基于路由交换配置的局域网安全防护体系构建

沈澍
中冶华天工程技术有限公司，江苏 南京 210000
DOI: 10.61369/TACS.2026060054

摘　　要： 在数字化办公环境和信息化业务不断发展的大背景之下，局域网作为关键基础设施，其起到数据传输、业务支撑的作用。网络架构中的重要部分就是路由交换机，其安全配置好坏直接影响到整个网络系统的安全防护水平。本文以路由交换技术应用场景为基础，结合中小型局域网实际运行情况，给出相应的对策建议，建立适合中小局域网的网络安全防护方案，希望能够加强网络整体安全性和稳定性，给中小型局域网的安全运维赋予了关键的技术支撑和操作参照。
关 键 词： 路由交换配置；局域网安全；防护体系构建

Construction of a Local Area Network Security Protection System Based on Routing and Switching Configuration

Shen Shu
China Metallurgical Huatian Engineering Technology Co., Ltd., Nanjing, Jiangsu 210000

Abstract: In the context of the continuous development of digital office environment and informationized business, the local area network, as a key infrastructure, plays the role of data transmission and business support. The important part of the network architecture is the routing switch, and the quality of its security configuration directly affects the security protection level of the entire network system. Based on the application scenarios of routing and switching technology and combined with the actual operation situation of small and medium-sized local area networks, this paper provides corresponding countermeasures and suggestions, and establishes a network security protection scheme suitable for small and medium-sized local area networks, hoping to enhance the overall security and stability of the network and provide key technical support and operational references for the safe operation and maintenance of small and medium-sized local area networks.
Keywords: routing and switching configuration; local area network security; construction of protection system

新兴技术物联网、大数据被大量使用之后，使得局域网接入设备数量大幅度上升，而网络架构也因此变得更加繁杂。目前，网络安全威胁正处在多样化、常态化、智能化的发展阶段，传统的局域网安全防护方式已经不能适应要求了。路由交换设备是局域网内完成数据传输和访问控制的关键点，它起到数据转发、子网划分、流量调度等主要作用，并且是构建网络安全体系的防线。通过对它底层的配置策略进行调整，既可以很好地抵御各种常规网络攻击，又能明显改善防御的整体效果。本文主要针对路由交换设备的配置优化来创建一体化的安全防护体系，以填补目前的安全防护技术上的不足，保证局域网业务正常运转。

一、基于路由交换配置的局域网安全防护研究意义

（一）夯实局域网底层安全架构

路由交换设备是局域网的中枢神经，它要承担数据包的转发任务、对终端进行准入控制以及不同子网之间数据交换的工作。安全配置状况决定着局域网底层防护能力的好坏。相比于独立部署的安全组件来说，依靠细致的管理来对路由交换设备实施控制，能够对网络内部的数据流实施精准的指引，对逻辑区域加以有效的划分，并且可以合理地安排访问权限，进而大幅削减因非法连接或者异常流量而产生的风险[1]。

（二）降低网络安全运维成本

众多的中小型企业由于资金、技术和人力资源等方面的限制，很难配备高水准的网络安全防护设备，过分依靠第三方的安全产品会加大维护成本。采用改进的路由交换机技术进行安全策略的部署，一方面可以防止新加入到系统中来的硬件设备，另一方面依靠 VLAN 的分层、访问控制列表（ACL）、端口监视、

作者简介：沈澍（1988—），男，回族，安徽马鞍山人，本科，助理工程师，研究方向为计算机网络及安全。

 Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.

协议加密等基本的设置项，达到较好的网络安全。这样一种方案可以大大降低硬件采购以及长期维护的费用，简化网络管理的程序，缩短由于故障或者威胁而进行的技术排查所需要的时间和人力投入，从而减轻人工维护的负担和由此造成的经济损失[2]。

（三）防范多元化网络安全风险

目前局域网存在的主要安全威胁有 ARP 欺骗、端口扫描、非法设备接入、跨子网攻击等，大多通过路由和交换设备配置上的薄弱之处来执行。传统的防御方式大多采取事后监控或者被动防护的方式，在面对低层网络攻击的时候存在着明显的不足。相比端口映射、动态 ARP 认证、流量特征检测和增强路由协议安全等技术路线，在检测出异常流量之后可以实现对网络的全面隔离，切断非法的终端与网络的连接，并将所有类型的攻击源都排除在网络的保护范围之外，在大大增强了局域网抵御威胁的能力的时候，也大幅缩减了由于恶意数据传输或者设备问题引发的数据泄露、业务中断以及关键服务不可用的现象出现的机会[3]。

