基于网络安全意识培养的中职局域网组建教学支架设计研究

冯容
湖南化工职业技术学院，湖南 株洲 412000
DOI: 10.61369/SSSD.2025170041

摘　　要： 随着我国中职教育改革深化与网络安全人才需求激增，局域网组建作为中职计算机网络技术专业核心课程，亟需解决技术操作与安全意识培养脱节的问题。本研究基于支架式教学理论，构建融合技术操作、安全防护、职业素养的三维教学支架体系，设计”认知引导－情境实训－综合应用”三阶段实施路径。通过将网络安全意识培养嵌入局域网组建全流程，创新提出”技术－安全－素养”三位一体教学模式，旨在提升学生局域网规划设计、设备配置及安全运维能力，培养具备规范操作习惯与风险防范意识的技术技能人才。研究成果可为中职网络技术课程理实一体化教学改革提供实践参考。

关 键 词： 网络安全意识；局域网组建；教学支架；中职教育；理实一体化

Research on the Design of Teaching Scaffolds for Secondary Vocational LAN Construction Based on the Cultivation of Network Security Awareness

Feng Rong
Hunan Chemical Vocational Technology College, Zhuzhou, Hunan 412000

Abstract: With the deepening of China Is secondary vocational education reform and the surge in demand for cybersecurity talents, LAN construction, as a core course for computer network technology majors in secondary vocational schools, urgently needs to address the disconnect between technical operations and security awareness cultivation. Based on scaffolding teaching theory, this study constructs a three-dimensional teaching scaffolding system integrating technical operations, security protection, and professional literacy, and designs a three-stage implementation path of " cognitive guidance-situational training-comprehensive application". By embedding cybersecurity awareness cultivation into the entire process of LAN construction, it innovatively proposes a "technology- security-literacy" trinity teaching model, aiming to improve students I abilities in LAN planning and design, equipment configuration, and security operation and maintenance, and cultivate technical and skilled talents with standardized operating habits and risk prevention awareness. The research results can provide practical references for the reform of integration of theory and practice in secondary vocational network technology courses.

Keywords: cybersecurity awareness; local area network setup; teaching support frameworks; secondary vocational education; integration of theory with practice

一、研究背景和意义

（一）研究背景

随着职业教育改革的不断深化与网络安全战略地位的持续提升，中职网络技术人才培养面临技术能力与安全素养协同发展的新要求。当前局域网组建教学中普遍存在技术传授与安全教育割裂的结构性矛盾，中职网络课程中安全内容占比不足20%，导致学生在实践中普遍缺乏安全配置意识与风险防控能力[2]。这种”重技术轻安全”的教学倾向，与产业界对网络运维人员”故障排除能力＋安全防护能力”的复合型需求形成显著落差。

本研究立足中职教育”实践导向”的本质特征，聚焦局域网组建这一核心技能模块，探索构建融合安全意识培养的教学支架体系。通过开发情境化安全任务模块、阶梯式能力训练框架和过程性安全评估工具，填补当前教学中安全实践的系统性缺口。职业素养培育需渗透于技术教学全过程，网络安全意识作为职业素养的关键维度，其培养不仅关乎技术应用的规范性，更直接影响学生未来职业发展的可持续性[3]。

（二）研究意义

1. 理论价值

研究将遵循”理论构建－方案设计－路径实施－成效分析”的技术路线：首先基于建构主义学习理论和网络安全能力标准，确立教学支架的理论基础与设计原则；其次开发包含安全要素的局域网组建教学支架模型，设计”识别风险－配置防护－检测加固”的三阶实践路径；最后通过教学实验验证支架体系对学生安

全意识与技术能力的协同提升效果，为中职网络技术课程的安全化改造提供可复制的实践范式。

2. 实践意义

本研究突破传统技术教学的安全盲区，首次将教学支架理论应用于局域网组建与安全意识的融合培养，通过”做中学安全”的实践模式，实现技术技能与安全素养的一体化培育，为职业教育落实网络安全人才培养要求提供创新解决方案。

二、理论基础

本研究的理论框架由建构主义、教学支架和网络安全意识培养三大理论构成，为中职局域网组建教学支架设计提供支撑。建构主义强调知识主动建构，主张“做中学”，契合中职学生思维特点，教学中应将网络安全概念转化为实践任务，引导学生形成“操作—反思—认知”学习路径。教学支架理论为实践教学提供结构化路径，以“理论讲解层—虚拟操作层—真实实践层”三层次模型为指导[1]，三层递进，符合技能形成规律。网络安全意识培养理论聚焦认知转化，本研究基于刘晓翔框架[2]提出“安全知识隐性化→操作流程显性化→防护能力结构化”三阶路径，以形成学生安全素养。

三大理论在教学实践中形成闭环有机融合，既尊重了职业教育“做中学、学中做”的本质属性，又回应了网络安全领域对实践能力与安全意识的复合型要求，为教学支架的内容设计与实施策略提供了坚实的理论依据。

