

5G 视频终端 NAT 穿越的 技术挑战与对策

Technical Challenges and Strategies for NAT Traversal in 5G Video Terminals

张建东 (华数传媒网络有限公司, 浙江 杭州 311258)
Zhang Jiandong (Huashu Media Network Co., Ltd., Hangzhou 311258, China)

摘要:

针对 5G 网络下视频监控系统面临的 NAT 穿越问题,提出了 5 种技术方案。通过分析固网与 5G 接入的差异,探讨了主流视频协议的特性,并详细评估了 DNAT、5G LAN、视频接入网关、GB/T28181 和后路由方案的适用性、成本与技术难度。这些方案能有效解决 NAT 穿越问题,为视频监控系统在 5G 时代的部署提供参考,增强了系统的稳定性和性能。

关键词:

5G; 视频监控; NAT 穿越; 无线接入; 5G RedCap; 双向访问
doi: 10.12045/j.issn.1007-3043.2025.08.009
文章编号: 1007-3043(2025)08-0040-07
中图分类号: TN915
文献标识码: A
开放科学(资源服务)标识码(OSID): 

Abstract:

It proposes five technical strategies to addresses the NAT traversal issues faced by video surveillance systems under 5G networks. By analyzing the differences between fixed network and 5G access, it explores the characteristics of mainstream video protocols and evaluates in detail the applicability, cost, and technical difficulty of DNAT, rear routing, 5G LAN, video access gateway, and GB/T28181 solutions. These strategies can effectively solve the NAT traversal problem, providing reference for the deployment of video surveillance systems in 5G era and enhancing the stability and performance of the systems.

Keywords:

5G Network; Video surveillance; NAT traversal; Wireless access; 5G RedCap; Bidirectional access

引用格式: 张建东. 5G 视频终端 NAT 穿越的技术挑战与对策[J]. 邮电设计技术, 2025(8): 40-46.

0 引言

在视频监控系统中,网络接入方式对实现高效、可靠的监控至关重要。传统的有线接入,如 PON 光纤线路,虽然稳定但部署成本高,且不够灵活。随着 5G 技术的兴起,其无线接入能力为视频监控提供了新的解决方案,尤其是在光纤难以覆盖或需要快速部署的情况下。然而,无线接入也带来了新的技术挑战,其中最显著的便是 NAT 穿越问题。由于 5G 无线接入增

加了一个路由网段,导致视频监控平台难以实现对前端 IPC 或物联网设备的反向访问,这对需要双向通信的视频监控系统是个关键的技术障碍。

为了克服这一挑战,本文提出了 DNAT、5G LAN、视频接入网关、GB/T28181 和后路由等 5 种不同的技术方案。本文将对这些方案的技术原理、优势、局限性以及适用场景进行详尽的分析和讨论,旨在为视频监控系统在 5G 时代的部署提供指导和参考。

1 固网与移网接入的差异

1.1 固网接入的拓扑

收稿日期: 2025-07-16

如图 1 所示,在网络摄像头(IPC)或者 NVR 设备的以太网口上配置业务 IP 地址,视频监控业务 IP 地址

的网关配置在运营商的 MPLS PE 设备上,视频监控平台与前端设备之间可以实现双向访问。

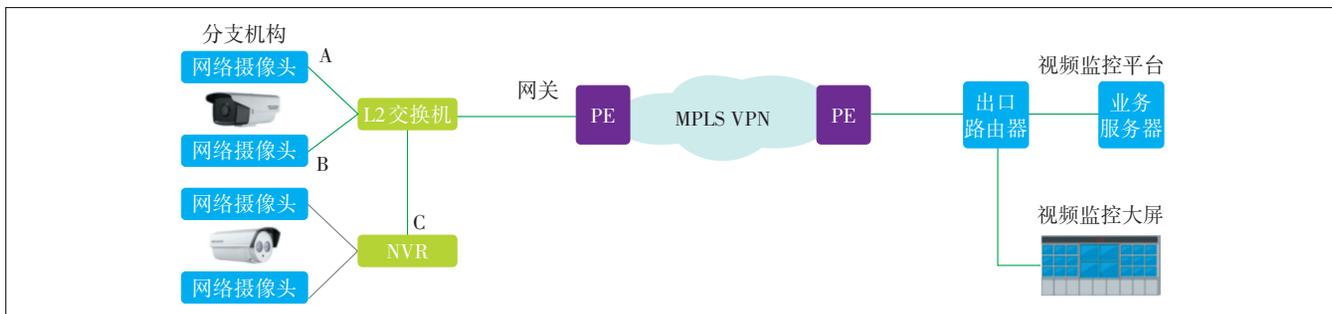


图 1 固网接入拓扑

1.2 5G 接入的拓扑

如图 2 所示,在 5G 网络中配置 IPC 或 NVR 设备时,业务 IP 地址通常配置在设备的以太网接口上,业务网关配置在 5G 路由器的 LAN 接口。与固网不同的是,5G 网络分配的 IP 地址位于 5G 路由器的无线 WAN

