2022

畅享连世界

5G专网&校园网融合解决方案

教育行业总监 赵奇峰

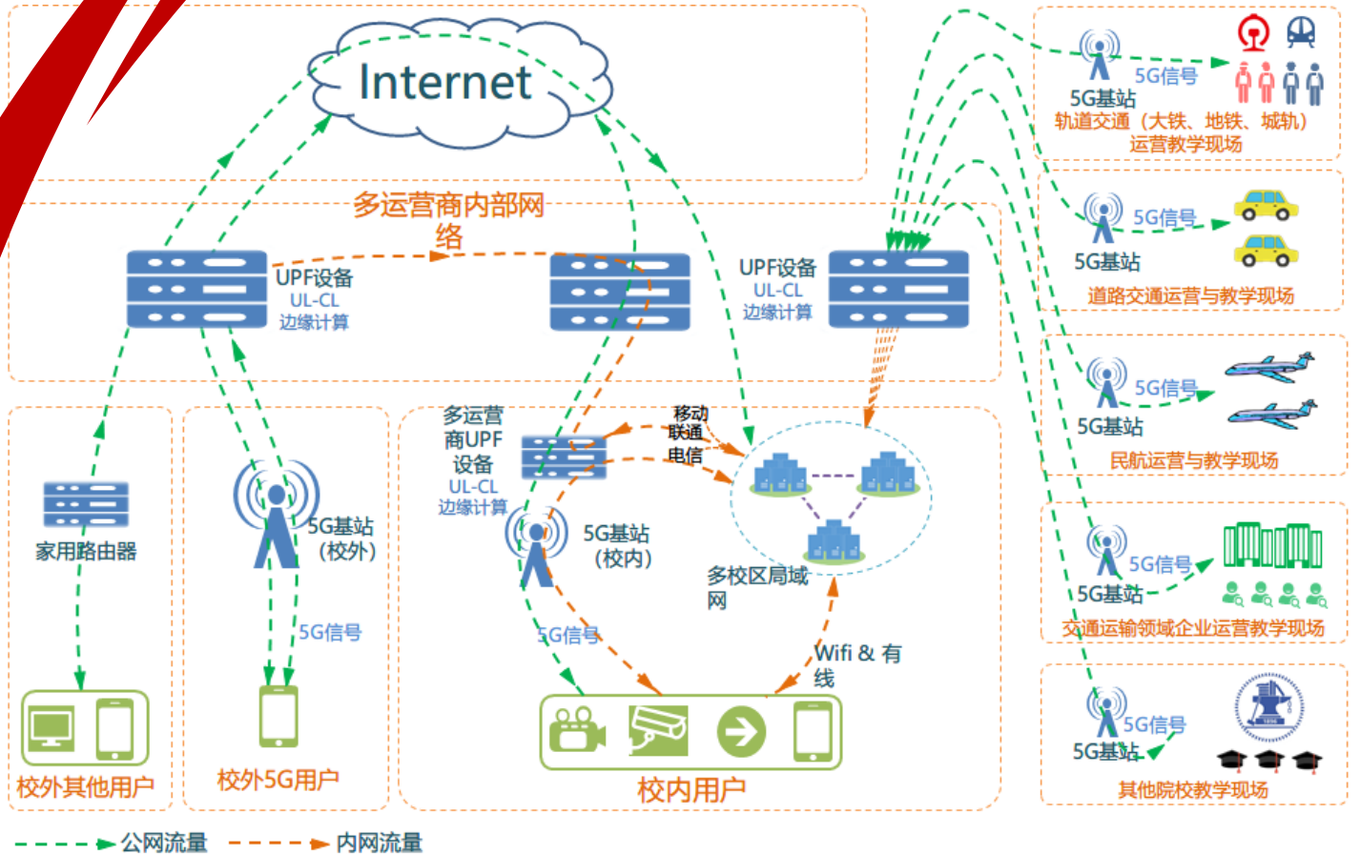
目录CONTENTS

01 5G专网简述 5G

02 5G校园网应用

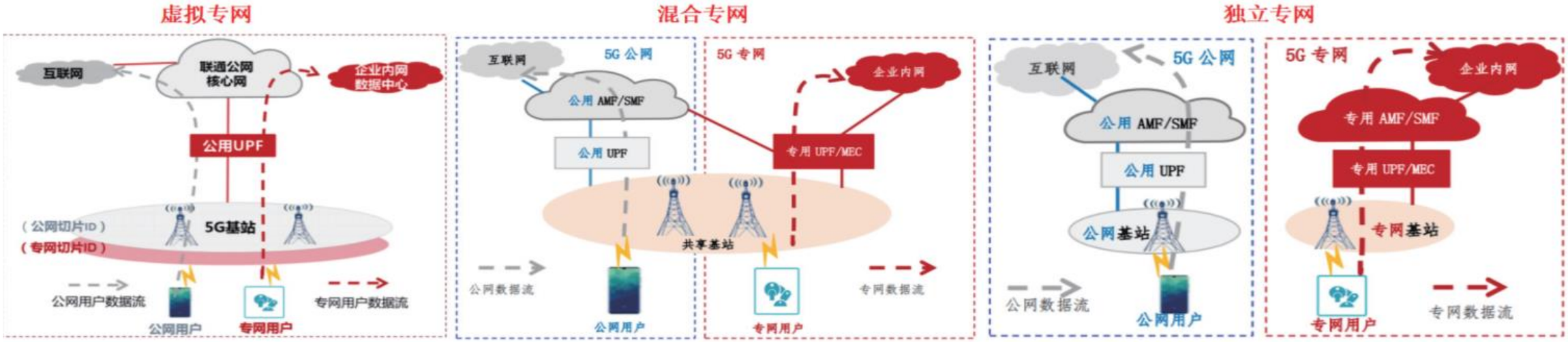
03 5G专网&校园网融合组网

04 5G专网&校园网融合安全



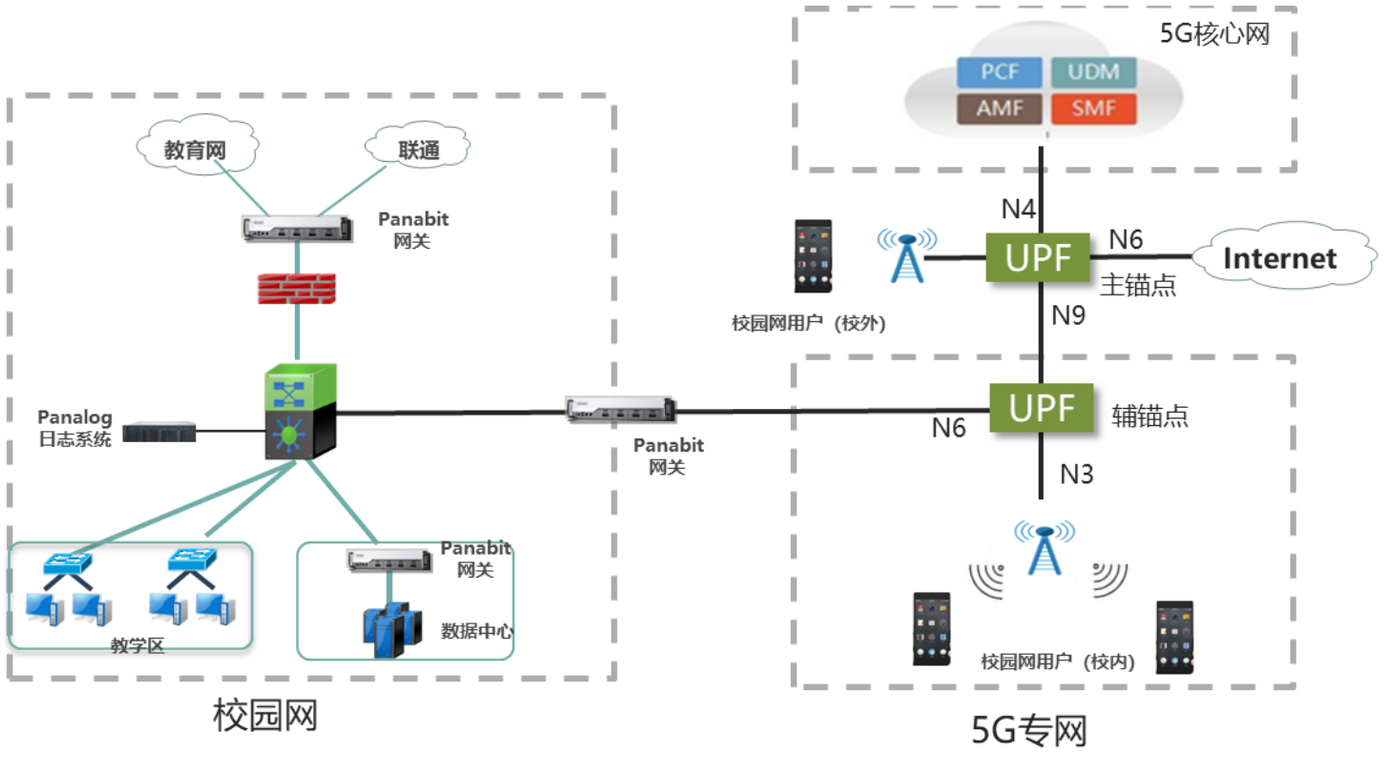
运营商5G专网

5G专网部署模式	中国移动	中国电信	中国联通
与公网完全共享	优享模式	致远模式	5G虚拟专网
与公网部分共享	专享模式	比邻模式	5G混合专网
独立部署	尊享模式	如翼模式	5G独立专网



5G专网即是建立在5G技术之上的专网，所谓专网，是指专用于特定用户的网络，不同于为所有人服务的公网，专网在安全隔离、网络的可靠性和稳定性等方面均具备绝对的优势。

5G专网融合部署示意图



UPF 主要支持UE（用户设备） 业务数据的路由和转发、数据和业务识别、动作和策略执行等

N3 接口是NG RAN（5G无线接入网） 与UPF 间的接口，采用GTP-U 协议进行用户数据的隧道传输。
N4 接口是SMF（5G会话管理功能） 和UPF 之间的接口，采用GTP-U 协议。

