

(一) 课程简介

课程名称：网络系统建设与运维 课程性质：专业核心课
教学目标：

- 知识目标：掌握 ACL 的定义、分类（标准 ACL、扩展 ACL）及配置方法。
- 能力目标：能通过华为 eNSP 模拟器实现网络流量控制与安全策略部署。
- 思政目标：培养网络安全法律意识、科技创新责任感及工匠精神。

(二) 案例主题

主题名称：从“ACL 网络流量控制”看技术合规与国家安全 对应教学单元：访问控制列表（ACL）的配置与应用

(三) 设计意图

- 价值引领：通过国产网络安全产品（如华为防火墙）案例，增强技术自立信念。
- 责任教育：结合《网络安全法》等法规，强调 ACL 配置的合法性与伦理责任。
- 实践导向：以企业真实场景（如数据防泄漏）为驱动，培养职业素养与问题解决能力。

(四) 结合点分析

教学内容	思政元素	结合方式
ACL 分类与标准 ACL 配置	资源分配公平性	对比中美 IPv4 地址资源分配差异（中国 0.45 个/人 vs 美国 5.3 个/人），反思技术霸权
扩展 ACL 细粒度控制	科技创新与工匠精神	分析华为 ACLv6 技术在 IPv6 部署中的突

教学内容	思政元素	结合方式
		破，体现国产技术从“跟随”到“引领”的跨越
ACL 防御 DDoS 攻击案例	网络安全与法律合规	引入《网络安全法》第 21 条，模拟“某高校因 ACL 配置疏漏导致网络瘫痪”事件
ACL 规则优化与性能考量	精益求精的职业态度	通过华为工程师优化国家级金融网络 ACL 规则的真实故事，强化“代码即责任”理念

（五）案例描述

1. 思政目标确定

- **核心目标：**理解 ACL 技术对国家关键信息基础设施的保护作用，树立“技术向善”理念。
- **支撑目标：**培养合规操作习惯（如 ACL 规则优先级排序）、系统性安全思维（全局流量控制）。

2. 教学内容选取

- **理论重点：**
 - ACL 工作原理（基于五元组的流量过滤）
 - 标准 ACL 与扩展 ACL 的适用场景对比
- **实践任务：**
 - **实验 1：**在 eNSP 中配置标准 ACL，限制特定 IP 访问财务服务器。

- **实验 2:** 配置扩展 ACL 阻断恶意端口（如 TCP 23）并启用日志记录。

3. 教学策略设计

- **混合式教学流程:**

- **课前:**
 - 学生调研“中国网络安全企业全球市场份额”（如天融信、深信服排名）。
 - 观看纪录片《中国网络安全保卫战》中 ACL 技术应用片段
- **课中:**
 - ① **案例导入:**
 - 播放“某医院因 ACL 配置错误导致患者数据泄露”新闻视频
 - 分组讨论《网络安全等级保护基本要求》中 ACL 相关条款。
 - ② **技术实践:**
 - 配置标准 ACL（代码示例）：

```
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule deny source 192.168.1.0 0.0.0.255
[Huawei-GigabitEthernet0/0/1] traffic-filter inbound acl 2000
# 强调 ACL 末尾隐含 deny all 规则的法律风险
```
 - 配置扩展 ACL 防御 Telnet 攻击：

```
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule deny tcp source any destination any destination-port eq 23
[Huawei-GigabitEthernet0/0/0] traffic-filter inbound acl 3000
```
 - ③ **伦理思辨:** 辩论“便利性（全开放）vs 安全性（严格 ACL）”的平衡策略

- 课后：

撰写《ACL 配置对国家政务云安全的影响分析报告》，需引用《关键信息基础设施安全保护条例》。

4. 思政目标达成路径

- **情感共鸣：**讲述华为工程师在“护网行动”中通过 ACL 阻断境外攻击的实战经历。
- **行为引导：**在实验报告中增加“合规性检查表”，标注每条规则的法规依据（如《网络安全法》第 24 条）。

（六）案例反思

1. 实施要点与策略

- **虚实结合：**通过 eNSP 模拟国家级网络遭受 DDoS 攻击场景，演练 ACL 应急响应流程。
- **双师协同：**邀请企业工程师解析“某银行 ACL 配置失误导致千万损失”真实案例。

2. 难点与解决思路

- **难点：**学生易忽视 ACL 规则顺序的战略意义（如优先阻断高危 IP）。
- **对策：**引入“北斗导航系统地面站 ACL 部署”案例，说明规则优先级对国家安全的决定性作用

3. 目标达成情况

- **定量评估：**课后测试显示，89%的学生能正确引用法规解释 ACL 配置逻辑
- **质性反馈：**学生报告中普遍体现“国产技术替代”“数据主权保护”等社会责任关键词

4. 改进方向

- **增强实战性：**开发“ACL 攻防靶场”，模拟 APT 攻击中的流量过滤对抗。
- **拓展国际视野：**增加“一带一路”跨境光缆 ACL 部署案例，培养全球化网络安全责任感

通过本案例，学生既能掌握 ACL 核心技术原理，又能深刻理解网络安全技术的战略价值，实现“知识传授-技能训练-价值塑造”三位一体的教学目标。