接口上。IPC 可以通过 SNAT 主动通过 5G 路由器访问视频监控平台,但反向访问时,由于 5G UPF 无法路由 IPC 的业务 IP 地址,导致通信失败。为实现双向通信,需选择适合 5G 网络结构的解决方案,确保 IPC 的业务 IP 地址能够被正确路由。

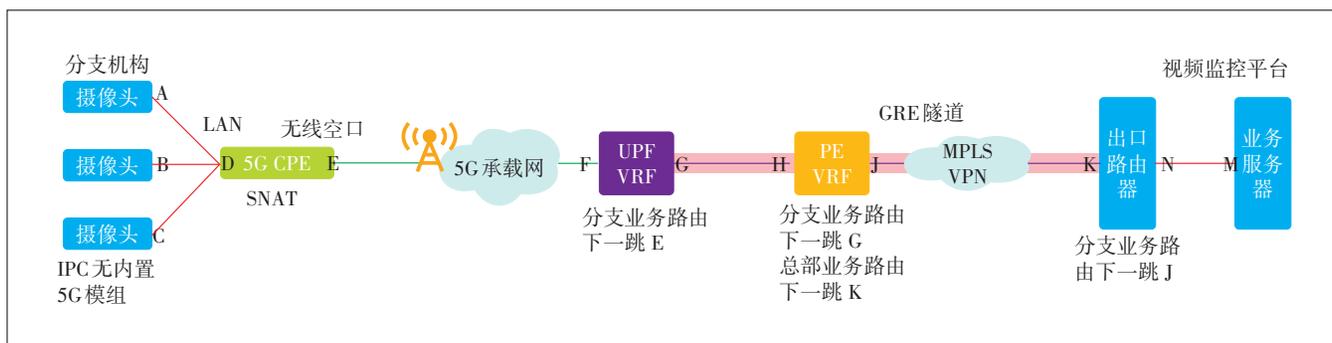


图 2 5G 接入的拓扑

2 视频协议比较

目前主流网络摄像头支持 4 种接口协议(API): ONVIF^[1]、ISAPI、SDK 和 GB/T28181(2016),这些主流视频协议的差异如表 1 所示。从表 1 可以看出,只有

表 1 4 种主流视频协议的差异

协议类型	ISAPI ^[2]	ONVIF	SDK	GB/T28181
传输协议	HTTP/TCP	HTTP/TCP	HTTP/TCP	SIP/TCP、UDP
取流协议	RTSP	RTSP	RTSP	SIP
通信安全	HTTPS 敏感数据加密	HTTPS	HTTPS	TLS
设备接入方式	被动	被动	被动	主动
协议风格	Restful	SOAP	SOAP	SOAP
文本格式	XML、JSON	XML	XML	XML
认证方式	摘要认证	摘要认证	摘要认证	摘要认证、数字证书认证

GB/T28181 支持前端设备的主动接入方式,可以解决视频监控平台反向主动访问前端 IPC 的问题,其他协议都存在后台无法反向访问前端的问题。

3 5 种 NAT 穿越的解决方案

3.1 DNAT 方案

DNAT 方案的拓扑如图 3 所示,具体步骤如下。

a) 当 IPC 正向访问视频服务器时,5G 路由器自动建立动态 NAT 会话表项^[3],将 IPC 的业务 IP 地址+端口做 SNAT 转换,将源地址转换为 5G 路由器 WAN 口的 IP 地址+端口。由于 WAN 口 IP 地址可以被 UPF 路由,所以业务正常。

b) 当视频服务器反向访问 IPC 时,由于 5G 核心网 UPF 只能路由寻址到 5G 路由器的 WAN 无线接口的 IP 地址,无法感知 5G 路由器 LAN 接口的 IP 网段,且由于

