的端口经过计时器延时后切换至转发状态，启用备份链路完成业务切换。传统 STP 默认收敛时间达到 30-50 s，较长的收敛时间对于实时业务并不友好，由此行业后续推出 RSTP 快速生成树与 MSTP 多生成树协议作为升级方案。

RSTP 在 STP 基础上优化端口角色与协商机制，收敛时间缩短至数秒；MSTP 则可以划分多个生成树实例，不同 VLAN 运行独立生成树，能够实现链路负载均衡，目前中大型园区网络普遍优先采用 MSTP 部署，向下兼容传统 STP 设备。

4 STP 实际部署过程中的常见问题

虽然 STP 能够实现环路自动阻断，但仅开启默认配置会暴露出不少短板，结合大量局域网运维案例，主要问题分为四个方面。

第一，收敛时间过长引发业务中断。标准 STP 依靠计时器完成端口状态迁移，网络拓扑变更后需要等待 30 s以上端口才能开始转发数据，对于视频监控、工业控制这类实时性业务，长时间收敛会造成业务断流。部分运维人员为加快收敛随意修改计时器参数，参数改动不当又会诱发临时环路，带来更大风险。

第二，根桥位置混乱，转发路径不合理。网络设备出厂时桥优先级全部一致，此时依靠 MAC 地址大小选举根桥，接入层交换机有可能抢占根桥角色，数据流量需要跨多层设备转发，网络时延增加，核心链路流量压力不均衡。

表2 STP、RSTP、MSTP 技术对比

协议	标准	收敛时间	端口角色	核心特点	适用场景
STP	IEEE 802.1D	30-50 s	根端口、指定端口、阻塞端口	构建单一生成树，兼容老旧交换机	小型简单局域网
RSTP	IEEE 802.1w	1-3 s	根端口、指定端口、替代端口、备份端口	快速收敛，增加边缘端口机制	中小型园区网络
MSTP	IEEE 802.1s	1-3 s	继承 RSTP 端口角色，支持多实例	多生成树实例，实现 VLAN 负载分担	大型企业、校园网络

第三，边缘接入端口引发拓扑震荡。接入交换机连接电脑、打印机等终端的端口属于边缘端口，这类端口插拔网线时端口状态反复变化，每一次变化都会触发 STP 重新计算全网拓扑，频繁的拓扑变动造成整个网络抖动卡顿。很多组网人员没有将接入终端端口配置为边缘端口，导致网络长期不稳定。

第四，STP 本身存在安全漏洞，易遭受人为干扰。外来人员私自接入一台交换机，若该设备桥 ID 更小，就有可能抢夺根桥地位，强行改变全网生成树拓扑；恶意设备发送伪造 BPDU 报文同样能够打乱原有网络结构，人为制造环路故障，普通 STP 没有自带安全防护能力。

5 基于 STP 的环路防控优化实施策略

针对上述工程问题，可以从规划、配置、安全加固、运维管理四个维度优化 STP 部署方案，充分发挥协议环路防控价值。

第一，提前做好拓扑规划，手动指定主备根桥。组网前期梳理网络层级，将性能最高的核心交换机配置为主根桥，一台汇聚交换机作为备用根桥，通过调低桥优先级固定角色，杜绝接入层设备意外成为根桥，保证流量转发路径最优。同时根据链路带宽合理配置路径开销，千兆链路、万兆链路设置不同开销值，引导流量按照规划路径转发。

第二，合理配置边缘端口，减少不必要的拓扑变更。所有直接连接电脑、摄像头的接入端口开启边缘端口功能，边缘端口启用后端口直接进入转发状态，端口启停不会触发全网拓扑计算。同时配套开启 BPDU 防护，一旦边缘端口收到 BPDU 报文，系统自动关闭该端口，防止私接交换机带来环路风险。

第三，根据业务场景选择合适生成树版本。小型简单办公网络使用基础 STP 即可；对业务连续性有一定要求的中小型园区网络选用 RSTP；拥有大量 VLAN、需要链路负载均衡的大型校园、企业网络优先部署 MSTP，把不同业务 VLAN 映射到不同生成树实例，让多条冗余链路同时分担流量，提升带宽利用率。不建议随意修改协议默认计时器，确需调整收敛参数必须经过仿真测试后再上线。

第四，完善后期运维与监测手段。在网管平台开启 STP 拓扑告警，当网络发生根桥变更、端口状态切换时及时推送告警信息，运维人员第一时间排查故障；做好设备配置备份，每一台交换机留存 STP 配置文档；定期巡检布线情况，严禁随意私接交换机、家用路由。对于高安全等级网络，还可以部署环路检测工具作为 STP 之外的补充防护，双重降低环路故障概率。

6 结语

二层交换环路是局域网运维中危害极大的典型故障，STP 生成树协议作为环路防控的主流技术，能够在保留物理冗余链路的前提下实现逻辑环路阻断，兼顾网络可靠性与稳定性。但协议本身只是一套技术工具，单纯开启默认配置远远达不到理想的防控效果。网络技术人员需要充分理解 STP、RSTP、MSTP 三者的差异，在组网阶段提前规划根桥角色，合理设置边缘端口与安全防护功能，结合网管监测手段形成一套完整的环路防控方案。

在物联网、智慧园区不断发展的背景下，局域网设备数量持续增长，网络结构日趋复杂，二层环路风险依旧长期存在。未来在传统生成树技术基础上，还可以结合智能化网络运维平台、SDN 技术进一步优化环路检测能力，持续降低环路故障发生概率，保障交换网络长期平稳运行。

参考文献

[1] 刘东旭，马亚琦。生成树协议 (STP) 在计算机网络中的应用 [J]. 电脑知识与技术，2020,16 (02):28-29.

[2] 吴树，李瑞霞。基于 Packet Tracer 的快速生成树协议研究与仿真实现 [J]. 黑龙江工业学院学报 (综合版),2020,20 (03):94-100.

[3] 温钰，龚尚福，王照峰。三层交换环境下生成树协议的应用研究 [J]. 网络安全技术与应用，2008 (02):48-49.

[4] 金诗谱。基于 ENSP 的 RSTP 可靠网络配置技术研究 [J]. 数字技术与应用，2024,42 (03):134-136.