N6 接口是UPF 和外部设备之间的接口，N6 接口要求支持专线或L2/L3 层隧道，可基于IP 与其它网络通信。

N9 接口是UPF 之间的接口，两个UPF 之间使用GTP-U 协议进行用户面报文的传输。

5G信号覆盖利用宏站+室分实现；通过“通用DNN（数据网络名称）& ULCL（上行分类）方案”将客户数据分流到校园网和公网，访问校园网采用专线方式解决。

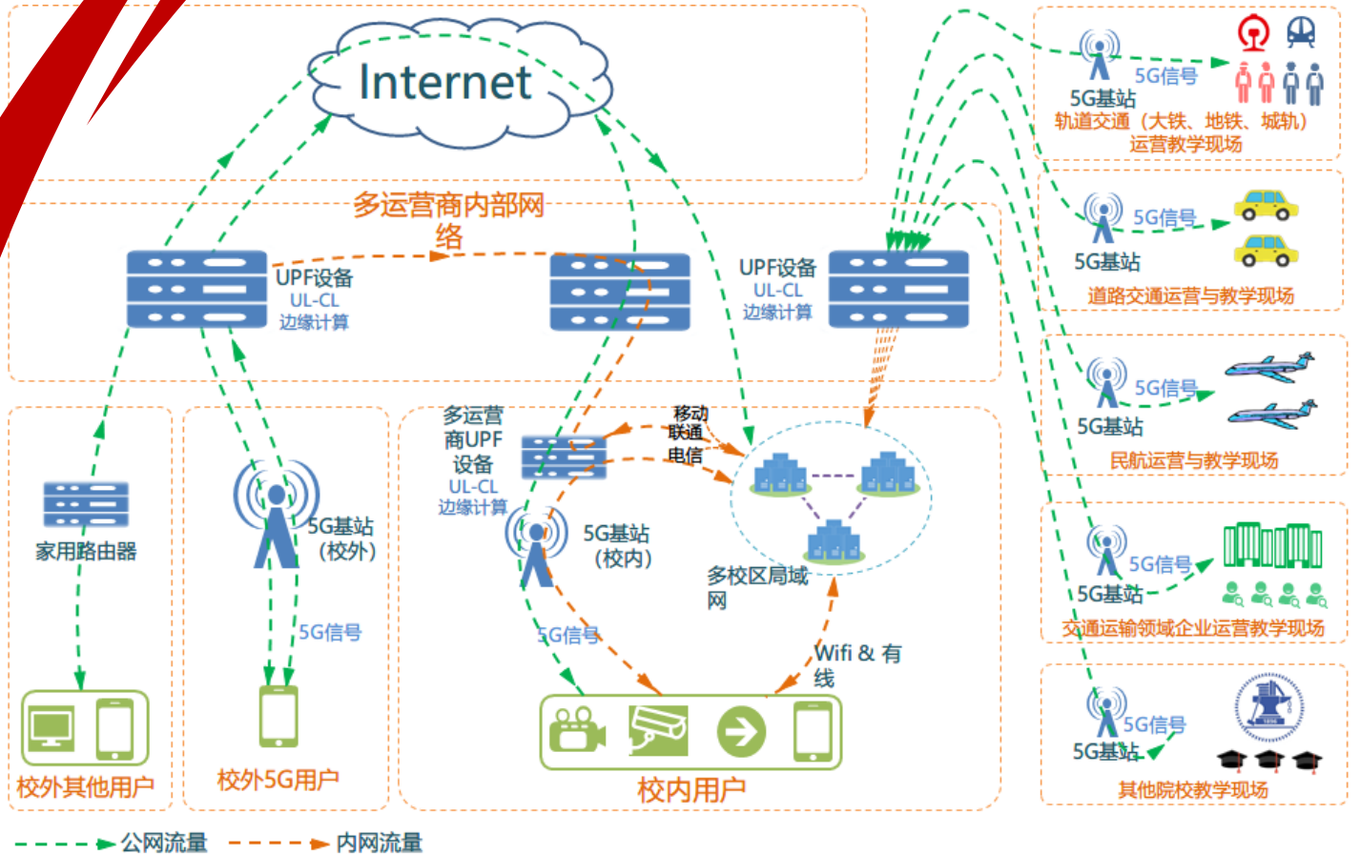
目录CONTENTS

01 5G专网简述

02 5G校园网应用 5G

03 5G专网&校园网融合组网

04 5G专网&校园网融合安全



5G校园网融合方案

背景

1. 国家政策，5G进入校园是趋势
2. 越来越多的高校建设5G校园网。

5G校园网意义

1. 学校5G专网可以作为校内无线资源补充；
2. 校外5G用户不通过VPN使用校园网资源、学术资源；
3. 更加便于打通校园网和运营商边缘计算；

校园网挑战

1. 如何实现5G用户二次鉴权实名制访问内网资源；
2. 如何实现基于5G用户群组访问内网的访问控制；
3. 如何实现对5G用户的审计和行为分析和管控；

5G校园网融合教育部相关文件

教 育 部 办 公 厅

教科信厅函〔2021〕33 号

教育部办公厅 工业和信息化部办公厅
关于提高高等学校网络管理和服务质量的通知

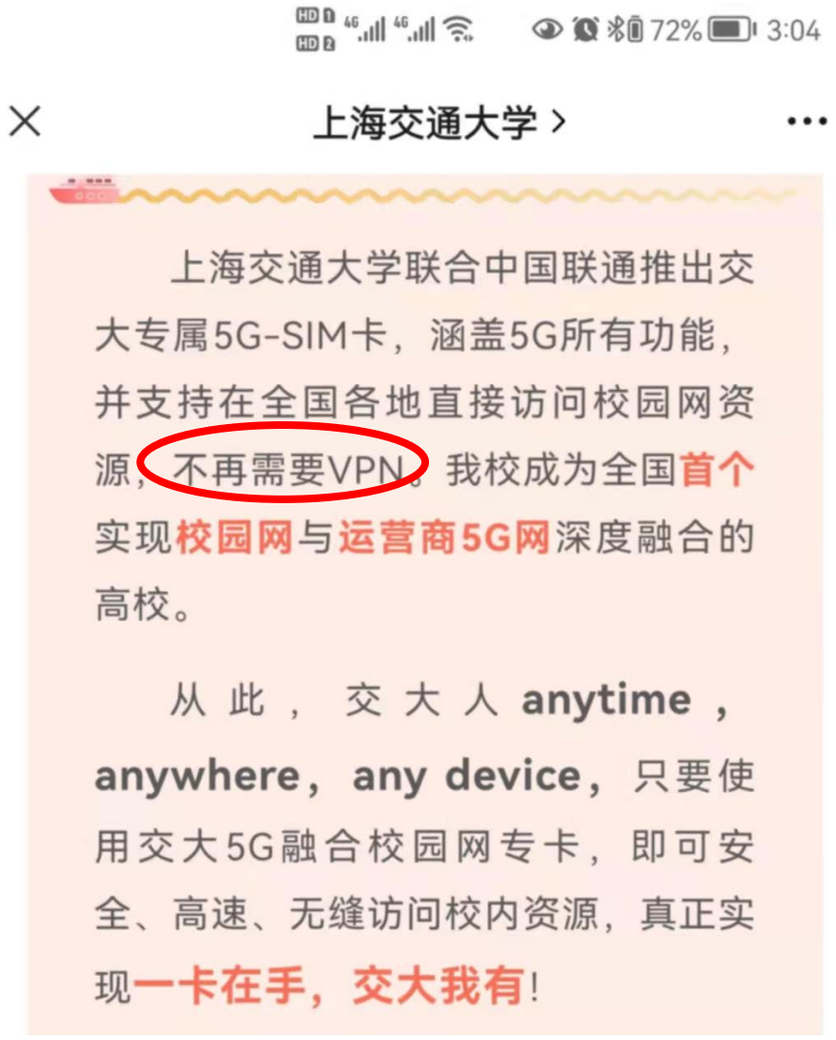
各省、自治区、直辖市教育厅（教委）、通信管理局，新疆生产建设兵团教育局、工业和信息化主管部门，部属各高等学校、部省合建各高等学校：

校园网络是学校为教职员工和学生提供网络接入，满足教学、科研、管理服务需求的信息化基础设施，包括有线宽带网络、无线局域网络和移动通信网络。为提高高等学校网络管理和服务质

二、提高校园网络环境建设水平

高等学校应会同基础电信企业加强对校园网络的总体规划，组织科学论证，统筹通信管道、光缆、基站、室内分布系统等设施建设布局，保障校园网络服务质量，推进基础设施共建共享，避免重复建设。鼓励高等学校建设校园局域网，统筹有线宽带和无线局域网，由学校统一为教职员工和学生接入校园局域网，再由校园局域网统一接入公用通信网络。学校新建的建筑应按照《公共建筑光纤宽带接入工程技术标准》等要求，同步设计、部署宽带网络设施，验收通过后方可统一接入公用通信网络。基础电信企业应对学校建立出口宽带网络弹性带宽保障机制，根据学校流量实际使用情况及时调整带宽；保障校园移动通信信号质量，确保基站对周围环境影响符合国家要求。高等学校会同基础电信企业扩大 5G（第五代移动通信）信号在高等学校的覆盖范围，推动 5G 技术在校园的深入应用。

