

5G 智慧警务 E2E 解决方案

中国移动宁夏有限公司

现有网络背景：公安客户网络全景与运营商可参与空间



移动警务的业务痛点分析



- 警力资源不足：人工监控和日常巡逻，占用大量警力
- 工作强度大：案件增长5倍，警力增长30%，基层公安机关每年300多项任务，完成率低

①日常巡逻



临时布控摄像机



临时布控摄像机

- 广场和CBD高空无法铺设光纤，摄像头安装难度大、施工成本高，时间长
- 人员密集区域4G网络拥塞严重，视频回传卡顿

④重大安保、应急

典型场景 — 某花城广场



- 人流量多、应急事件多、大型活动多
- 周边CBD商业区、领事馆、海心沙体育馆、图书馆、K11、少年宫

- 准确识别：执法现场无法准确识别嫌疑人，错失抓捕机会



警务通



AR眼镜

②现场执法

- 出警速度不能达标：要求3分钟到现场
- 警力分布掌握困难（室内）



警力分布



无人机



执法仪

③接警处警

5G+云+AI 使能智慧新警务

5G与警务相关的技术优势

上行大带宽
(100M~1G)

移动警务宽带化、视频监
控高清化

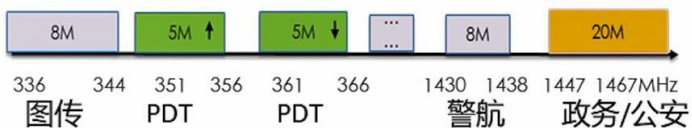
安全(数据, 用户, 架构)
可信机制贴合警务诉求

低时延 (10ms) 警
务无人机, 无人车
远程操控

定位精度 (3D,米级)
处警精准化

公安移动警务短期内不会自建5G网络

公安无5G频谱, 短期专网无法获得5G增益

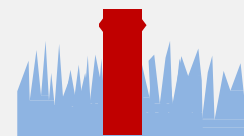


- 5G标准暂不支持5MHz以下带宽, 小带宽增益不明显
- 1.4G频率政府、公安共享

5G给公安行业带来新模式



- 优先等级的网络服务

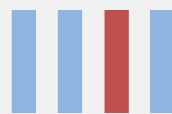


QoS/RB或频谱预留



指定运营商

- 专用切片保障网络质量

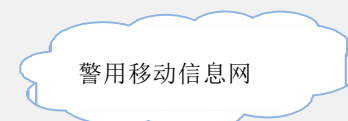


网络切片



专用于公安用户

- 未来趋势: 按需买5G服务



警用移动信息网

PDT

公网
(4G/5G)



- 提供高安全性的VPN服务
- 人群聚集、公网管控及紧急情况下, 保证公安用户优先接入
- 网络规划给公安用户提供专用网络切片, 降低系统延时

业务场景一：日常巡逻

业务场景

- 警务车巡逻：常规治安巡逻
- 无人车巡逻：公园/海滨步行道治安巡逻
- 机器人巡逻：人员密集场景安保巡逻

XX市，警务车约**3000+**辆、无人巡逻车**100+**辆，巡逻机器人**50+**个

业务诉

求：

- 1、**警务车**巡逻：车载3-7路摄像机持续拍摄，视频回传公安专网进行AI分析，
- 2、**无人车**巡逻：车载180度（4路拼接）广角摄像机，视频回传，AI分析，远程喊话、人员驱离
- 3、**机器人**巡逻：人员密集场景，红外摄像机人员核检及测温

现状： 人员巡逻为主

- 1、人员巡逻
- 2、警车巡逻



痛点： 警力不足，缺少智能化手段

- ① **警力资源不足**：人工监控和日常巡逻，占用大量警力。
- ② **工作强度大**：案件增长5倍，警力增长30%，基层公安机构每年300多项任务，完成率低

5G+警务： 视频+AI、自动化巡检，减少人力



业务场景二：现场执法（设卡检查）

业务场景

- 临时布控
- 检查人：重点人员盘查、身份核验
- 检查车：违章、酒驾

XX市公安执法，全年上路执法检查 **1.2万次**



业务诉求

求：

- 1、人/车核验：**警务通**安全连接公安内网，进行人/车核验
- 2、执法视频实时回传：**执法仪**高清视频实时回传，执法取证及远程指挥应对
- 3、**临时布控视频回传**：态势摄像机等回传公安内网，实时分析/监控人流、重点人员/车辆识别追踪等