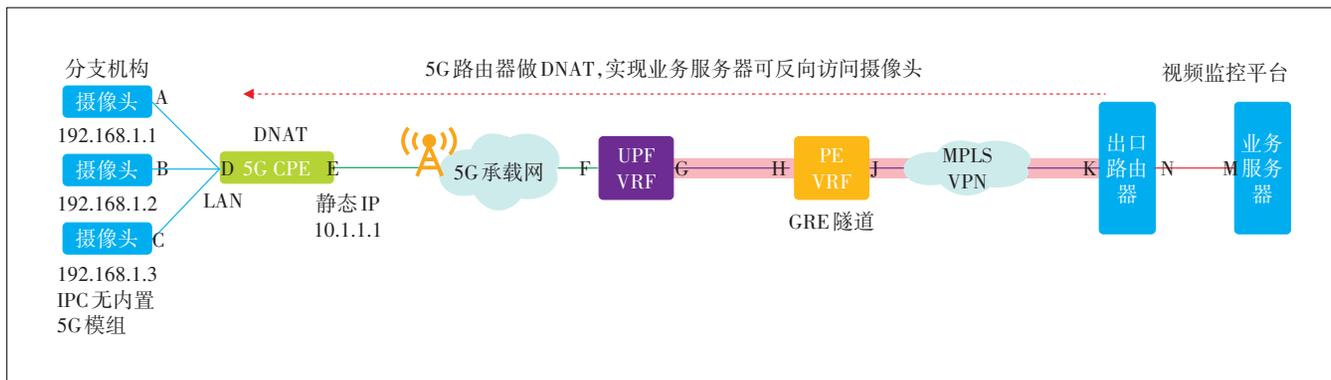


图3 DNAT拓扑

5G 路由器上并没有 NAT 表项, 因为之前 IPC 正向访问服务器时动态建立的 NAT 表项已经老化, 所以视频服务器无法反向访问前端 IPC 或 NVR 设备, 要实现反向访问, 就需要在 5G 路由器上配置 DNAT 功能, 在 5G 路由器上生成静态 NAT 表项, 从而实现服务器反向访问 IPC。

c) DNAT 方案适用场景为前端设备采用固定 IP 地址, 接入侧的 NAT 路由器支持静态 DNAT 功能, 摄像头至监控平台只经过一次 NAT。如果前端设备采用动态 IP 地址或者经过多次 NAT 的场景, 则不适合采用本方案。

3.2 5G LAN 方案

5G LAN 协议栈示意如图 4 所示。传统 5G 在承载此类业务时, 只能提供网关级的地址管理和访问, 无法提供 CPE 向的行业终端的管理和访问, 需叠加 DNAT、后路由等复杂的辅助方案, 因而组网复杂、维护成本高。传统通信方案仅提供终端 IP 层数据的承载功能, 5G LAN 则支持 5G VN 组成员通过 Ethernet 的 PDU 会话接入^[4], 提供终端数据链路层的承载与通信。从协议栈角度来看, 5G LAN 技术方案对传统 5G 方案

进行了优化。

对于传统 PDU 会话接入, DN 网络只能感知到 UE 的 IP 层及以上的数据信息; 在行业终端通过 CPE 网关接入组网情况下, DN 网络只能感知到 CPE 的 IP 地址信息。即在传统 5G 通信模式下, 服务端只能感知到末端网络设备, 若末端网络设备再下挂额外设备则无法感知。

在 Ethernet PDU 会话接入下, DN 网络可以感知到 UE 的 MAC 层及以上的数据信息; 在行业终端通过 CPE 网关接入的情况下, DN 网络可以直接感知到 CPE 向行业终端中的 MAC 层及以上数据信息, 类似于有线接入。即在 5G LAN 通信模式下, 服务端可以感知到末端网络设备, 即使末端网络设备再下挂额外设备, 服务端也能感知。由此可见, 5G LAN 通过支持 Ethernet PDU 会话^[5], 实现了 5G 对行业终端数据更强的感知、承载和传输能力^[6-7]。

CPE 路由器作为二层桥接设备, 可以挂载多个终端, 直接传输 Ethernet 报文, UPF 实现交换机功能, 按照 MAC 地址转发以太网帧, SMF 管理路径, 识别转发环路。

