5G校园专网安全接入研究

深圳大学 江魁

2023.11.28

目 录
CONTENTS

01 背景介绍

1.1 政策背景

- 2021年《政府工作报告》提出要“加大5G网络和千兆光网建设力度，丰富应用场景”。
- 工信部《十四五信息通信行业发展规划》:加快“5G+工业互联网”的融合创新和先导应用，推进5G在能源、交通运输、医疗、邮政快递等垂直行业开发利用与应用推广。促进5G行业虚拟专网规模化发展，全面提升5G应用和安全能力。
- 2021年7月5日，工业和信息化部、中央网络安全和信息化委员会办公室、国家发展和改革委员会、教育部等共十部门印发《**5G应用“扬帆”行动计划（2021-2023年）**》

其中提出:

—— 5G应用关键指标大幅提升。5G个人用户普及率超过40%，用户数超过5.6亿。5G网络接入流量占比超50%，5G网络使用效率明显提高。5G物联网终端用户数年均增长率超200%。

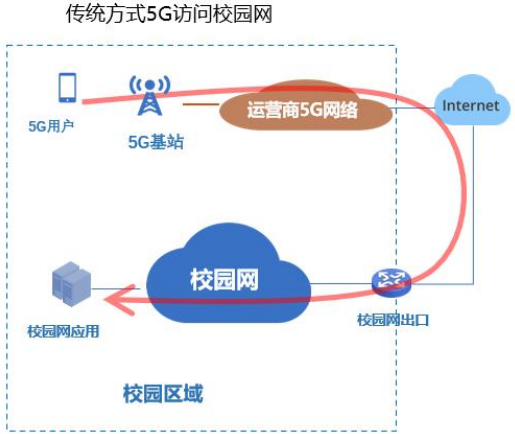
—— 5G+智慧教育。推动5G技术对教育专网的支撑，结合具体应用场景，研究制订网络、应用、终端等在线教育关键环节技术规范。加大5G在智慧课堂、全息教学、校园安防、教育管理、学生综合评价等场景的推广，提升教学、管理、科研、服务等各环节的信息化能力。