现状：4G网络

- 1、移动接入/回传：4G
- 2、安全：终端加密卡+VPDN

痛点：无优先保障，4G带宽不满足

- 1、人员密集场所，4G回传执法视频不能保证优先接入
- 2、4G高清视频回传质量较差（丢帧、卡顿）

5G+警务：切片优先保障、大带宽满足视频回传



业务场景三：接警处警

业务场景

- 无人机侦察：先期抵达
- 无人机控制及救援：警具/救援器械抛投
- 人员搜寻：走失/特殊人员的识别
- 指挥调度：根据实时警力分布情况，调度就近警力处警

业务诉求： 1、无人机侦察：受限于交通及环境情况，由无人机先期抵达现场。

无人机视频回传+远程操控，超视距控制

2、**无人车控制及救援**：无人机抛投警具（锁网等），喊话控制嫌疑人；无人机抛投救生圈等装备进行施救

3、**人员搜寻**：**识别、轨迹跟踪和防逃**：借助AR、移动/固定摄像头，识别和分析人员，进行轨迹跟踪和防逃措施

4、**警力分布实时情况**：掌握警力在室内/室外的准确分布

现状： 到达现场时间长，无定位能力

1、交通情况对处警时长影响大

2、无人机活动范围受限



痛点： 警力分布掌握困难（室内）

① **出警时效要求严格**：无人机大范围远程操控，连续性、低时延；高清现场视频回传难以保证

② **警力分布**：警力实时分布情况较难掌握，无法有效组织就近警力处境

5G+警务：

1、无人机视频回传+远程操控，降低接处警时间，先期抵达，采取应对措施

2、实时准确定位，掌握警力分布，指挥调度

3、移动端5G视频回传+AI识别分析，人员识别跟踪，同行人分析等，实现人员搜寻

场景1：先期抵达，控制



场景2：无人机施救



场景3：指挥调度



场景4：人员搜寻



业务场景四：重点安保

业务场景

- 重点区域保障：人群密度监控、预警
- 重点人员防控：目标识别、关联追踪、抓捕防逃
- 无接触查验：测温、人/车查验
- 指挥前移：通信保障快速开通

业务诉求：

- 1、无接触查验/测温：AR眼睛、固定/移动摄像头，根据视频内容进行人员、车辆识别，信息推送到警员
- 2、重点人员防控：借助AR、移动/固定摄像头，识别分析重点人员，进行轨迹跟踪和防逃措施
- 3、无线优先接入：警务业务优先接入，回传及指挥高保障
- 4、满足临时性网络需求：指挥前移，避免临时拉光纤时效低

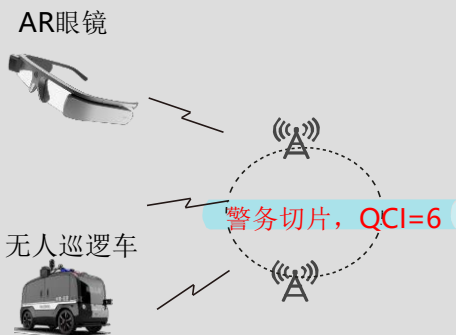
现状：无优先保障，临时拉光纤

- 1、无优先接入，基本信息在拥塞后都无法回传
- 2、重保前临时拉光纤做保障，事后再拆除

痛点：警力不足，缺少智能化手段

- 1、重保无优先保障，拥塞时基本信息都无法回传
- 2、临时性光纤部署困难且时效性差，短期使用再拆除成本高
- 3、重点人员无法调用历史轨迹、缺乏轨迹跟踪、取证困难