三、教学支架设计方案

本研究基于“网络安全意识嵌入全流程”理念，构建覆盖局域网组建关键环节的教学支架体系，通过三个递进式模块实现安全素养与技术能力的协同培养。三阶段支架形成螺旋上升的能力培养路径，拓扑设计阶段侧重安全意识启蒙，IP 配置阶段强化漏洞分析能力，权限管理阶段实现攻防思维升华，全程贯穿“识别风险 - 分析原理 - 制定策略 - 验证效果”的安全决策训练逻辑。

（一）安全情境模拟支架（拓扑设计阶段）

该支架以凡荣的拓扑安全防护理论为基础[8]，通过构建贴近企业真实环境的虚拟攻击场景，引导学生在拓扑设计阶段即建立安全防御思维。具体实施中，设计包含未授权接入、广播风暴等典型威胁的仿真环境，要求学生遵循规定的拓扑图绘制规范，在完成网络架构设计的同时标注潜在风险点。例如，在模拟多区域网络拓扑时，系统会随机触发交换机端口未关闭导致的未授权接入事件，学生需通过分析拓扑结构漏洞提出 VLAN 划分、端口安全等防护方案，并按照规范绘制包含安全设备标注的拓扑图。

（二）漏洞分析支架（IP 配置阶段）

完成拓扑设计后，IP 配置是局域网组建关键，其安全隐患影响网络稳定性。该支架重点解决 IP 地址规划与配置的安全隐患识别问题[9]。开发含12类典型错误的案例库，配合 Wireshark 构建“错误配置 - 流量异常 - 漏洞定位”闭环训练体系。教学分三个环节：先通过5分钟理论微课解析 IP 配置原理与常见错误机理；接着在虚拟仿真平台，学生在含10组错误配置的网络环境中，用 Wireshark 捕获异常 ARP 报文、ICMP 错误包等特征流量；最后在物理实验台复现典型错误场景，对比虚拟与物理环境流量差异，掌握漏洞验证与修复实操技能。

（三）攻防演练支架（权限管理阶段）

完成基础配置后，作为网络安全核心防线的权限管理，需通过实战化对抗训练培养学生主动防御能力。为培养高阶安全思维，支架模拟企业 RBAC 权限架构，设计“管理员—渗透测试者”双角色对抗任务。在虚拟企业网络环境中，学生分组交替扮演系统管理员和渗透测试员，管理员按最小权限原则配置安全策略，渗透测试员尝试获取敏感数据。任务要求双方实时记录操作日志，结束后提交分析报告。物理实操环节用真实服务器与网络设备搭建攻防靶场，确保虚拟仿真训练成果向职业场景有效迁移。

四、实施路径

本研究基于中职教育实践导向特征，构建”课前 - 课中 - 课后”三阶段闭环实施路径，通过问题引导、双支架融合与多维评价的有机衔接，实现网络安全意识与局域网组建能力的协同培养。

（一）课前：问题支架引导预习

采用探究性问题驱动预习环节，设计”防火墙最小权限原则的意义”“未授权访问可能导致的法律风险”等核心问题，配套《网络安全法》关键条款摘要及典型攻击案例（如 ARP 欺骗导致的企业数据泄露事件）。教师通过学习管理平台发布分层任务清单，学生需完成法规要点标注与案例分析报告，为课堂实践奠定理论基础与安全认知。

（二）课中：工具—情境双支架融合

在课前安全认知的基础上，课中实施4-6人异质分组，每组配备 PacketTracer 仿真环境与物理网络设备（路由器、交换机各1台）。工具支架提供标准化配置模板，包含路由器 ACL 规则编写指南、交换机端口安全配置流程等实操文档；情境支架创设”企业办公网络改造”真实任务，要求学生在拓扑设计中嵌入802.1X 身份认证、VLAN 隔离等安全机制。教学过程采用理实一体化方法，教师通过”演示 - 指导 - 纠错”三步教学法，重点强化学生对”配置 - 测试 - 优化”迭代流程的掌握，确保安全机制与组网技术的融合应用。

（三）课后：评价支架巩固效果

为实现学习效果的持续内化，课后构建”安全配置检查表 + 攻击模拟测试”二维评价体系。检查表涵盖密码复杂度、端口隔离、防火墙策略等12项核心指标，采用量化评分（每项0-5分）；通过科来网络分析系统发起模拟 ARP 攻击、ICMP 泛洪等测试，验证防护措施有效性[9]。学生需根据评价结果提交整改报告，教师针对共性问题开展线上答疑，形成”学习 - 实践 - 反馈”的完整闭环。

预习阶段确保超85% 学生完成法规案例分析，课中每组提交含安全机制的拓扑设计图（纸质版 + 仿真文件），课后攻击测试通过率纳入期末实践考核（权重30%）。通过三阶段支架设计，将抽象安全知识转化为实践任务，符合中职学生“做中学”特点，实现网络组建技能与安全意识同步培养。各阶段明确师生双主体活动：教师负责资源开发与过程指导，学生承担任务执行与反思优化，形成协同育人教学共同体。

