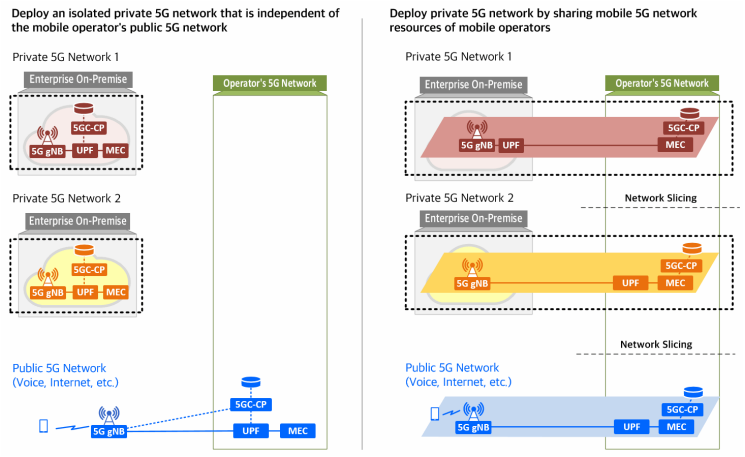
专用5G网络的7种部署方案

SDNLAB君 • 19-10-23

实现5G的应用，首先需要建设和部署5G网络，在本文中，我们将分析如何构建一个专用5G网络，专用5G网络可以通过以下两种方式实现。

第一种是部署物理隔离的专用5G网络（5G孤岛），该网络独立于移动运营商的公共5G网络（就像在企业中建立有线局域网或Wi-Fi WLAN）。在这种情况下，企业或移动运营商可以建立专用的5G网络。第二种是通过共享移动运营商的公共5G网络资源来构建专用5G网络。在这种情况下，运营商将为企业建立专用的5G网络。



1）企业自建5G局域网（本地5G频率，完全私有，不共享）

2）移动运营商构建的隔离5G局域网（许可频率，完全私有，不共享）

3）公网和专网之间的RAN共享

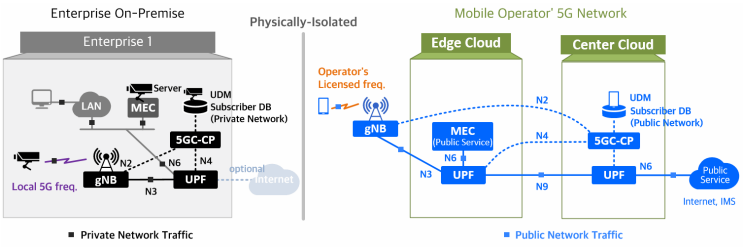
4）公网和专网之间的RAN和控制平面共享

5）公网和专网之间的RAN和核心共享（端对端网络切片）

6）N3 LBO(Local Breakout)

7）F1 LBO(Local Breakout)

1.企业自建5G局域网（本地5G频率，完全私有，不共享）



企业在其场地（站点/建筑）内部署全套5G网络（gNB，UPF，5GC CP，UDM，MEC）。企业中的5G频率是本地5G频率，而不是移动运营商的授权频率。对于私人频率由政府分配的国家，这是一种可构建的体系结构（目前在日本、德国和美国等先进国家是可实施的）。

由谁建立：在这种情况下，通常企业会建立自己的私有5G网络，但是根据各国政府的政策，包括移动网络运营商在内的第三方可能会帮助企业建立私有5G网络。

企业可以使用本地5G频率构建自己的5G局域网，从而摆脱传统的有线局域网和无线局域网的烦恼（有线局域网的局域网电缆布线工作，距离短，无线局域网的安全性和网络稳定性）。此外，5G技术的超低延迟和超大连接可创建新的企业应用或优化现有应用程序。