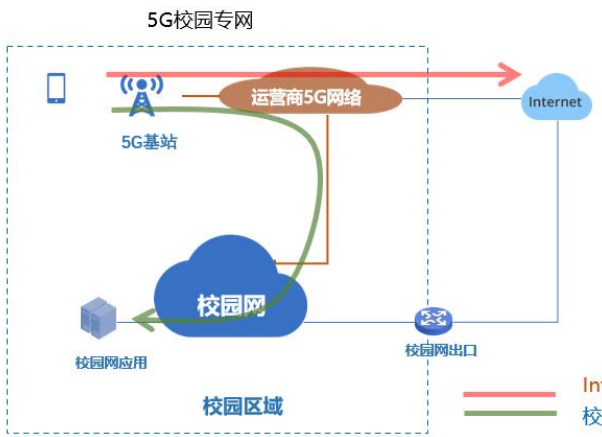
1.2 校园需求

传统校园网不足

1. 覆盖不全、带宽不足、设备管理复杂

2. 接入校园内网困难、易断开、需频繁切换





5G网络优势

高速率、低延迟、大容量、广覆盖、多连接。

传统5G访问不足

1. 校内访问需绕行，增加数据暴漏面

2. 无法充分发挥大带宽、多接入、低时延的优势

3. 占用校园网出口带宽，成本持续增加

4. 往往缺少定制化的网络服务

5G校园专网

02 5G校园专网

2.1 5G校园专网优点

5G校园专网是基于5G技术在校园范围内部署的专用网络，是5G专网和校园网的一次有机融合。这种网络可以提供高质量、 高可靠性和高安全性的网络服务。

覆盖广

传统网络难以覆盖校园各个区域，利用广覆盖的特点，拓展校内网的广度，为校内边缘地区提供高质量的网络服务

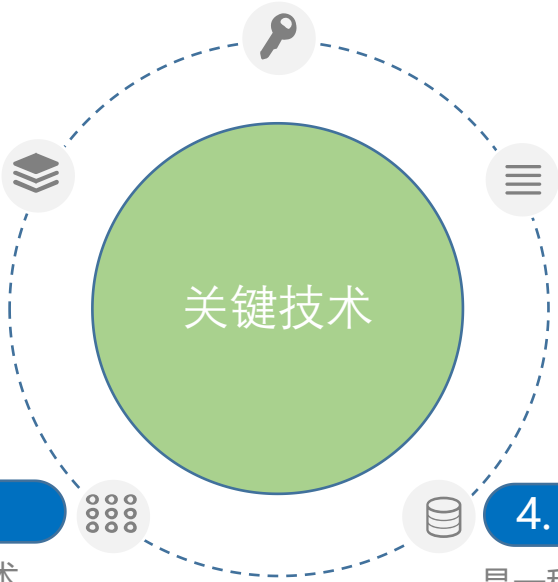
容量大、延迟低

有利于学校开展多元化、多媒体化的教育布局，实现教育方式的创新

拓展性强

更利于在学校边缘部署其他技术的应用，实现技术的融合与落地，如物联网、边缘计算等