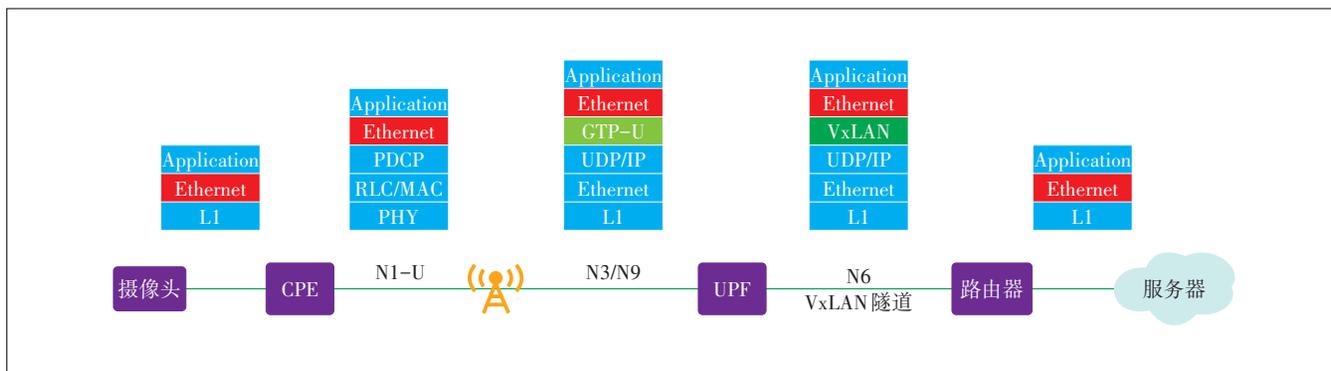


图4 5G LAN协议栈示意

5G LAN 方案拓扑如图 5 所示。

3.3 视频接入网关方案

如果客户的视频摄像头 IPC 或 NVR 采用 5G 无线网络做视频回传,使用动态 IP 地址接入,视频监控平台部署在公有云或私有云上,前端设备与视频平台之间经过了多次 NAT,那么很难使用 DNAT 方案或者后路由的方案来实现反向访问。

视频接入网关方案就是视频接入网关必须一直保持住与前端视频终端的 TCP 长连接不释放,此连接是终端主动联系服务器的正向访问,由于终端的 IP 地址和端口不变,5G 路由器上的 NAT 会话不会超时老化,所以可以确保服务器反向访问终端是正常的。在设计视频接入网关方案时,确保与前端视频终端的 TCP 连接的持久性是关键^[8]。终端通过主动建立 TCP 连接访问服务器,由于终端的 IP 地址和端口保持不变,5G 路由器上的 NAT 会话不会超时,从而保证了服务器能够反向访问终端。

在正向访问过程中,5G 路由器通过 SNAT 创建 NAT 会话表项。这些表项在未达到老化时间前是有效的,允许进行通信。但在反向访问时,若没有相应的目的 DNAT 条目,并且 NAT 会话表项由于长期无活动而被系统老化删除,这将导致反向访问无法正常进行。因此,为了维持双向通信的连续性,视频接入网关的设计需要考虑 NAT 会话的持久性,确保在反向访问时,相关的 NAT 会话表项不会因为空闲超时而失效。

视频接入网关方案通过视频终端主动上报实现反向访问,在业务服务器一侧部署 2 台服务器,一台用于信令注册管理,一台用于流媒体服务。具体流程分为以下 3 个步骤。

第 1 步:信令注册与 TCP 长连接建立。摄像机配置有信令注册服务器的 IP 地址和端口信息。基于此配置,摄像机初始化一个 TCP 连接至信令注册服务器。

一经服务器认证通过,该 TCP 连接将被持久维持,以确保信令通信的连续性。

第 2 步:信令指令的转发与命令执行。当用户请求实时视频图像或希望对摄像机执行反向控制操作时,信令注册服务器接收来自客户端(电脑或移动设备)的请求命令。服务器随后将该请求转换为预定义的指令格式,并利用已建立的 TCP 长连接(即 Socket),将指令发送回摄像机。

第 3 步:媒体流的建立与传输。摄像机在接收到指令后,若确认该指令是针对本机,则将独立创建一个新的通信通道,该通道可以是基于 TCP 或 UDP 协议。摄像机通过此通道将流媒体推送至信令服务器所指定的 IP 地址和端口。流媒体服务器在接收到视频流信息后,将其转发至请求的移动端或电脑端,完成实时视频的传输。

3.4 GB/T28181 方案

《安全防范视频监控联网系统信息传输、交换、控制技术要求》(GB/T28181)是由公安部科技信息化局提出,由全国安全防范报警系统标准化技术委员会(SAC/TC100)归口,公安部一所等多家单位共同起草的一部国家标准^[9-10]。

GB/T28181 解决的一个主要问题就是如何远程、跨区域、跨级别的访问网络中的监控设备(IPC、NVR)。在没有 GB/T28181 协议之前,想要远程访问某个局域网中的监控摄像头相当麻烦,通常要进行动态 IP 地址映射、端口映射、动态域名绑定等操作,在稳定性和易用性方面都较差。