5G校园网融合案例

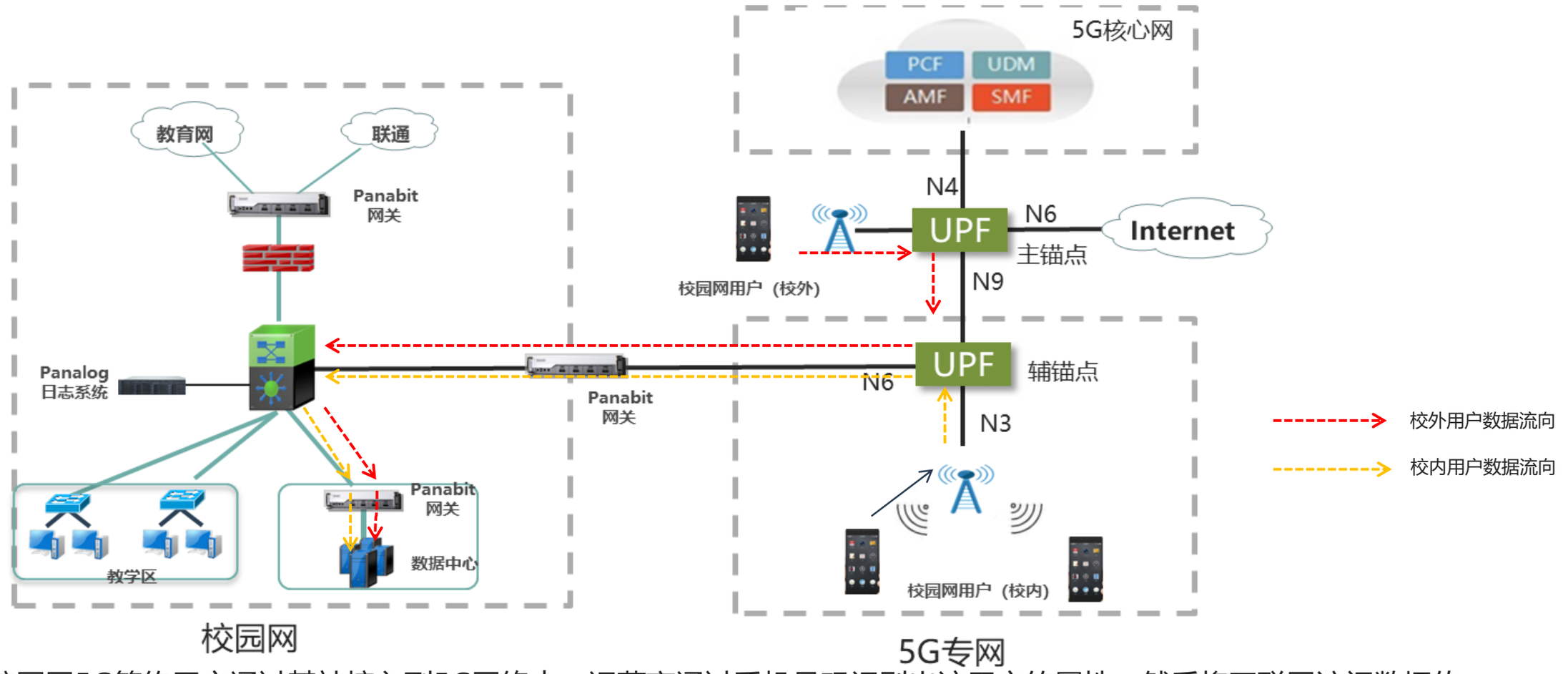


复旦大学116周年校庆之际传来消息：该校5G校园网上线，中国联通、中国移动、中国电信三大运营商全覆盖。去年起，三大运营商和复旦合作，启动5G虚拟校园网联合建设项目，目前已在上海地区初步建成一张“无边界5G虚拟校园网”。这意味着，身在校外的复旦师生，今后无需VPN就能直连访问校内资源。随着我国5G网络建设推进，这张网还将延伸到国内更多城市。 5G虚拟校园网，指的是以5G移动通信网络及边缘计算技术为基础，满足学校业务连接、高速计算、信息安全等需求的校园虚拟专用网络。作为原校园有线网络及无线网络的延展与补充，这张虚拟校园网将极大提高校园网络覆盖面。 需额外安装软件？下载速率不稳定？——VPN的这些问题，5G虚拟校园网都能解决。大带宽、低时延、广覆盖、无障碍访问学校内网，下载文件高速度，观看视频无卡顿，为复旦师生提供访问内网的更多选择。复旦大学现代物理研究所副研究员钟晨说：“除了复旦大学邯郸校区和江湾校区的核心团队外，我们在嘉定的中科

中山大学网络与信息技术中心赵琼老师

中大校园5G网作为原校园有线网及无线网的延展与补充，最大的优势在于免除VPN拨号等繁琐过程，在广州市内可直接快速、无感知的访问校内资源，让中大师生在有5G的地方，都有中大校园网。同时，5G网络与校园网络的边界是安全可控的，学校对下发的IP路由、域名实行白名单机制，对目标访问实行必要的安全防护措施，进一步加强了校园5G网的安全性。

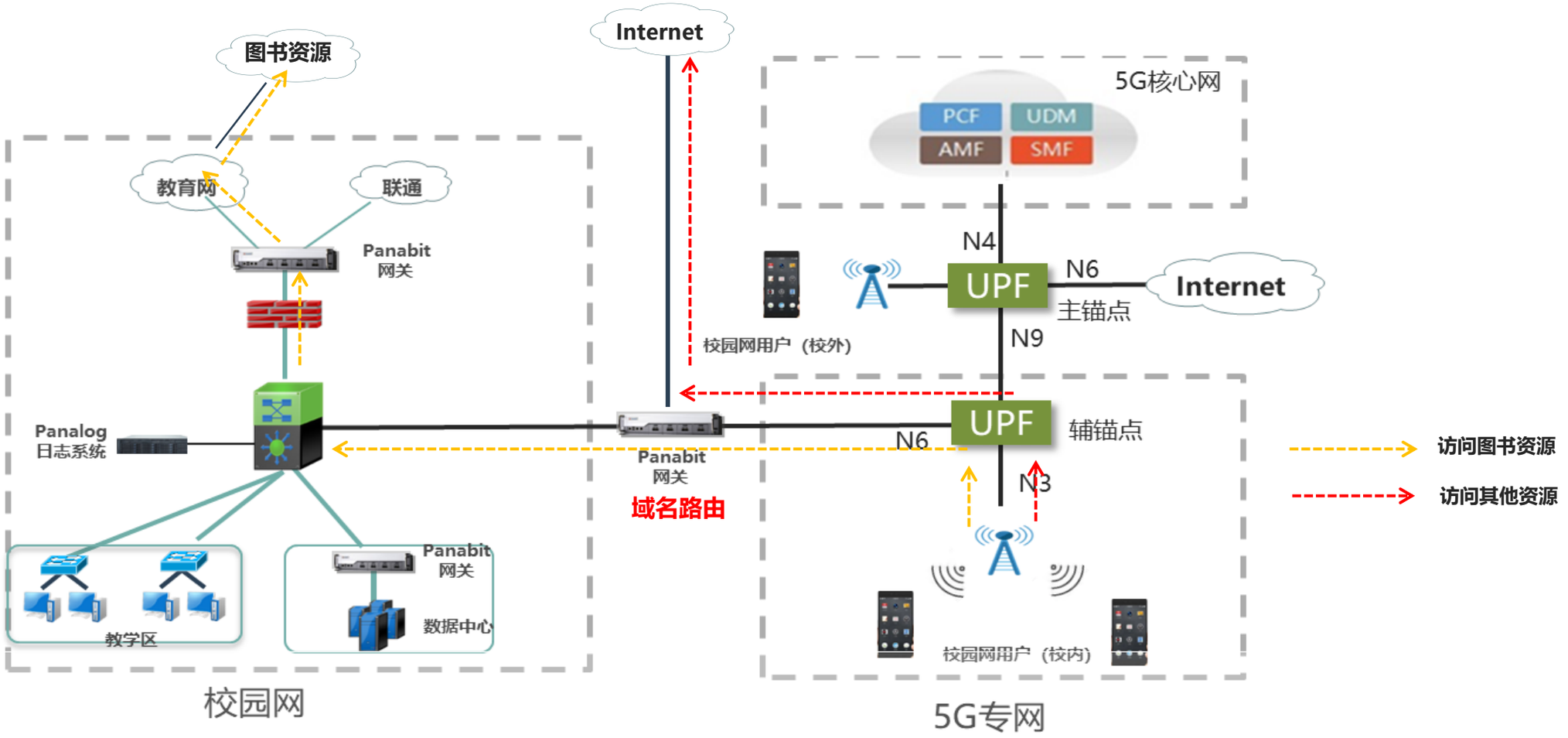
校园网5G融合应用—访问校内资源



校园网5G签约用户通过基站接入到5G网络中，运营商通过手机号码识别出该用户的属性，然后将互联网访问数据传输到相关的UPF设备

1. 如果5G签约用户在校内，连接校内5G基站，由辅锚点UPF将数据包分流到校内；
2. 如果5G签约用户在校外，连接本地基站，数据包先路由到主锚点UPF，然后根据签约用户属性，路由到对应的辅锚点，然后由辅锚点路由数据包到校内。