2.2 关键技术



2. 安全与隐私保护

采用多种安全技术和机制，包括加密通信、身份认证、授权管理等

1. 虚拟化技术

一种资源管理技术，将实体资源抽象、转换后呈现出来，打破实体间的结构，资源更好地被利用，技术包括NFV和SDN等

3. 网络切片

将物理基础设施划分为多个逻辑上独立的虚拟网络段，可分为软切片和硬切片，虚拟化技术是网络切片的基础

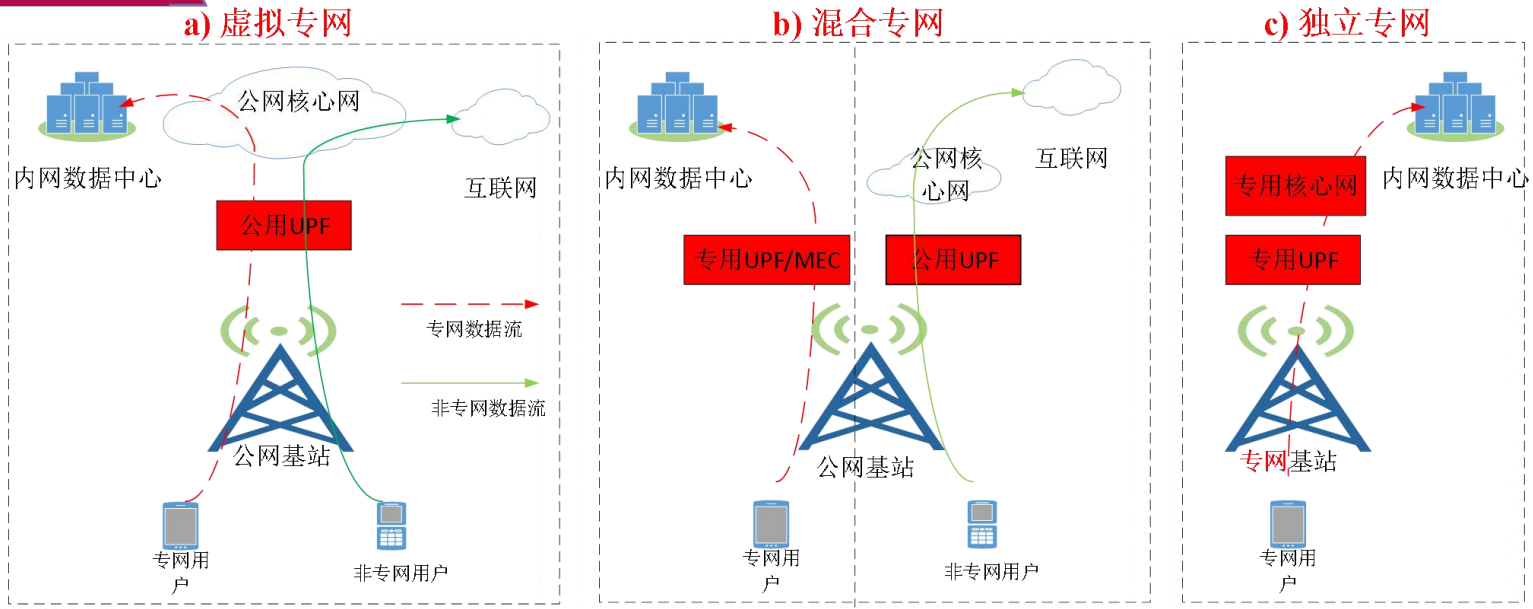
5. 其他技术

高频段传输、大规模MIMO、D2D技术、精确定位技术、异构网络、多接入技术等

4. 多接入边缘计算

是一种将计算、存储和网络资源推向网络边缘的计算模型，能将计算能力和服务面向用户侧，实现低延迟、 高带宽的边缘服务

2.3 组网方式



虚拟专网模式，通过网络切片技术切片，使用公有UPF分流，成本低但定制化能力较差

混合专网模式，通过网络切片技术切片，使用专用UPF分流，定制化能力较强但依赖UPF性能

独立专网模式，国家提供专用5G频段，自建5G专网，独立性、安全性强但成本极高