5G+警务：视频+AI、关联分析，提升处置效率



场景1：重点人员防控



场景2：人员搜寻

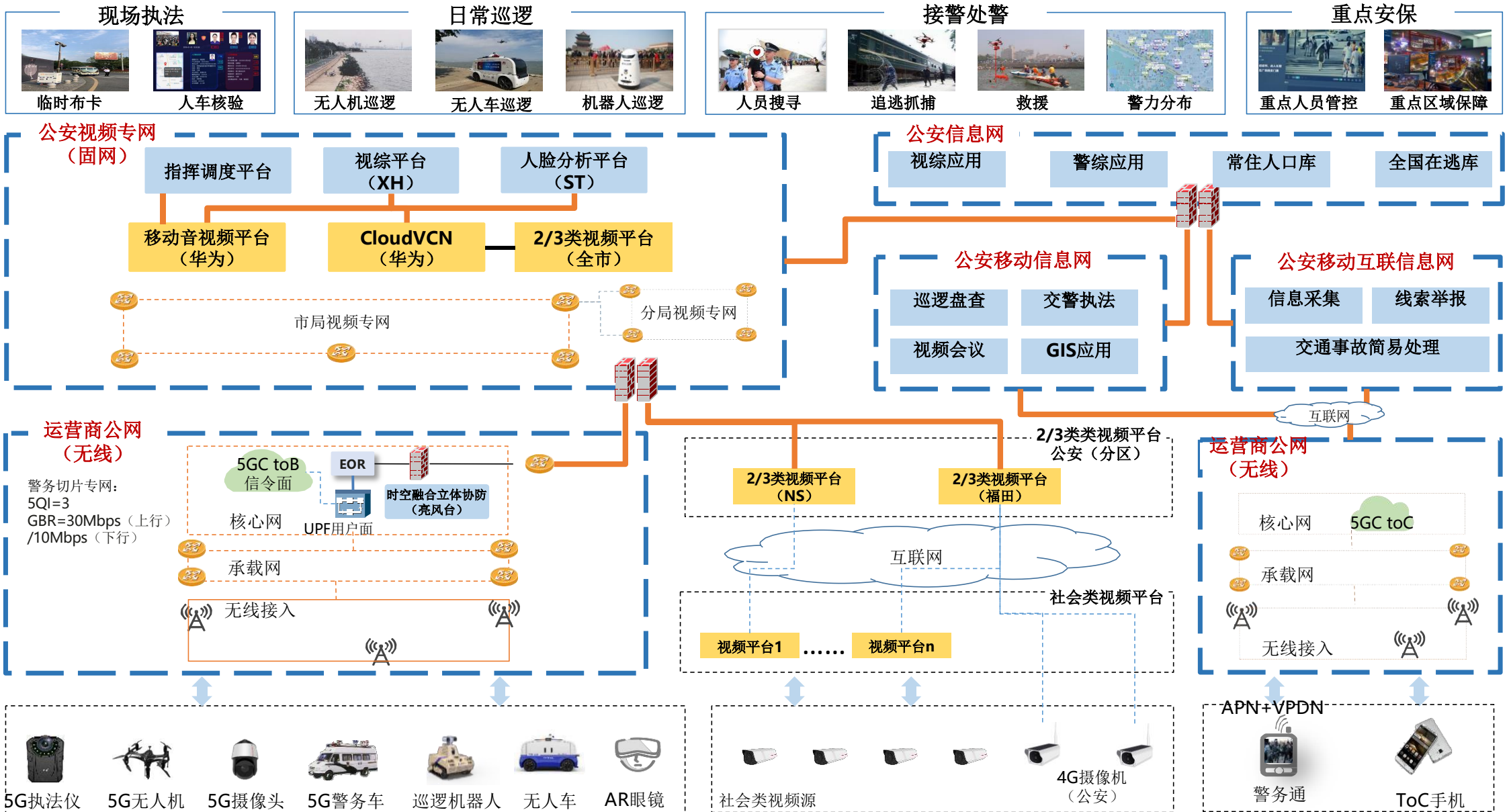


场景3：重点区域保障

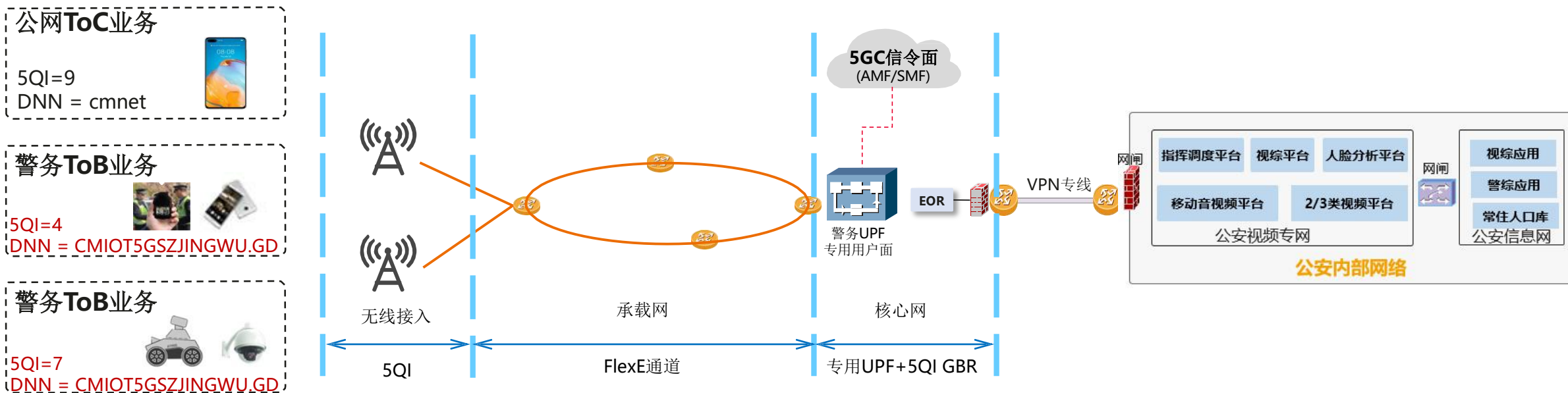


视频综管平台 视频库 AI分析+应用平台

5G智慧警务整体架构



5G警务切片解决方案



✓ 5G切片：无线5QI + 承载FlexE通道 + 专用UPF/GBR

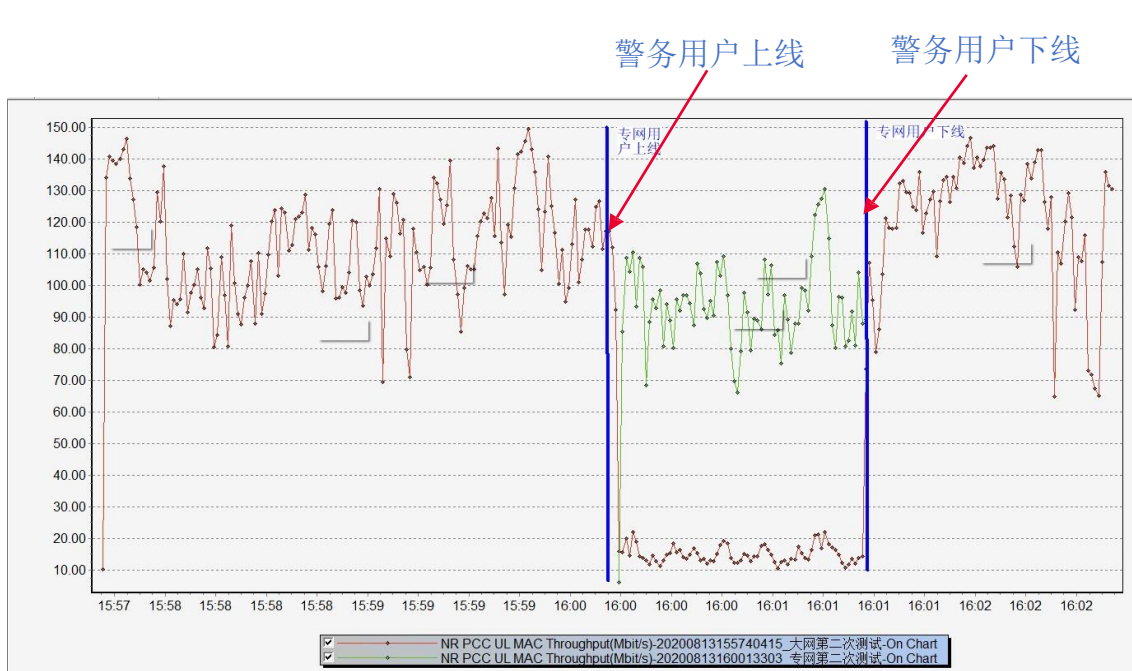
• 注：5QI=4/7是建议值，根据运营商产品设计及警务购买级别确定

业务	DNN	5QI	FlexE通道	保障方式	备注
公众业务	cmnet	9（默认）	/	/ 无保障，默认公众用户	
警务（执法仪、警务通）	CMIOT5GSZJINGWU.GD	专载5QI=4(GBR)	带宽1G（共用）	5QI=4, GBR=10Mbps（上行）/20Mbps（下行）	警务专用
警务业务（无人车、5G摄像头）	CMIOT5GSZJINGWU.GD	专载5QI=7(GBR)	带宽1G（共用）	5QI=7, GBR=20Mbps（上行）/10Mbps（下行）	警务专用