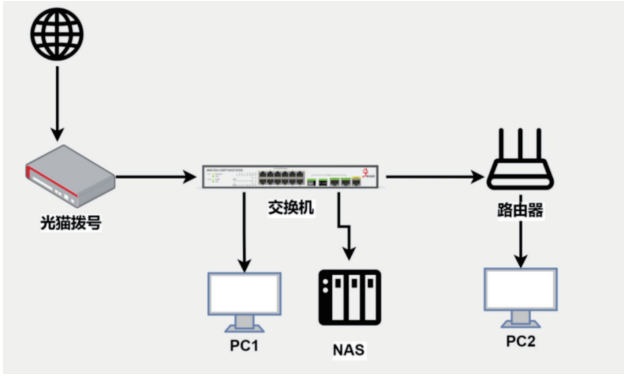

图 1 路由器连接情况

二、基于路由交换配置的局域网安全防护核心策略

（一）设备基础安全加固配置

就目前而言，对路由器交换设备基础配置的脆弱性加以全面系统化并且加以规范化的技术改进措施还远远不够[4]。从设备运维的角度来讲，要重点加强账号权限管理的机制，先清除出厂默认的账号，创建单独的安全管理员账号，并使用高强度的加密算法生成唯一的密码，然后根据不同的职责分工来设置不同的层次的访问权限，即管理员、操作员、普通用户等不同的用户角色，禁止任何一种身份的匿名登录或者越级登录的行为。另外需要建立完善的远程控制系统安全策略，采取把 Console 端口限制住、设置 Telnet 超时检测以及用 SSH 密钥认证来增强安全性的措施。硬件资源冗余的应有之义是全面缩减，将闲路的物理接口全部关闭并标示禁用标志，清除掉非核心业务所依赖的 IP 组播转发、HTTP 简易界面显示这些功能模块，从而大幅度降低被利用的可能性。网络边界处还要实行严格的端口准入控制措施，用 MAC 地址绑定规则和最大并发连接数限制策略来实时监测异常流量的变化趋势，及时做出应对。创建起完整的日志记录和分析体系，包含操作系统日志、用户交互日志以及流量审计报表等各个方面的数据，可以实现本地保存和云平台同步存取的功能，并且能够长久地保存重要的信息，为事件的追溯以及事后处理给予充分的支撑。根据上面的方案可以有效地提高现有的网络架构的安全性[5]。

（二）优化网络隔离与访问控制策略

本研究设计出一个层次化的网络安全防护体系，用子网细分加多级访问控制的方式对网络横向扩展的风险进行了遏制，又防止了非法的跨域访问行为的发生。本方案适合企业或者校园局域网的实际情况下进行部署使用，主要目的是建立一个分层隔离的安全架构。根据组织结构、职能划分以及信息安全的要求，使用虚拟局域网（VLAN）技术对企业的内网进行精细重组：办公终端、研发设备、核心服务器和访客区都被划入了各自独立的逻辑分区，而不再使用以前的单一广播域的方式，大大减少了由于单点故障造成的安全风险。在完成 VLAN 的配置之后，用三层交换机和路由器配合使用基于访问控制列表（ACL）的安全策略，设置来源地址、目的地址、端口信息、协议类型等参数来监控高危端口的通信活动，重点封锁常用的攻击端口（135、139、445 等），实时阻止可疑威胁数据包，阻拦蠕虫流传扩散，远程探测侵入，恶意代码嵌入等行为。对不同的 VLAN 之间进行交互操作时要按照权限管理规则执行，只开放已经验证过的核心业务流通道，其他的非授权跨网段连接都被禁止。为了增强局域网内的安全性，在接入层加入动态 ARP 监测、MAC/IP 绑定、DHCP 日志分析等安全配置项，对局域网内所有协议的报文行为进行全方位的分析，可以及时找到并消除 ARP 中毒攻击以及其它虚假 IP 注册的现象。

（三）完善运维审计与应急防护机制

为了提高路由交换设备安全防护的效能，急需创建起系统化的、标准化的运维管理机制，并将其嵌入到日常的运营中去。应该逐渐抛弃传统的被动式管理方式，转变为一种以主动防御为战略的安全治理模式。首先要对常规的周巡检、月度系统检查、季度综合评价等重要环节进行优化。这些操作可以及时发现配置错误、端口状态异常、流量波动、软件版本安全风险等，用固件更新等方式消除潜在的威胁。还要建立动态的风险评估和应对措施调整机制。还需要建立统一的日志管理系统来整合全局范围内路由表的变化记录、设备命令执行日志、告警事件等各个方面的数据，利用大数据分析技术来准确发现可能存在的非法入侵企图、大规模扫描活动、违规操作等可疑信号，并且能够做到迅速定位和有效处置。参数变更权限要严格控制，任何影响路由或者交换功能的修改操作都要经过审批并产生详细的日志，保存原文件副本作为备份依据；还要编制 DDoS 攻击、中间人篡改、恶意代码注入等常见威胁的应急预案，规定预警规则、应急响应步骤和恢复措施，细化团队协作分工，全面提高突发事件应对能力。应当有规律地开展专业训练和技术演习，对已有的防护手段予以检验并加以改良改良，进而塑造起一套包含从初次布置，持续观察直至事后分析总结等各个环节的完备防护体系运营管理机制，以此提升局域网的安全防护水平以及运行稳固程度。创建常态化的路由交换设备运维体系，需要从设备安全巡检、参数调整、漏洞排查等多方面着手，依靠固件升级和加强防护的方式，实现主动规避风险的目的。设计一体化的日志审计平台，将设备运行日志、

Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.