校园网5G融合应用—访问校外图书资源



方案说明：

由于某些UPF只能基于IP地址作路由，而很多校外图书资源是通过CDN发布，IP地址经常变化，因此无法实现通过UPF进行图书资源域名路由。

Panabit网关支持域名路由，可以基于图书资源进行域名路由，讲图书资源数据包路由到校内，而其他流量通过单独的链路进行NAT和负载均衡出网。

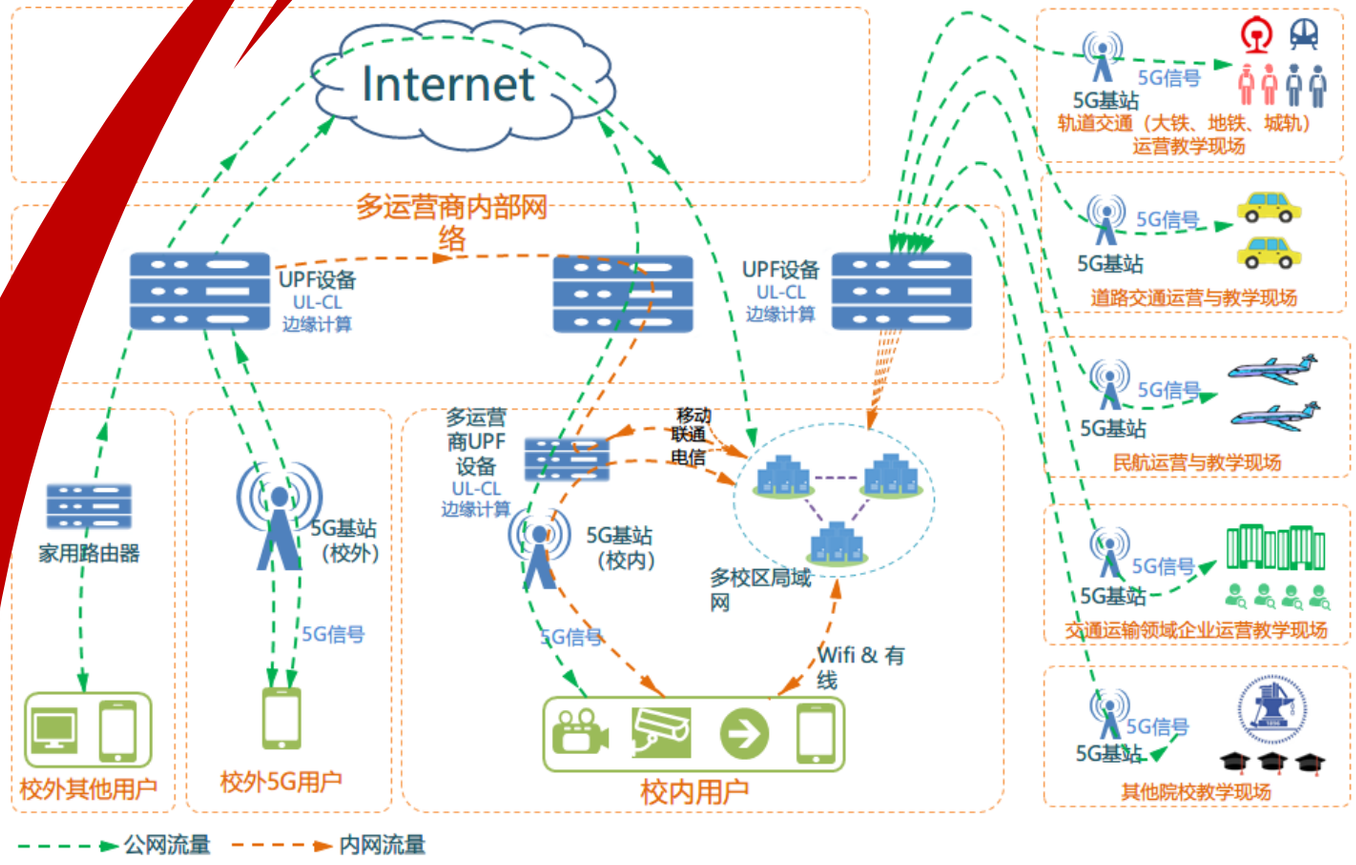
目录CONTENTS

01 5G专网简述

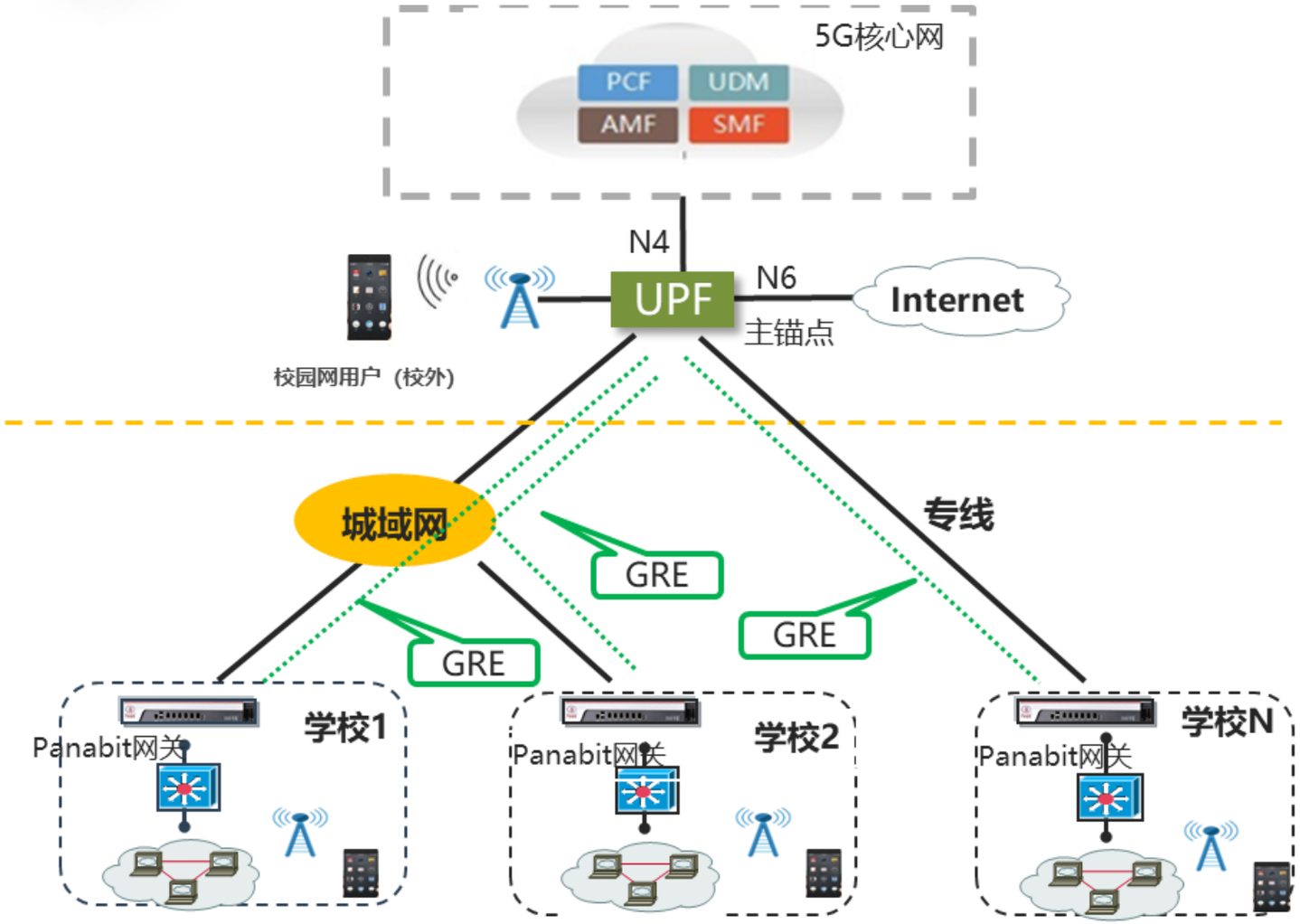
02 5G校园网应用

03 5G专网&校园网融合组网 5G

04 5G专网&校园网融合安全



5G校园网融合组网— GRE隧道