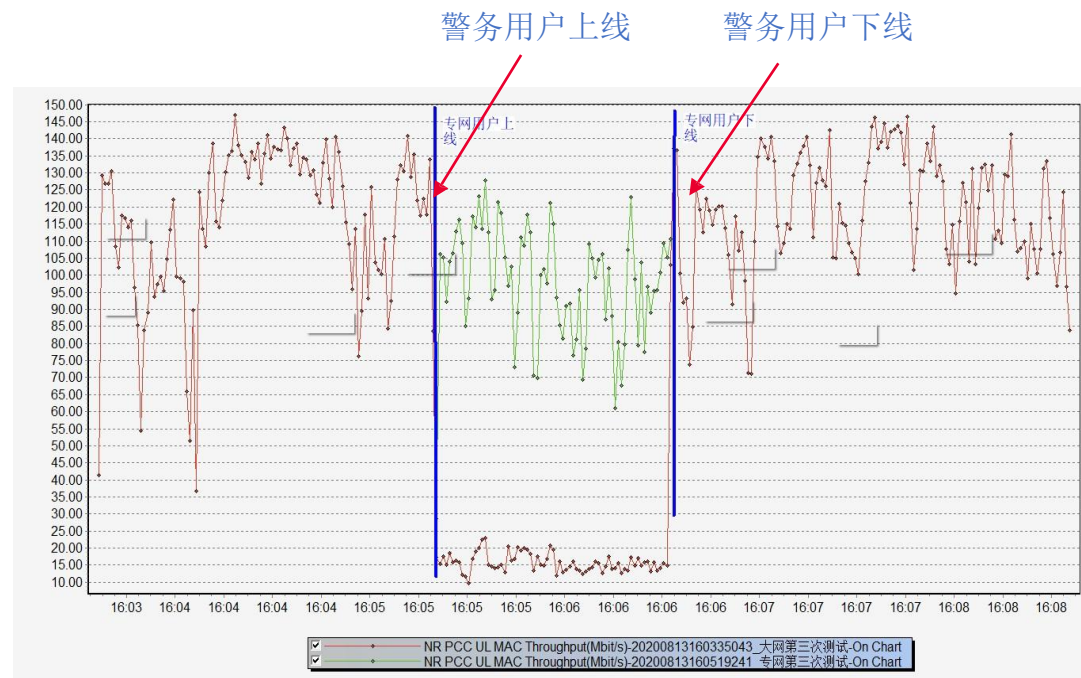
- 当前（初期）采用Qos+GBR切片方式保障警务业务优先级和带宽质量
- 后续计划采用静态/动态RB资源预留方案，使警务业务的保障能力得到更高

警务网络切片QOS测试结果

□ 【测试结果】 通过5G网络对警务专网用户配置高优先级5QI和带宽保证，可以在最大程度上保障警务专网用户的业务带宽得到优先调度， 在网络压力下配置QOS的警务用户可以抢占普通用户带宽。