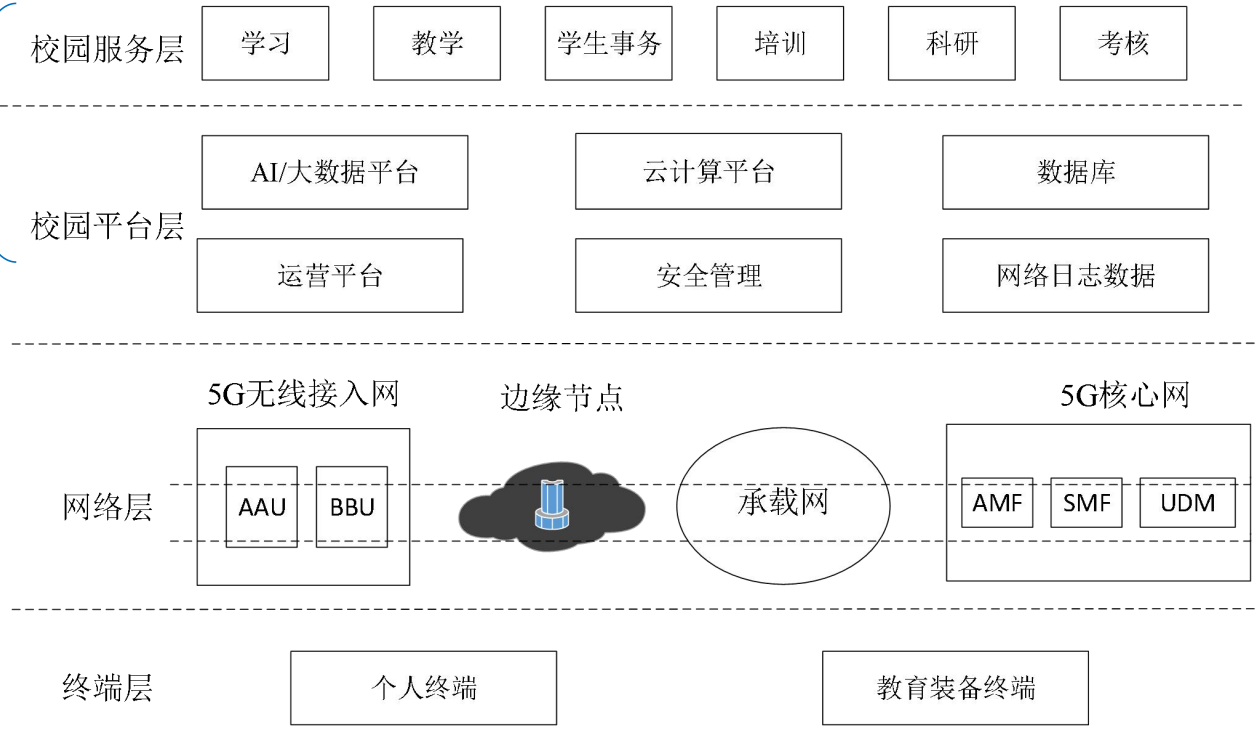
2.4 应用架构

服务层和平台层属于校园应用层面，**对外提供应用服务**

前提

校园侧应用安全

- 用户的安全可控接入
- 细颗粒度的授权管控



03 5G校园专网接入安全分析

3.1 5G校园专网安全风险

校园用户特点

基数大　分布广　流动性强　高敏感

1. 弱口令风险

帐号多、格式相对统一、且不倾向使用强密码策略，容易导致一账号泄露、多应用沦陷现象

2. 账号管理风险

校内业务系统间存在一定的独立性,在面对学生入学、毕业、退学、转校、教职工入职、离职等情况时，账号管理成本较大，无法实现各系统间流畅的联动和实时的账号管理

3. 权限管理风险

缺乏足够的、持续的用户权限管控，容易导致越权行为

4. 热点分享风险

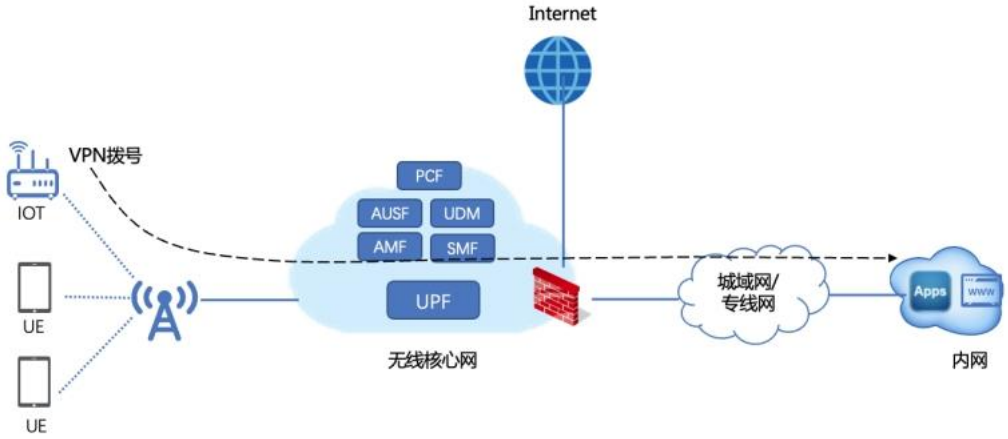
未授权的设备通过连接专网用户热点，可以将授权设备当作跳板，进而访问内网

3.2 安全接入方案分析

接入过程：主认证和二次认证

1. 主认证过程是指从终端到核心网的认证过程，需要借助AMF、SMF、AUSF、UDM等核心网网元，以及5G-AKA等认证机制完成