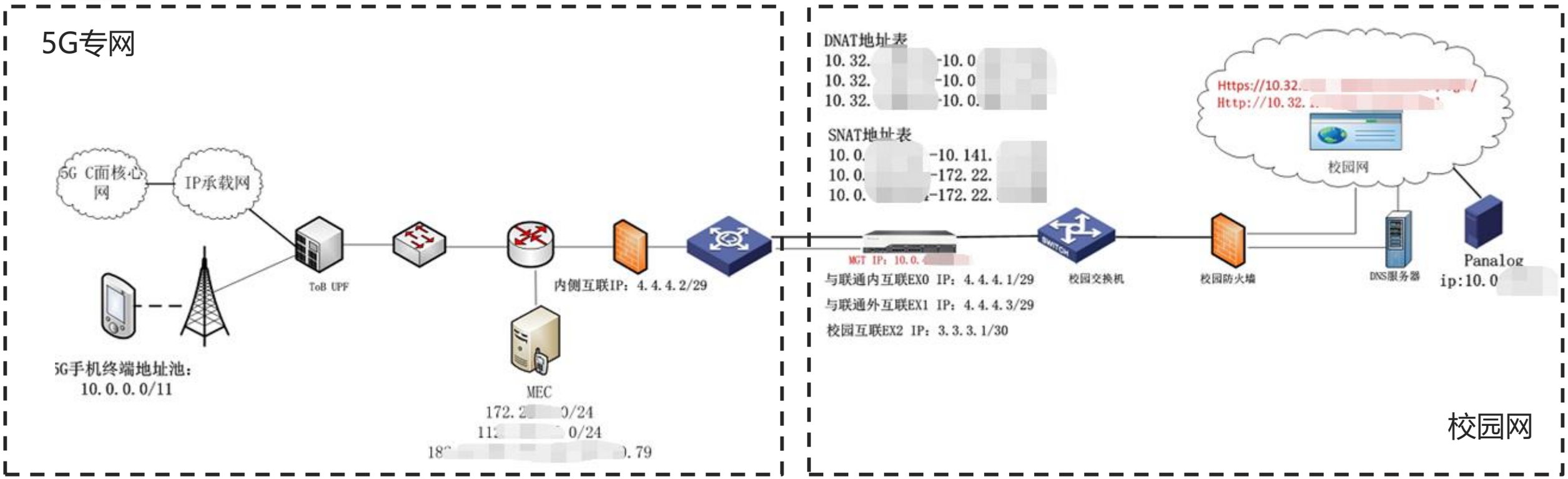


方案说明：

1. 运营商采用共享UPF模式进行组网，一台UPF设备面对多个高校；

2. 为了进行不同高校5G专网的隔离，不同学校使用不同的GRE隧道，因此需要5G融合网关支持GRE隧道功能

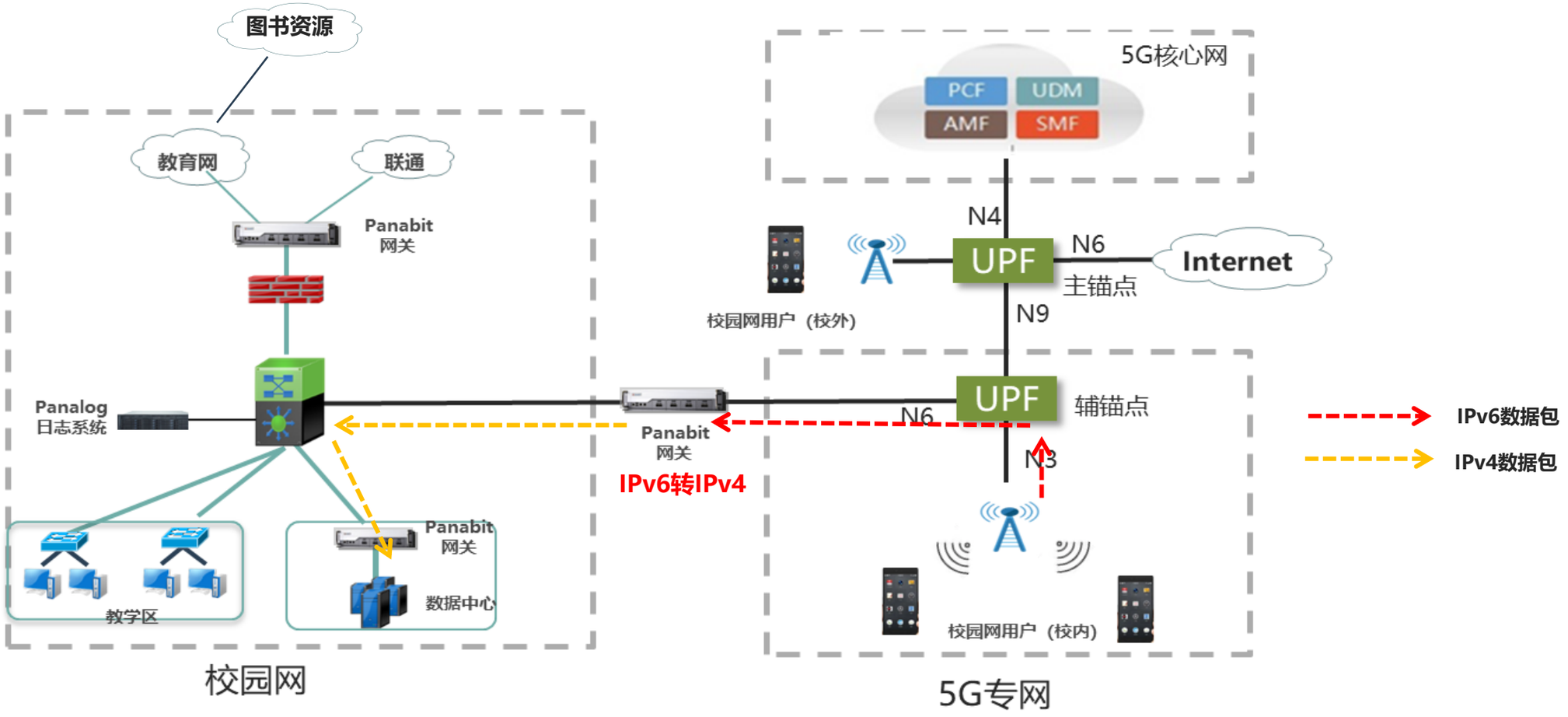
5G校园网融合组网— IP地址重复问题



方案说明：

1. 某厂商UPF分配给5G手机的IP地址只能是10.0.0.0/11（10.0.0.1~10.31.255.255）的IP地址；
2. 校内正好也使用10.0.0.0/8的IP地址；
3. 为了解决互联互通问题，从5G专网到校内网络需要同时进行大量IP地址的源地址转换和目标地址转换；