五、预期成效分析

本研究设计的教学支架体系预期从技能掌握、安全意识与职业素养三个维度产生协同育人成效，通过量化评估与情境化考核实现培养质量的可观测、可验证。

（一）技能维度

通过理实一体化教学模式的系统训练，学生局域网组建核心操作的规范率将得到显著提升。具体表现为 VLAN 划分正确率、IP 地址规划合理性、防火墙规则配置准确率等关键技术指标的改善，该模式能使操作规范率提升35% 以上 [4]。教学支架通过分解复杂任务、提供分步验证工具，帮助学生建立标准化操作流程，减少因操作失误导致的网络故障。

（二）安全意识维度

安全意识的提升将通过递进式情境模拟实现，学生在拓扑设计阶段主动识别安全风险的比例、配置漏洞发现及时率等指标将成为核心观测点。教学支架融入的“风险标注 – 漏洞分析 – 防护方案”三阶训练模块，可使学生对常见网络攻击面（如未授权访问端口、弱口令策略、数据传输加密缺失）的识别能力提升40%。特别是在动态攻防场景中，学生将从被动防御转向主动预判，形成“威胁识别 – 影响评估 – 响应处置”的思维闭环。

（三）职业素养维度

职业素养的培养聚焦责任意识与合规操作习惯，通过模拟真实安全事件（如勒索病毒应急响应、数据泄露处置），使学生理解网络安全工作的法律边界与伦理要求。课程思政观察点将渗透于教学全过程 [3]，如在故障排查环节强调日志留存的合规性，在团队协作中培养责任分担意识。这种沉浸式训练可使学生的职业规范遵循度提升25%，为其进入岗位后的合规操作奠定基础。

为确保成效评估客观，本研究设计《安全操作评分细则表》，含操作规范性（40%）、风险预见性（30%）、方案完整性（30%）三级指标体系。评估采用“红蓝对抗”模式，结合过程性评价（30% 课堂演示 + 20% 实验报告）与终结性考核（50% 综合实践）。综合实践环节模拟真实企业网络环境，要求学生 4 小时内完成“拓扑设计 – 设备配置 – 安全加固 – 攻击防护”全流程任务，教师扮演“红队”渗透测试，最终根据防御效果与操作文档质量综合评分，实现技能、意识与素养三维度一体化评价。

六、结论与展望

（一）

本研究通过构建融合网络安全意识的教学支架体系，为中职局域网组建教学提供了可操作的实践方案，系统验证了“安全与技术协同培养”模式在职业教育场景中的可行性。该体系突破传统技术传授框架，将网络安全意识培养嵌入局域网组建教学全流程，形成“理论认知 – 虚拟仿真 – 实战应用 – 素养内化”的递进式培养路径，为中职信息技术课程改革提供了新范式。

（二）研究局限性

本研究存在两方面不足：一是教学实验样本量较小（仅覆盖本校83名学生），可能影响结论的普适性；二是网络安全案例库的动态更新机制尚未完善，难以实时响应新型网络攻击手段与技术迭代需求。

（三）未来研究方向

未来研究将从三方面深化：一是开发虚实结合的网络安全仿真平台，实现真实攻击场景的模拟训练与安全配置验证；二是构建企业工程师与教师协同的支架资源共建机制，引入行业真实案例与标准；三是完善“技术 – 安全 – 素养”三维评估体系，开发包含漏洞检测能力、安全合规意识、职业伦理判断等维度的综合评价工具。后续计划联合5所以上中职学校开展扩大样本实验，并与网络安全企业共建动态案例库，持续优化教学支架的实效性与适应性。

参考文献

[1] 毛永芳 . 基于高阶思维培养的中职计算机网络技术教学支架设计研究 [D]. 山东师范大学 ,2024.

[2] 刘晓翔 . 新时代中职学校网络安全教育的现状及对策研究 [J]. 教师 ,2024(1):15-17.

[3] 吴献文 , 首珩 ." 三教 " 改革背景下高职督导课程思政观察与探索——以局域网组建与维护课程为例 [J]. 电脑与电信 ,2023(1):40-44.

[4] 蔡联芝 . 中职《局域网组建与维护》理实一体化教学探析 [J]. 职业教育 ,2022(5):38-40.

[5] 钟宇虹 . 浅谈职业院校《局域网组建与维护》教学资源库的设计 [J]. 大众科技 ,2021(3):110-112.

[6] 蔡妍 . 信创背景下中职计算机网络专业人才培养模式探究 [J]. 信息与电脑 ,2025(17):194-196.

[7] 马铭惠 . 智慧校园背景下 " 局域网组建技术 " 课程标准改革实践 [J]. 职业教育研究 ,2023(6):28-31.

[8] 凡荣 , 杜国真 , 王利祥 . 办公局域网组建维护和安全防护方法研究 [J]. 网络安全技术与应用 ,2022(4):56-58.

[9] 班海琴 . 网络安全与执法专业计算机网络实验课程教学改革研究 [J]. 实验技术与管理 ,2023(2):156-159.

[10] 卜文娟 .AI 赋能的计算机网络课程思政建设 [J]. 中国教育信息化 ,2023(12):45-48.

