

移动CT车5G专网接入卫生专网技术方案

一、需求概述

1. 业务场景

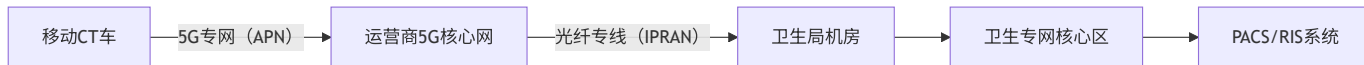
- 移动CT车通过中国电信5G专网将采集到的影像等数据，经车载CPE终端的5G网络再回传至卫健局数据机房，保障实时传输CT影像、患者数据至卫生专网（PACS系统）。
- 5G网络切片技术实现全链路封闭（与互联网物理隔离），符合医疗数据安全要求。
- 运营商机房通过将专用IPRAN传输设备下沉卫生局机房，光纤专线接入卫生专网。

2. 核心需求

- 封闭性**：5G专网与互联网完全隔离，运营商侧新建独立逻辑网络APN，限制互联网访问。
- 高带宽**：单台CT车需≥200Mbps带宽（支持DICOM影像实时传输）。
- 低时延**：端到端时延≤50ms（确保远程诊断流畅性）。
- 安全性**：数据加密+终端准入+传输通道隔离。

二、网络架构设计

1. 整体拓扑（封闭式组网）



2. 关键组件说明

节点	设备/技术	功能说明
移动CT车	5G CPE（如华为5G Industrial Router）	通过运营商分配的唯一APN接入5G专网，支持VPN加密隧道。
运营商机房	5G核心网UPF（用户面功能）	数据流量本地卸载，通过光纤专线直连卫生局，不经过互联网。
卫生局接入层	防火墙（如华为USG6600）	对CT车数据做IPS/IDS检测，并通过IPSec VPN与运营商机房建立加密通道。
卫生专网核心	高性能交换机（如H3C S10500）	提供DICOM影像数据的高速转发，QoS优先级标记（DSCP 46）。

三、关键技术实现

1. 5G专网隔离方案

- **独立APN：**
 - 运营商为CT车分配专用APN，与公众5G网络逻辑隔离。
 - 专用手机卡绑定固定IP地址，限制接入设备IMSI/IMEI和卡号白名单，未授权用户无法接入专用APN逻辑网络。
- **网络切片（可选）：**
 - 申请5G uRLLC切片，保障低时延和高优先级传输。

2. 数据传输安全

- **端到端加密：**
 - CT车CPE与卫生局防火墙之间部署**IPSec VPN**（IKEv2+国密SM4算法）。
 - DICOM文件传输启用**DICOM TLS**（端口2762加密）。
- **终端准入控制：**
 - 卫生专网侧部署**Radius服务器**，CT车需证书+MAC地址双认证。

3. 链路可靠性

- **主备双链路：**
 - 主链路：5G专网（200Mbps）。
 - 备用链路：车载LTE路由器（通过运营商4G VPDN接入，带宽50Mbps）。
- **心跳检测+自动切换：**
 - 通过BFD协议检测链路状态，故障时5秒内切换至备用链路。

四、设备选型与配置

设备类型	推荐型号	配置要点
5G CPE	华为 5G CPE 5	支持5G、WiFi6、双千兆口，支持APN接入点网络配置和5G SA网络。
运营商UPF	华为E9000-H	本地分流CT车数据，与互联网隔离。
卫生局防火墙	深信服AF-4000	启用IPS+防病毒，日志留存≥180天。
光纤专线	运营商MPLS专线	带宽≥500Mbps，SLA承诺99.9%可用性。

五、实施步骤

1. Phase 1：
- 运营商部署5G专网APN，完成UPF数据分流配置。

- CT车安装5G CPE，测试APN接入与VPN连通性。

2. Phase 2:

- 运营商开通至卫生局的光纤专线，防火墙策略联调。
 - 卫生专网侧配置DICOM服务器接收策略（如AE Title权限）。
-

六、运维与保障

- **实时监控：**

- 通过Zabbix监控5G信号强度、专线延迟、防火墙会话数。

- **应急响应：**

- 运营商IPRAN传输设备下沉卫生局机房，上联光纤不同光缆经双路由环路保护，保障链路安全可用；备用IPRAN传输设备充足，设备硬件故障时可短期内迅速修复。

- **合规性：**

- 符合《医疗卫生机构影像数据安全指南》《5G医疗专网建设规范》。