5G校园网融合组网—IPv6转换IPv4



5G专网在运营商处，分配的会有IPv6的IP地址，但校内服务器可能使用的IPv4地址，因此，需要把运营商5G专网的IPv6地址进行转换，从而保证服务器顺利访问。

目录CONTENTS

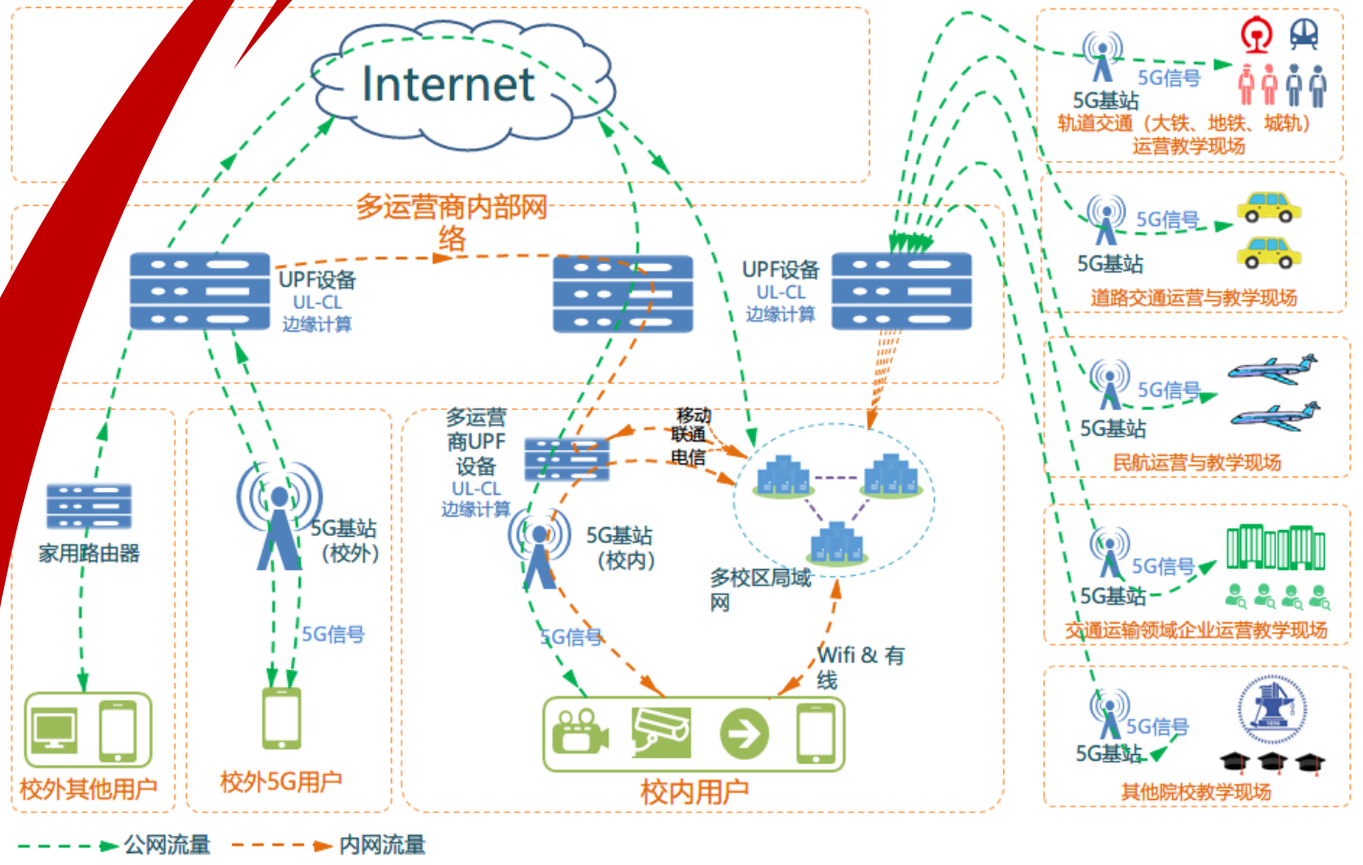
01 5G专网简述

02 5G校园网应用

03 5G专网&校园网融合组网

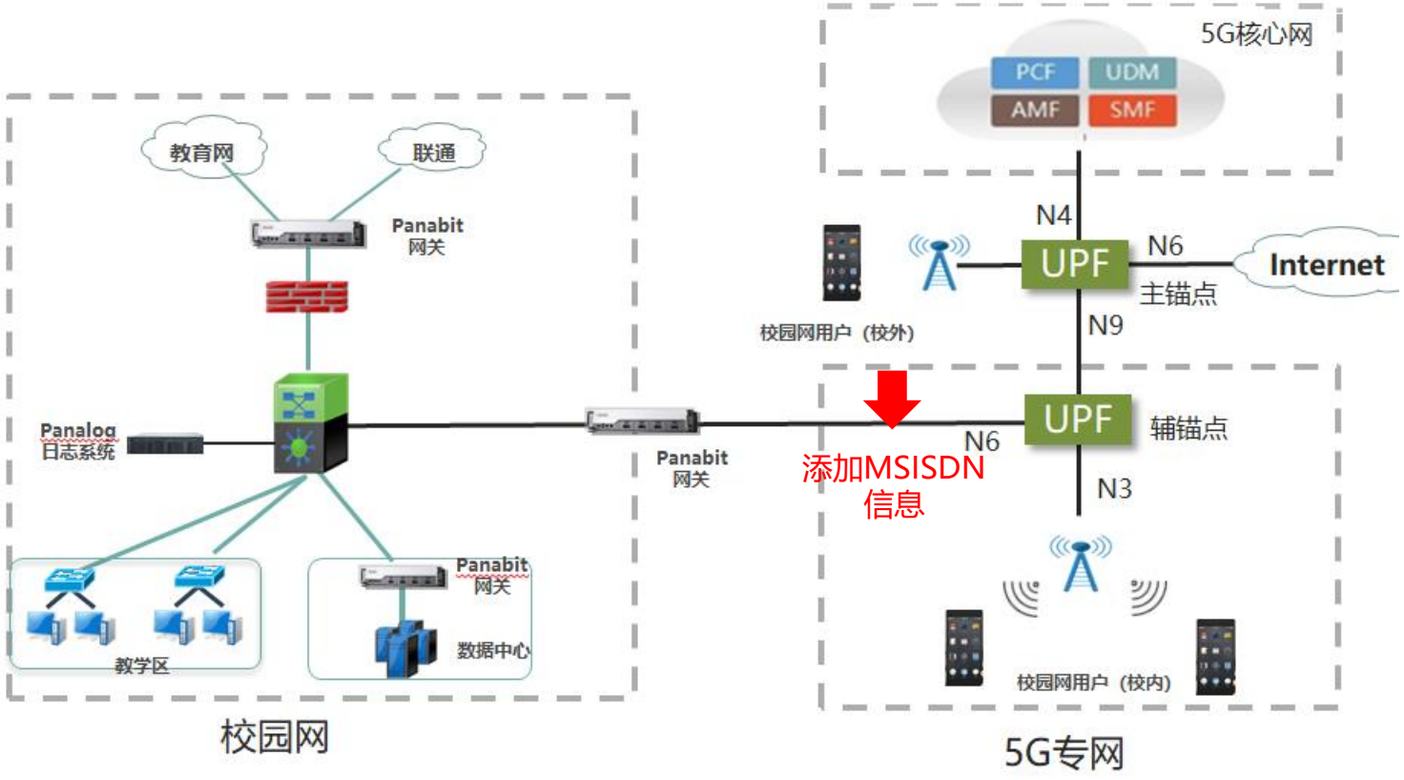
04 5G专网&校园网融合安全

5G



5G校园网融合安全部分— 校园网二次鉴权

针对大学管控需求，需要**识别**出登陆校园内网的**用户身份**，可以通过如下方式实现。
在UPF上配置**“头增强”**功能，添加MSISDN（用户手机号）在每次传输的报文中，校方通过识别MSISDN获悉用户身份。