GB/T28181 平台由管理平台、信令服务器、流媒体服务器、监控设备(IPC、NVR)、管理终端等几部分组成(见图 6)。信令服务器是与网络中监控设备与管理终端之间进行通信的代理,也是各级系统之间的代理,信令服务器要有固定的 IP 地址或域名,如果要面向公网服务,还需要有公网 IP 地址。由于是监控设备

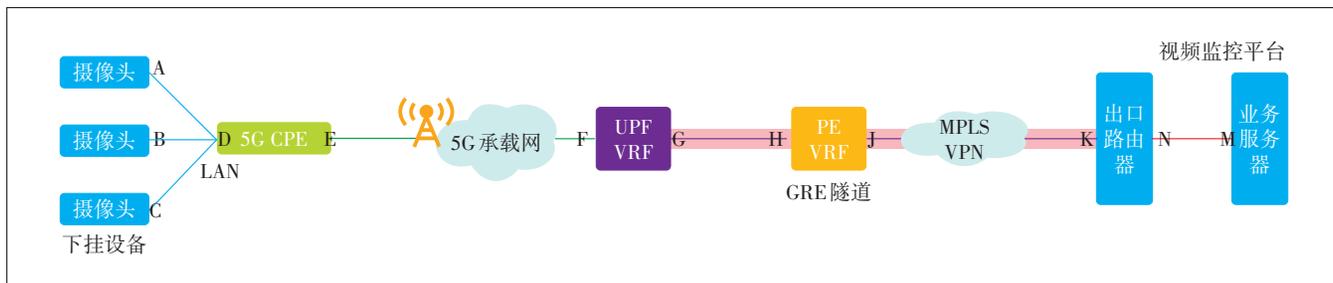


图 5 5G LAN 方案拓扑

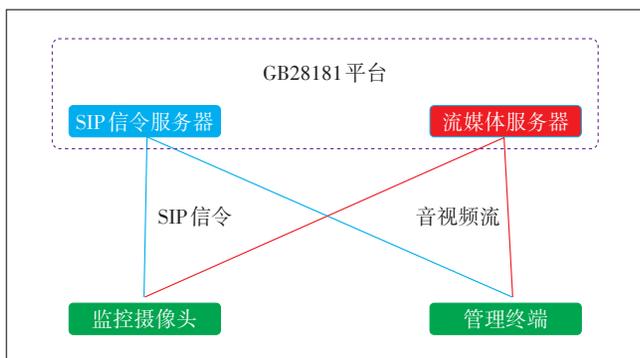


图6 GB/T28181方案示意

主动向信令服务器注册,所以监控设备不需要有固定的IP地址。监控设备注册到信令服务器上之后,管理者通过向信令服务器发送指令来管理监控设备。流媒体服务器是视频传输的代理,该系统接受监控设备发送的视频流,向视频调取方转发视频。视频调取方可以是监控视频的用户、第三方业务系统或者是上下级平台。协议规定监控设备通过RTP协议向流媒体服务器发送视频流,但是没有约定流媒体服务器向其他方转发视频的协议,因此在视频转发时具有更大的灵活性,可以根据需要采用合适的协议转发视频。

由于GB/T28181采用的是SIP的注册机制,如果前端视频设备和后端视频平台都支持GB/T28181标准,则可以解决NAT穿越问题,满足客户反向访问监控前端的需求。

3.5 后路由方案

3.5.1 后路由技术概述

后路由(Frame Routing)技术是5G网络中的一项关键功能^[1],它支持UE后面的IP网络,允许多个IP地址或多个IPv6前缀,通过单个PDU会话实现与远端网络进行数据交互,也支持UE下挂设备之间或者与UE互通,UE即5G路由器。这一技术的核心优势在于它能够使网络中的服务器主动感知并管理连接到UE的终端设备,即便这些设备是通过UE的网络接口间接接入的。这对于需要远程控制和设备管理的应用场景(如视频监控、物联网(IoT)设备管理等)具有重要意义。后路由技术方案示意如图7所示。

在企业专网的业务中,存在服务器对终端进行反向控制的需求,由于终端通过CPE获取本身的地址,服务器端无法获得终端IP地址,也就无法进行反向控制。需要通过帧路由技术,实现服务器对终端地址的感知和反向控制。后路由技术通过在UDM中配置连