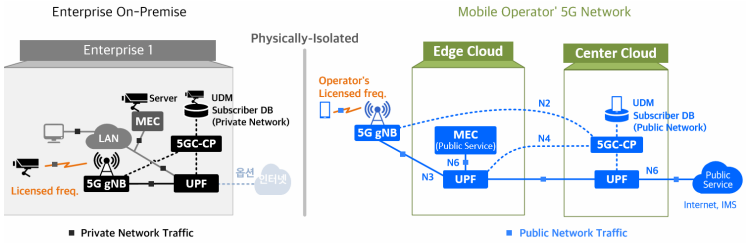
优点：企业内部有独立的5G网络全套设备。

- 隐私和安全性：专用网络与公用网络物理隔离，提供完整的数据安全性（从专用网络设备产生的数据流量，专用网络设备的订阅信息和操作信息，仅在企业内部存储和管理。企业内部数据不外泄）
- 超低延迟：由于设备和应用程序服务器之间的网络延迟在几毫秒内，因此可以实现URLLC应用服务。
- 独立性：即使移动运营商的设施烧毁，该公司的5G专用网络也可以正常工作。

缺点：

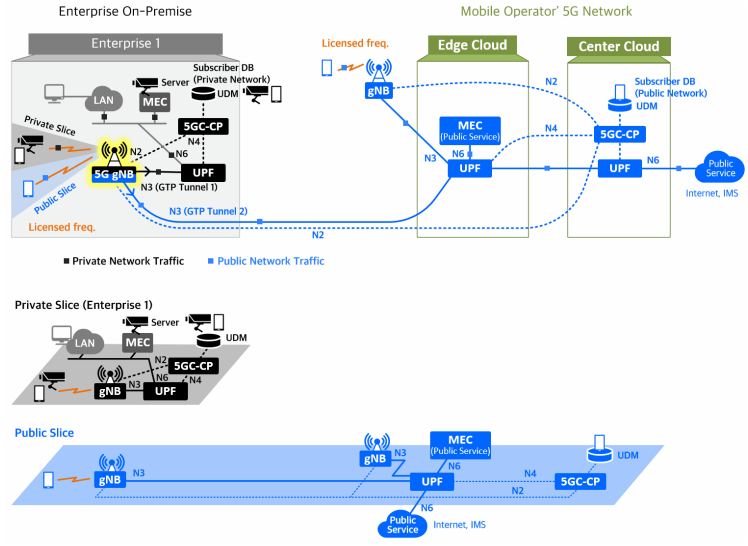
- 部署成本：普通企业，特别是小型企业要自费购买和部署全套5G网络并不容易。
- 运营人员：现有的专用局域网（有线以太网局域网，无线Wi-Fi局域网）运营团队没有构建和运营5G网络的专业知识，企业需要有合适的工程师。