方案说明— UPF侧：

1. 在分流到校园网的数据包，在UPF上配置“头增强”功能，添加MSISDN（用户手机号），校方通过识别MSISDN获悉用户身份；

2. Panabit设备串接在运营商5G网络和校园网之间，当用户数据包通过5G网络传输到学校时候，Panabit设备在数据包里面识别MSISDN（用户手机号）获悉用户身份，同时记录IP和用户名的对应关系；

5G校园网融合安全部分— 用户无感知认知

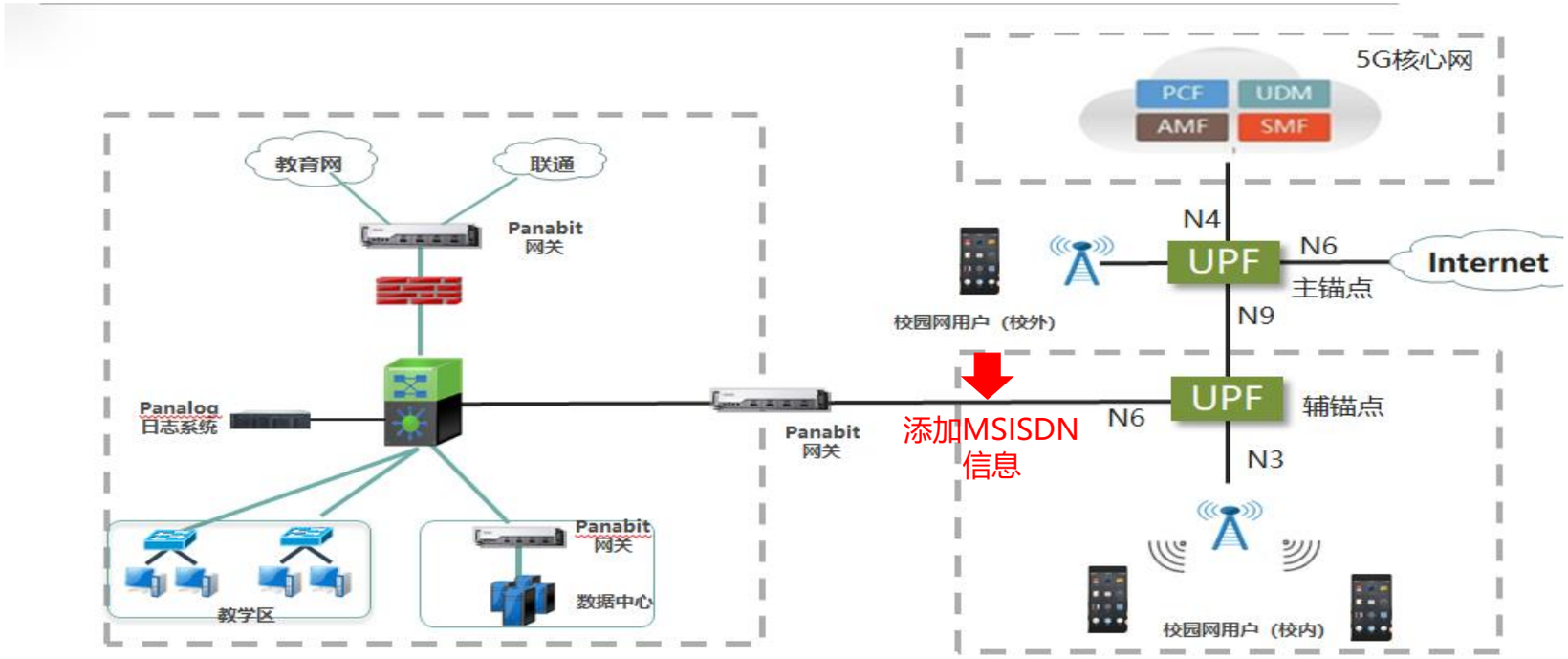
5G专网用户

- 5G签约用户登录校内自服务平台，用户直接进行手机号码和校内账号绑定，然后由校方进行审批。

Panabit设备处理

- 在UPF上配置“头增强”功能，添加MSISDN（用户手机号）在传输的报文中，UFP通过头增强发过手机号码后，Panabit到自服务系统进行查询，看看这个手机号码是否绑定成功，如果不成功，阻断访问，反之就放行。
- 由于MSISDN（用户手机号）是在局端UPF处临时加入的，有些服务器是不能识别该数据包（例如HTTPS），因此，Panabit设备需要去除MSISDN包头，然后传输数据包到相关服务器，实现了图书资源访问的诉求。同时，由于数据包经过Panabit设备后，已经没有MSISDN（用户手机号），也保证了用户是隐私性。
- Panabit网关设备维护会话认证名单，对于同一个IP地址+手机号的会话以前认证过，直接放行，从而实现用户5G无感知认证。

5G校园网融合安全部分— 访问控制&日志审计



方案说明—Panabit侧：

1. Panabit 设备可以基于用户群组进行访问控制，不同用户群组访问内容不同；例如：网络中心的人员可以对网络设备进行管理；学生只能访问选课、图书资源等相关资源。
2. Panabit设备将相关访问的记录传给Panalog，进行访问日志1:1留存。将源IP地址、目标IP地址、NAT后地址、使用的协议名称，用户名、访问资源的域名等信息在一张表上显示。实现的5G用户访问校内资源日志记录，从而完成相关审计和查询工作。

5G校园网融合安全部分—访问控制界面

序号	线路	首包接口	源接口	内网地址	外网地址	协议	应用	动作	IP限速	备注	操作
100	any	any	any	学生5G用户	校内图书资源	any	图书资源	✓	0	学生5G用户访问校...	
200	any	any	any	学生5G用户	any	any	any	✗	0	禁止学生5G其他应用	

5G校园网融合安全部分—审计界面

序号	设备	协议名称	类型	接口	访问时间	连接时间	源地址:端口	MAC	目标地址:端口	NAT地址	用户账号	域名
1	1	DNS	UDP	em0	2021/12/02 12:55:36	0	10.27.144.146:25267	F4-A4-D6-7A-85-F9	192.168.20.2:53	10.63.154.140:25267		oa .edu.cn
2	1	DNS	UDP	em0	2021/12/02 12:55:37	0	10.27.144.146:64685	F4-A4-D6-7A-85-F9	192.168.20.2:53	10.63.154.140:64685		oa .edu.cn
3	1	DNS	UDP	em0	2021/12/02 12:55:54	0	10.27.144.146:24075	F4-A4-D6-7A-85-F9	192.168.20.2:53	10.63.133.119:24075	861350	ss .edu.cn
4	1	DNS	UDP	em0	2021/12/02 12:55:54	0	10.27.144.146:64340	F4-A4-D6-7A-85-F9	192.168.20.2:53	10.63.133.119:64340	861350	ss .edu.cn
5	1	DNS	UDP	em0	2021/12/02 12:55:54	0	10.27.144.146:4396	F4-A4-D6-7A-85-F9	192.168.20.2:53	10.63.133.119:4396	861350	m .edu.cn
6	1	DNS	UDP	em0	2021/12/02 12:55:54	0	10.27.144.146:16161	F4-A4-D6-7A-85-F9	192.168.20.2:53	10.63.133.119:16161	861350	m .edu.cn
7	1	其它HTTPS	TCP	em0	2021/12/02 12:55:54	37	10.27.144.146:48972	F4-A4-D6-7A-85-F9	192.168.11.11:443	10.63.133.119:48972	861350	s .edu.cn
8	1	其它HTTPS	TCP	em0	2021/12/02 12:55:54	37	10.27.144.146:36288	F4-A4-D6-7A-85-F9	192.168.11.65:443	10.63.133.119:36288	861350	.edu.cn
9	1	其它HTTPS	TCP	em0	2021/12/02 12:55:54	37	10.27.144.146:36290	F4-A4-D6-7A-85-F9	192.168.11.65:443	10.63.133.119:36290	861350	.edu.cn
10	1	其它HTTPS	TCP	em0	2021/12/02 12:55:54	51	10.27.144.146:48974	F4-A4-D6-7A-85-F9	192.168.11.11:443	10.63.133.119:48974	861350	ss .edu.cn
11	1	其它HTTPS	TCP	em0	2021/12/02 12:56:31	14	10.27.144.146:36298	F4-A4-D6-7A-85-F9	192.168.11.65:443	10.63.154.140:36298	86135098	ny .edu.cn
12	1	其它HTTPS	TCP	em0	2021/12/02 12:56:31	14	10.27.144.146:36300	F4-A4-D6-7A-85-F9	192.168.11.65:443	10.63.154.140:36300	86135098	my .edu.cn
13	1	其它HTTPS	TCP	em0	2021/12/02 12:56:31	68	10.27.144.146:48984	F4-A4-D6-7A-85-F9	192.168.11.11:443	10.63.154.140:48984	861350	ss .edu.cn
14	1	Android	TCP	em0	2021/12/02 12:55:37	131	10.27.144.146:44180	F4-A4-D6-7A-85-F9	192.168.49.33:80	10.63.154.140:44180	861350	oa .edu.cn

Panalog进行5G专网访问校内资源日志1:1留存。将源IP地址、目标IP地址、NAT后地址、使用的协议名称，用户名、访问资源的域名等信息在一张表上显示。便于学校进行查询和溯源。

2022

畅享连世界

THANK YOU