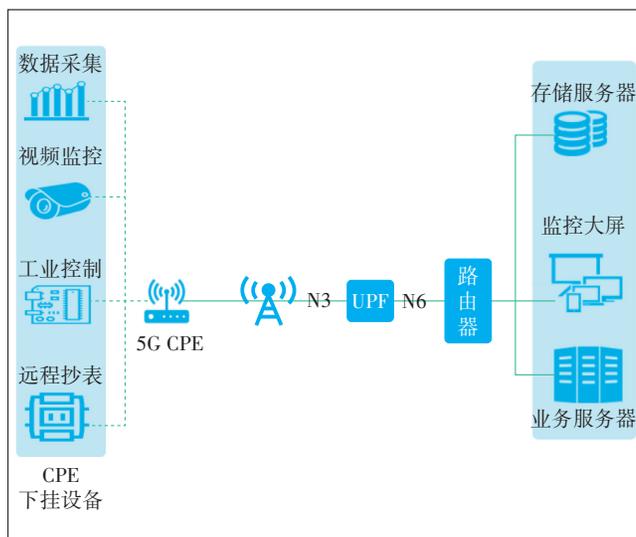


图7 后路由技术方案示意

接到CPE下的终端的IP地址,SMF将终端的IP地址发送到UPF,从而企业服务器可获取到终端的IP地址,实现对终端设备的直接管理和维护。通过UE后路由,可以实现应用服务器和UE下挂网络设备的互联互通,如用于企业网专网资源连接,部分业务服务器需要反向控制终端进行软件升级,实时播放UE下挂网络摄像头采集到的视频信息,通过UE下挂设备直接操作DN侧设备等。

UPF可以设置UP Function Features IE中的FRRT标志位来告诉SMF支持后路由特性。当SMF确认UPF支持后路由时,通过以下步骤来指示UPF启用后路由特性。

- 下发的PDR规则携带Framed-Route IE、Frame-Routing IE和Framed-IPv6-Route IE。
- 对于上行用户数据分组,需将IP报文中的源IP地址与Framed-Route IE或Framed-IPv6-Route IE中的IP地址或IPv6前缀进行匹配。
- 对于下行用户数据分组,需将IP报文中的目的IP地址与Framed-Route IE或Framed-IPv6-Route IE中的IP地址或IPv6前缀进行匹配。

在UDM配置UE的IMSI号码和UE下挂设备的IP网段地址(此网段包含UE通过DHCP分配的IP地址)后,SMF会生成UE后路由转发表项并下发给UPF。当UPF收到目的地址为UE下挂设备的IP的报文后,进行如下操作。

- 查找UE后路由转发表项。
- 根据表项中的IMSI号码,UPF选择对应的GTP

隧道封装原始报文。

- c) UPF 网元将封装后的报文转发给基站。
- d) 基站收到封装后的报文后,剥离报文的外层 IP 头得到原始 IP 报文。
- e) 基站通过空中接口将原始报文转发给 UE。
- f) UE 收到原始报文后,根据报文的目 IP 地址将报文转发给下挂设备。

配置完路由后,对于支持后路由功能的 CPE,其下挂的设备可以支持与 N6 外部网络双向互联互通。如图 8 所示,由于 5G 核心网^[12-13]UPF 可以感知到 IPC 的 192.168.1.0 网段,并且有 192.168.1.0/24 下一跳为 5G 路由器 WAN 口的路由表项,下行报文到达 5G 路由器后再查本地路由表寻址转发到目的 IPC 设备。

3.5.2 后路由运行机制

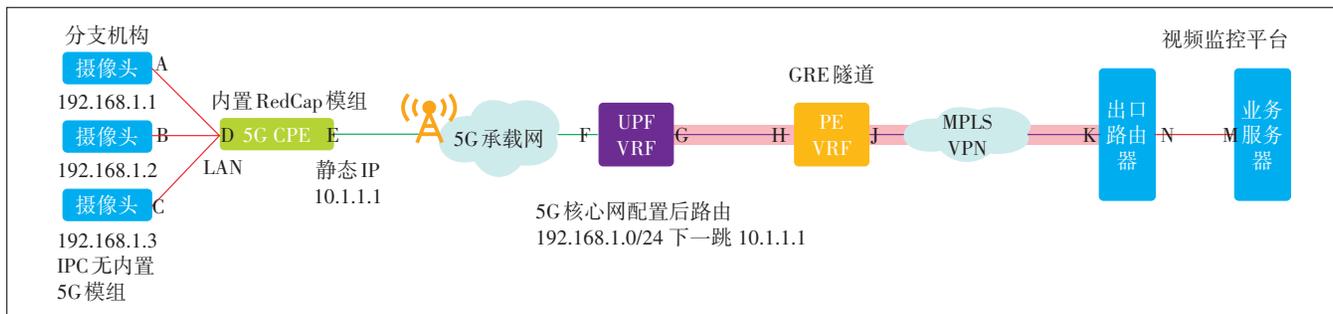


图 8 后路由方案拓扑

在转发用户平面报文时,对于上行方向,UPF 收到 gNodeB 的报文后,执行 GTP 解封装,然后将原始 IP 报文通过 N6 接口转发到 DN;对于下行方向,UPF 收到 DN 的报文后,执行 GTP 封装操作,然后将封装后的报文通过 N3 接口转发给 gNodeB。