2. 二次认证(二次鉴权)是指垂直领域根据需求对用户进行的认证过程，通常需要结合AAA及上述网元实现



专网接入内网大多通过如下方式：

1. 运营商AAA和校园AAA对接

2. 终端使用VPN等软件或定制化登录平台拨入网关的方式

3. UPF分流并在UPF侧打通到内网路由的方式

3.2 安全接入方案分析

成本较高

二次认证过程需要借助AAA及部分网元完成，存在落地门槛

适配度低

终端要安装专用的客户端程序，或定制化登录平台，输入账号密码信息才能接入内网，减低用户适配度和体验感

暴露风险

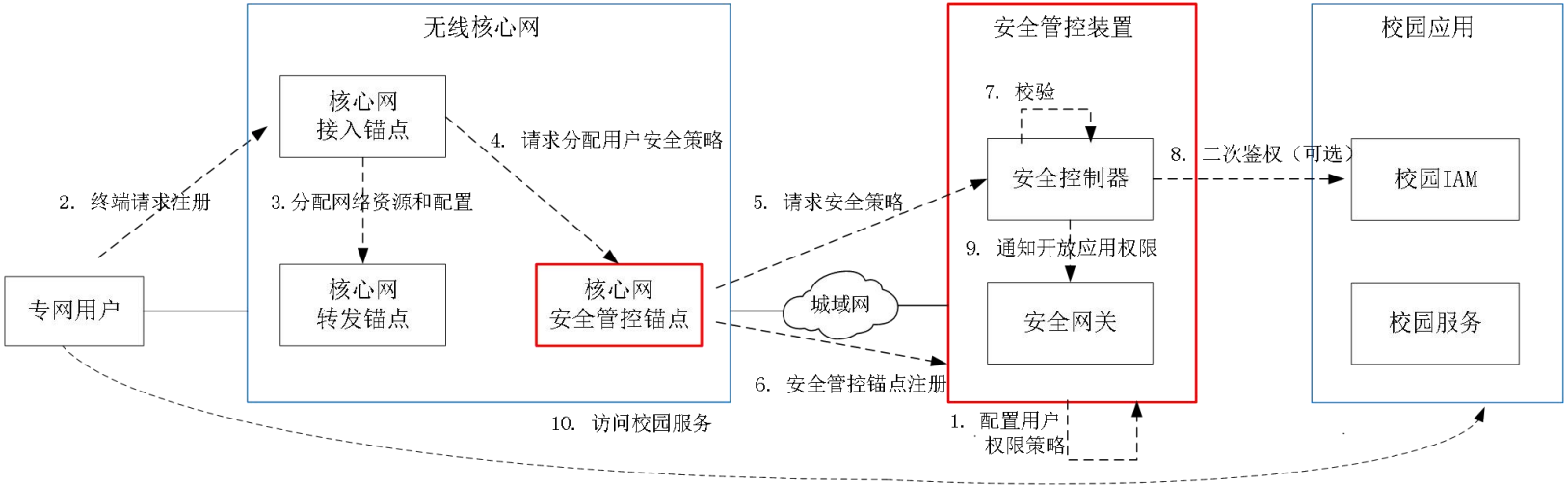
终端接入后，即可连通全部的内网应用，内网存在端口双向暴露风险和越权风险

缺乏管控

无法实现基于用户身份+应用基本细颗粒度严格授权管控，存在较大的网络安全风险

04 安全接入和授权管控方案

4.1 方案框架

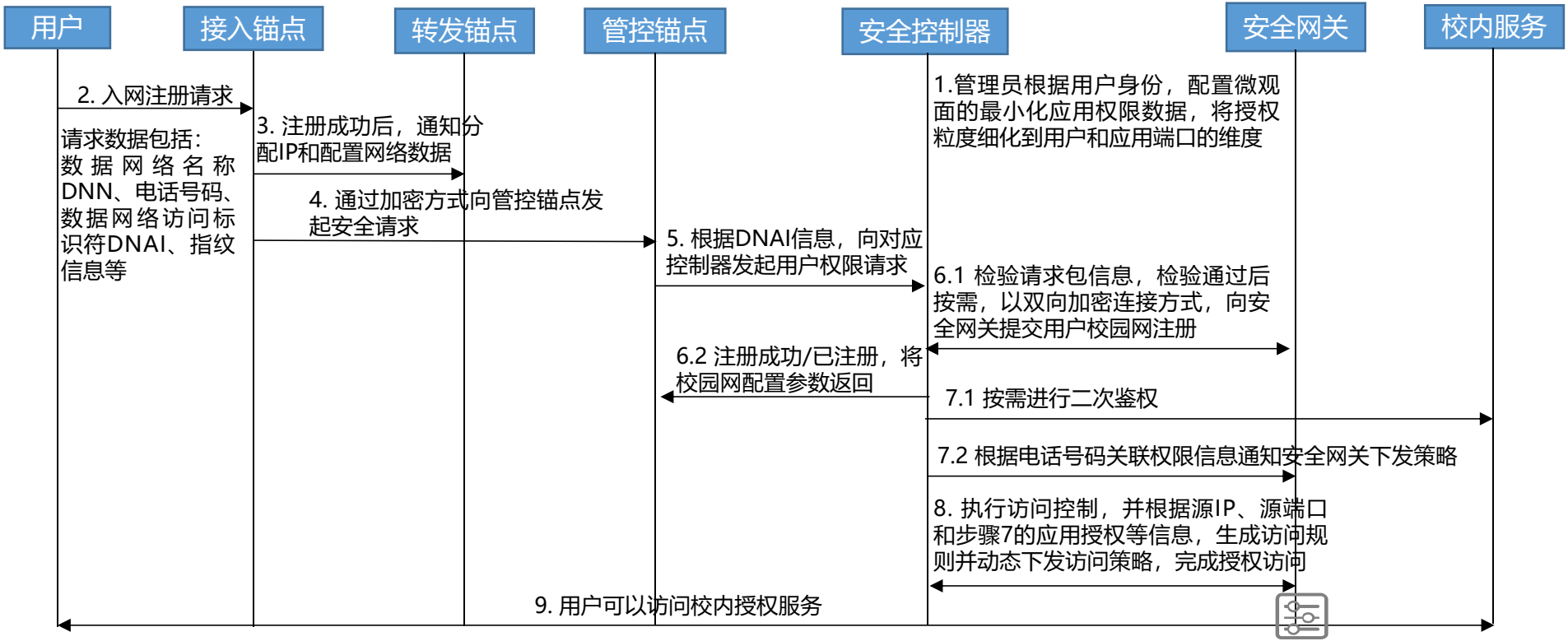


安全管控锚点：负责响应专网用户的安全策略(即应用权限)请求

安全管控控制器：核心控制模块，负责处理来自专网用户的应用权限请求和访问策略下发

安全管控网关：安全策略执行模块，动态处理来自安全管控锚点的加密连接请求，下放策略，并执行专网用户访问应用的安全访问控制

4.2 业务流程


用户
接入锚点
转发锚点
管控锚点
安全控制器
安全网关
校内服务
2. 入网注册请求
请求数据包括：数据网络名称DNN、电话号码、数据网络访问标识符DNAI、指纹信息等
3. 注册成功后，通知分配IP和配置网络数据
4. 通过加密方式向管控锚点发起安全请求
5. 根据DNAI信息，向对应控制器发起用户权限请求
1.管理员根据用户身份，配置微观面的最小化应用权限数据，将授权粒度细化到用户和应用端口的维度
6.1 检验请求包信息，检验通过后按需，以双向加密连接方式，向安全网关提交用户校园网注册
6.2 注册成功/已注册，将校园网配置参数返回
7.1 按需进行二次鉴权
7.2 根据电话号码关联权限信息通知安全网关下发策略
8. 执行访问控制，并根据源IP、源端口和步骤7的应用授权等信息，生成访问规则并动态下发访问策略，完成授权访问
9. 用户可以访问校内授权服务