流量分析、告警信息等各方面数据综合起来，可以达到对网络态势进行实时监测、预警的目的。制定全方位的网络安全应急响应预案，就服务中断、数据泄露、攻击事件等情形制订出具体的处理程序，而且要确定好各方面的责任划分。

表1 局域网路由交换安全防护配置对比表

防护维度	传统配置模式	优化后安全配置模式	防护效果
设备账号安全	沿用默认账号密码，无权限管控	修改默认账号、高强度密码、权限分级、登录锁定	杜绝暴力破解、非法登录设备后台
网络网段隔离	无 VLAN 划分，全网同一广播域	按业务划分 VLAN，配置 ACL 跨域管控	阻断风险横向扩散，实现网段安全隔离
终端接入管控	端口无限制，任意终端可接入	MAC 绑定、端口安全、DAI 检测	防范非法终端接入、ARP 欺骗攻击
运维审计	无日志记录，无巡检机制	全量日志记录、定期巡检、配置备份	支持攻击溯源、故障快速排查

（四）路由协议安全加固配置

路由协议是局域网和广域网中的主要数据传输和路径选择技术，一旦路由协议有安全漏洞，在实际运用过程中很容易被攻击者利用进行恶意操作，比如路由劫持、路径篡改以及伪造攻击等等。从上述研究中可知，改善主流动态路由协议安全性能，就是改善整个网络的安全性。目前，RIP（Routed Information Protocol）和 OSPF（Open Shortest Path First）等传统协议仍被广泛部署于各类网络环境中，但由于缺乏完善的身份验证与数据完整性保护机制，在特定条件下可能遭受非法操纵。攻击者可以利用在路由信息中插入虚假的路由、修改现有的路由表项或者发送伪造的报文等方法来破坏正常的通信过程，进而造成网络的不稳定以及信息安全保证能力的降低。为了克服以上问题，需要对现有的动态路由进行系统性的改善，即在 RIP、OSPF 等协议中加入基于 MD5或者 SHA-2家族哈希函数的安全加密认证机制，只让合法的邻居节点之间传输加密的信息，另外还可以通过路由毒化防护、垂直分层控制、毒性逆转修正等功能模块来进一步降低由于配置错误或者硬件故障造成的拓扑震荡风险。还要对异常的外部数据包进入关键路由数据库加以限制，用防火墙规则对可能的威胁信号进行筛选。对在老式终端设备上运行着的多余的辅助服务程序应当及时关掉或者删掉。创建出多维协同的防护机制，对局部入侵造成的影响可以很好地控制事态的扩散范围，也可以减小损害的程度。

三、结语

在数字化转型过程当中，局域网成了企业内部开展业务合作、信息流转的主要枢纽，在提升运作效率，保证数据安全方面起着无法代替的作用。路由交换设备属于局域网架构里的关键部分，其初始配置优化对于创建底层网络安全体系有着十分重要的意义，相较于传统依靠静态防火墙达成被动防御的模式而言，此种办法表现出更为灵活且经济的特点。本文针对目前局域网中路由交换机配置存在的安全漏洞问题，从硬件加强、访问权限控制、运维管理三个角度提出了系统的改进方法，以达到全方位防御非法入侵、横向扩散、参数篡改等常见安全风险的目的。

参考文献

[1] 李江华，胡桂银，闻顺杰 . " 路由交换技术 " 课程教学改革的思考和研究 [J]. 铜陵职业技术学院学报 ,2022,21(01):91-94.

[2] 张跃 . 路由交换技术在教学应用中的研究 [J]. 电子制作 ,2022,30(02):42-44.

[3] 柳兵 . 小型 RapidIO 交换网络的设计及路由配置方法 [J]. 电子世界 ,2021,(15):137-139.

[4] 赵姣，杨珂 . 一种 PCIE 交换芯片交换管控方法 [J]. 中国集成电路 ,2020,29(Z4):62-67+84.

[5] 杜春立 . 探究式教学模式在网络专业教学中的应用——以 " 跨交换机的 VLAN 配置与管理 " 教学为例 [J]. 中国管理信息化 ,2020,23(13):233-235.

 Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.