3.5.3 后路由转发流程

UE 与 DN 网络之间的报文转发,当 UE 注册上网络后,5GC 会为 UE 分配 IP 地址。获取 IP 地址后,UE 可以访问 DN 网络内的应用。

DN 向 UE 正向发送报文的示意如图 9 所示,DN 向 UE 反向发送报文与正向发送的过程相反。

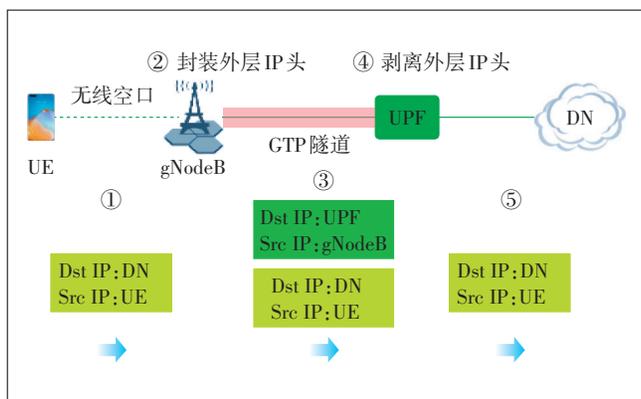


图 9 DN 向 UE 正向发送报文的示意

配置 UE 后路由后,5GC 会生成 UE 后路由转发表项^[14],该转发表项主要包含 UE 的 IMSI 号码和 UE

下挂设备的网段地址和掩码。

UE 的 IMSI 号码固定,但其入网后使用的 IP 地址不一定固定,所以后路由使用 UE IMSI 与下挂设备网段地址组成 UE 后路由转发表项。5GC 配置 UE 的 IMSI 号码和 UE 下挂设备的网段地址(此网段地址包含 UE 通过 DHCP 功能分配的 IP 地址)后,5GC 会生成 UE 后路由转发表项。当 5GC 收到目的地址为 UE 下挂设备的 IP 地址的报文后,它将查找 UE 后路由转发表项,根据表项中的 IMSI 号码,UPF 网元选择对应的 GTP 隧道封装原始报文,UPF 网元将封装后的报文转发给 eNodeB,最终将报文转发给 CPE 下挂设备。

3.5.4 后路由信令流程

有的 5G 设备厂商支持通过 UDM 配置下挂设备的 IP 网段地址后路由的部署方案,具体方案如图 10 所示。

当 UE 作为 CPE 的下挂设备时,CPE 通过 DHCP 功能为下挂 UE 分配 IP 地址。未配置后路由时,下挂 UE 获取 IP 地址后,可单向访问外部网络内的应用。但由于 UPF 无法感知到下挂设备的存在,更无任何下挂设备的 IP 表项信息,所以当 UPF 收到 N6 接口外部网络发来的报文后,仅转发目的地址为 CPE 路由器 WAN 接口 IP 地址的报文,其他报文将被丢弃,转发目的地址为下挂设备 IP 的报文也随之被丢弃。后路由仅用于 DNN 连接或 IP 类型的 DNN 会话(IPv4 或 IPv6)。

UPF 可以设置 UP Function Features IE 中的 FRRT

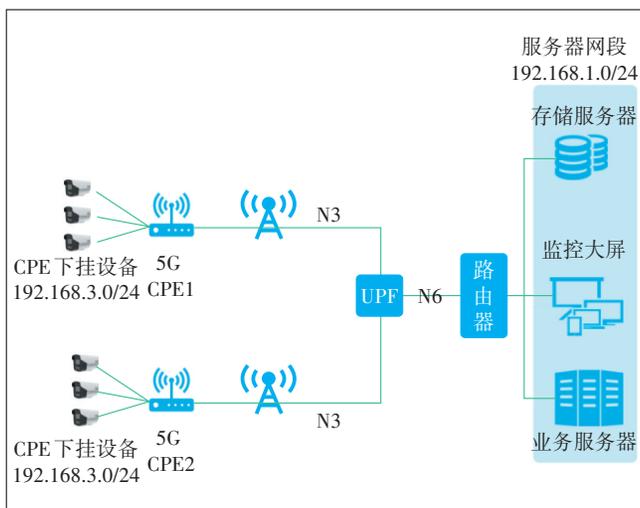


图 10 后路由部署方案拓扑

标志位来告诉 SMF 支持后路由特性。当 SMF 确认 UPF 支持后路由时,指示 UPF 启用后路由特性。在 UDM 上配置 UE 的 IMSI 号码和 UE 下挂设备的 IP 网段地址(此网段包含 UE 通过 DHCP 分配的 IP 地址)后,SMF 会生成 UE 后路由转发表项并下发给 UPF。