4.3 方案应用

在实际应用中，可进一步结合零信任网关，构造校园无感零信任安全接入和管控系统

签约

校园网5G手机用户订购/签约套餐后，加入校园网的5G专网

分流

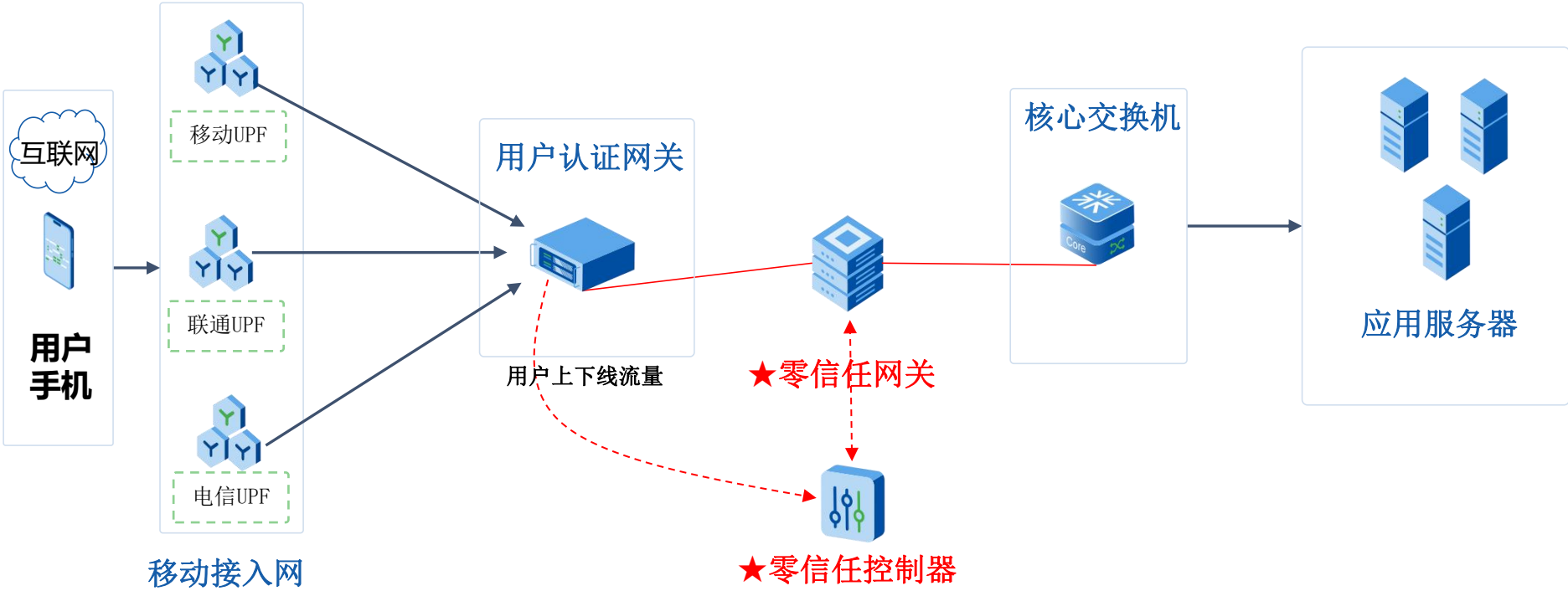
用户流量经过运营商5G网络的切片专网时，UPF对校园内网流量进行分流，并将其引导至零信任安全网关

访问控制

零信任安全网关根据安全管控控制器的消息和二次认证的结果，进行用户访问策略的开通，并执行用户访问合法性的检查，将合法流量引入校园内网，实现对校园资源的访问

管理后台由校园网安全管理员按需灵活规划专网用户的访问权限。在有多个运营商接入的情况下，零信任网关可以与多个运营商UPF进行对接，实现一体化管理、运维，也可以按需对系统进行扩容，从而应对不同规模的用户接入。

4.4 方案落地


互联网
用户
手机
移动UPF
联通UPF
电信UPF
移动接入网
用户认证网关
用户上下线流量
★零信任网关
★零信任控制器
核心交换机
Core
应用服务器

4.5 方案价值

方案价值

1. 业务无边界、内外网无感知，校内二次鉴权，避免双向暴露风险，提升整体安全性
2. 基于用户体系、应用体系的调度编排， 实现基于身份与应用级别细颗粒度的最小化授权管控
3. 独立部署安全控制器模块，实现与安全网关的控制与转发平面分离，可以实现多运营商多出口、多网关系统的统一策略编排，具备灵活的系统灾备和扩展能力

谢 谢 聆 听

T A H N K Y O U F O R W A T C H I N G