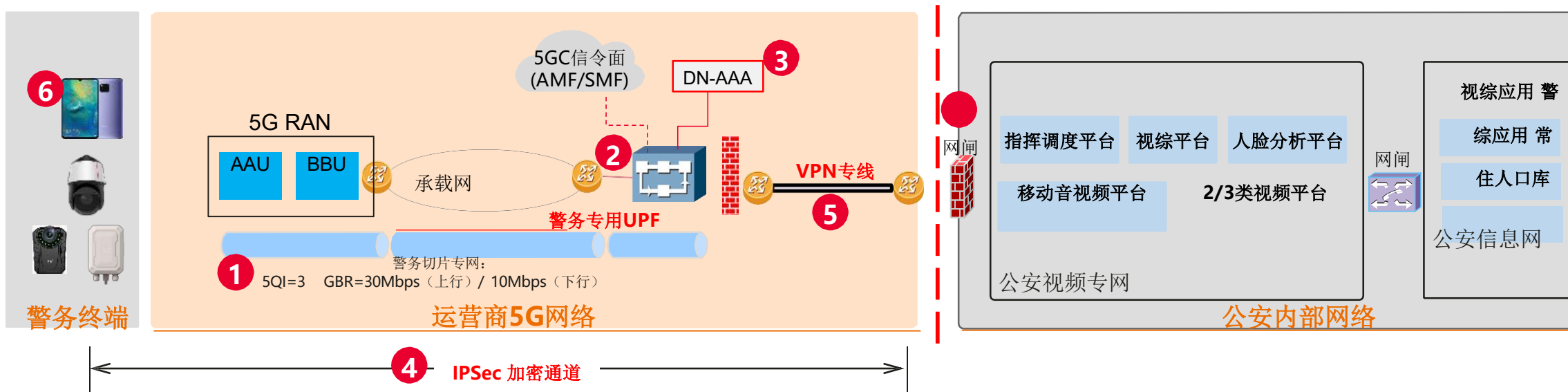


□Case1: 有网络负载的情况下，进行上传业务时，警务用户抢占普通用户带宽并达到稳定



□Case2: 有负载的情况下，进行下载业务时，警务用户抢占普通用户带宽并达到稳定

5G警务安全保障方案



资源专享

二次认证

通道安全

终端安全

边界防护

1 警务业务专用5G切片网络

2 警务专用UPF，资源隔离

3 警务DN-AAA，公安自维认证信息

- 符合认证的流量才分流公安内网

4 E2E IPSec加密通道

- 警务UPF通过VPN专线对接公安内网

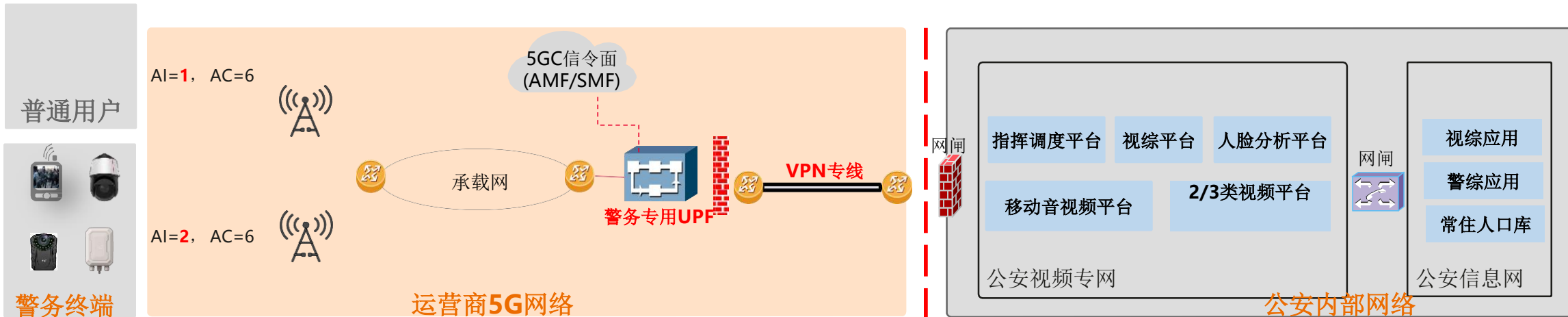
6 警务通，双系统

- MAC绑定，无法盗用

7 安全检测、扫描、诱捕、审计

- 用户接入可信
- 接口访问控制
- 可信边界网管、集控探针

优先接入：人员大量密集的应急保障场景下5G高优先接入方案



场景：警务用户应能在应急保障场景下（如重大活动保障、人员大量密集场景、自然灾害等情况下），优先使用5G网络，获得应急通信保障，支持公安等关键业务部门的特殊终端高优先接入5G网络

1、开户设置 核心网UAC配置

普通用户
AI=1, AC=6
禁止概率：0%
禁止时间：4s

警务用户
AI=2, AC=6
禁止概率：0%
禁止时间：4s

2.1、拥塞场景：

普通用户接入概率降低，保证警务用户优先接入

普通用户
AI=1, AC=6
禁止概率：90% ↑
禁止时间：30s ↑

警务用户
AI=2, AC=6
禁止概率：0%
禁止时间：4s

无线RACH通过AI优先接入

- 警务用户在核心网配置特定Access Identity
- 拥塞情况：触发UAC（统一接入控制）：
 - ✓ 特定AI警务用户接入概率不受流控影响
 - ✓ 普通用户接入概率可设置降低

2.2、极端场景：

小区预留，仅警务用户可接入

普通用户
AI=1, AC=6
禁止概率：0%
禁止时间：4s

警务用户
AI=2, AC=6
禁止概率：0%
禁止时间：4s