配置完后路由后,对于支持后路由功能的 CPE,其下挂的设备即可支持与 N6 外部网络的双向互联互通。

4 结束语

本文深入探讨了 5G 网络环境下视频监控终端面临的 NAT 穿越问题,并提出了 DNAT、5G LAN、视频接入网关、GB/T28181 和后路由等 5 种不同的技术方案。每一种方案都针对特定的应用场景和技术需求提供了有效的解决策略。

综合比较这些方案可以看到它们在部署成本、技术成熟度和实施复杂性等方面各有千秋。选择合适的方案不仅需要考虑当前的技术条件和成本效益,还应充分考虑未来的发展和可扩展性。随着 5G 技术的不断进步和应用领域的扩展,这些解决方案将有助于推动视频监控系统向更高效、更智能的方向发展。

在实际部署时,应根据项目的具体需求、资源状况以及预期的业务增长进行全面的评估和选择。通过精心设计和正确实施,这些方案将确保 5G 网络下的视频监控终端能够实现无缝的双向通信,为用户提供更加稳定和可靠的监控服务。

参考文献:

[1] ONVIF Mandarin [EB/OL]. [2025-01-12]. <https://www.onvif.org/>

ch/.

[2] 海康 ISAPI 开发手册[EB/OL]. [2025-01-12]. <https://www.iteye.com/resource/polluxsky-9144761>.

[3] 华三 NAT 技术白皮书[EB/OL]. [2025-01-12]. https://dl.h3c.com/cn/202408/15/20240815_11928787_99-%e6%95%b4%e6%9c%ac%e6%89%8b%e5%86%8c_2240063_30005_0.pdf?signature=80c3ca030c18163d68a496c442120ea1×tamp=1741771432.

[4] 5G LAN 赋能工业互联网产业发展白皮书(2023)[EB/OL]. [2025-01-12]. <https://max.book118.com/html/2025/0107/6003131203011022.shtm>.

[5] 江林华. 5G NR 新空口技术详解[M]. 北京:电子工业出版社, 2021: 78-84.

[6] 3GPP. Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN): 3GPP TS 29.061 [S/OL]. [2025-01-12]. ftp://3gpp.org/Specs/2024-03/Rel-15/29_series/.

[7] 3GPP. Interworking between 5G Network and external Data Networks: 3GPP TS 29.561 [S/OL]. [2025-01-12]. [ftp://3gpp.org/Specs/2024-03/Rel-15/29_series/3GPP TS 29.561](ftp://3gpp.org/Specs/2024-03/Rel-15/29_series/3GPP%20TS%2029.561).

[8] 视频安全接入系统(V1.2)技术白皮书[EB/OL]. [2025-01-12]. https://wenku.baidu.com/view/6ce2f1427d21af45b307e87101f69e314332fa81.html?_wkt_s_ =1741848762796&bdQuery=%E8%A7%86%E9%A2%91%E6%8E%A5%E5%85%A5%E7%BD%91%E5%85%B3%E6%8A%80%E6%9C%AF%E7%99%BD%E7%9A%AE%E4%B9%A6.

[9] 公安部. 公共安全视频监控联网系统信息传输、交换、控制技术要求:GB/T 28181-2016[S]. 北京:中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会, 2016.

[10] 公安部. 公共安全视频监控联网系统信息传输、交换、控制技术要求:GB/T 28181-2022[S]. 北京:中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会, 2022.

[11] H3C 4G UE 后路由技术白皮书[EB/OL]. [2025-01-12]. <https://www.h3c.com/cn>.

[12] 华三 MPLS 技术白皮书[EB/OL]. [2025-01-12]. https://www.h3c.com/cn/Service/Document_Software/Document_Center/.

[13] 5G-Advanced 核心网演进白皮书[EB/OL]. [2025-01-12]. https://roll.sohu.com/a/741463906_121656383.

[14] 华三 GRE 隧道技术白皮书[EB/OL]. [2025-01-12]. https://www.h3c.com/cn/Service/Document_Software/Document_Center/.

作者简介:

张建东,高级工程师,学士,主要从事 5G 核心网、承载网、接入网、IP 城域网的规划和维护工作。