2.由移动运营商构建的隔离5G局域网（获得许可的5G频率，完全私有，不共享）



专用5G网络架构与方案1相同。它们之间唯一的区别是，移动运营商在企业中使用自己许可的5G频率构建和运行5G局域网。

3.公网和专网之间的RAN共享



UPF、5GC CP、UDM和MEC部署在企业中，并与公共网络在物理上是隔离的。

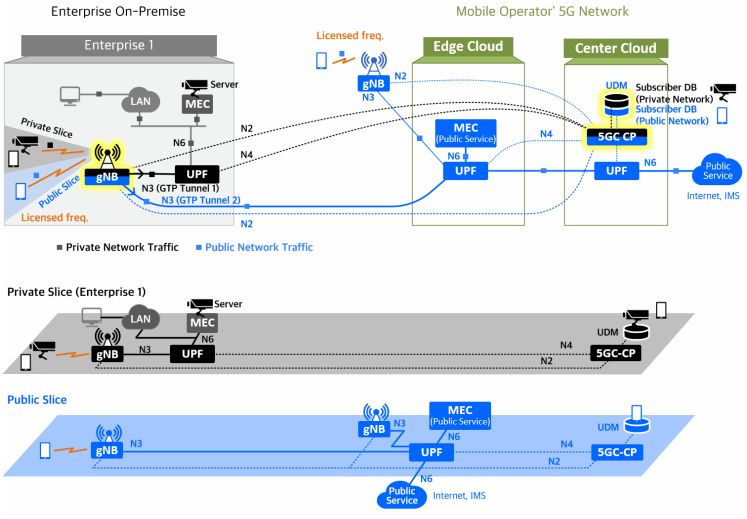
专用网络和公共网络之间仅共享企业内部的5G基站（gNB）（RAN共享）。

属于私有切片（专用网络）设备的数据流量被传递到企业中的私有UPF，属于公共切片（公用网络）的设备的数据流量交付给移动运营商的边缘云的UPF。换句话说，内部设备控制的数据、内部视频数据等之类的专用网络流量仅保留在企业中，而像语音和Internet之类的公共网络服务流量则被传输到移动运营商的网络。尽管基站不是物理上而是逻辑上分离的，但是在RAN级别的私有网络中收集数据信息几乎是不可能的，因此企业中专有网络数据流量的安全性得到了保证。

私人专用的5GC CP和UDM内置在企业中，因此企业中专用网络设备的订阅信息和操作信息可以在内部存储和管理，以免泄漏到企业外部。

UPF和MEC位于企业中，可在device-gNB-UPF-MEC之间提供超低延迟的通信，这种方法非常适合使用URLLC应用程序的公司，例如自动驾驶和实时机器人、无人机控制。

4.公网和专网之间的RAN和控制平面共享



私人专用的UPF、MEC内置于企业中。企业中的5G基站（GNB）和移动运营商边缘云中的5GC CP、UDM在专用

网络和公共网络之间共享（RAN和控制平面共享）。
gNB、5gcp和udm在专用网和公用网之间逻辑上分开，
UPF和MEC在物理上分开。

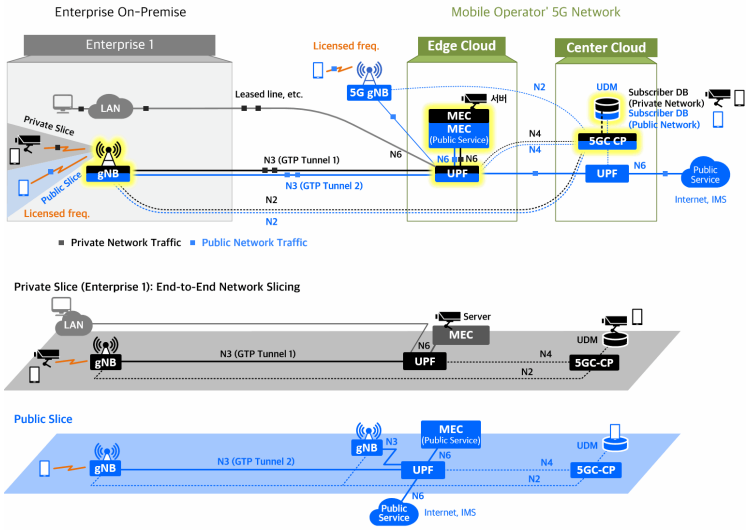
属于私有切片（专用网络）设备的数据流量被传递到企业中的私有UPF，属于公共切片（公用网络）的设备的数据流量被传递到移动运营商边缘的UPF。如同3中RAN共享一样，内部设备控制的数据、内部视频数据等之类的专用网络流量仅保留在企业中，而像语音和Internet之类的公共网络服务流量则被传输到移动运营商的网络，企业内部数据流量的安全性也很明确。

专用网络设备和公用网络设备的控制平面功能（身份验证，移动性等）由移动运营商网络中的5GC CP和UDM执行。

也就是说，企业中的专用网络设备、gNB和UPF与移动运营商的网络互通并由其管理（通过N2，N4接口）。可能存在的问题是，私有网络设备的操作信息和订阅信息存储在移动运营商的服务器中，而不是存储在内部。

和3的情况一样，由于UPF和MEC位于企业中，因此它提供了设备-gNB-UPF-MEC之间的超低延迟通信，并且适合使用URLLC应用程序的公司。

5.公网和专网之间的RAN和核心共享（端到端网络切片）



当gNB部署在企业内部，UPF和MEC只存在于移动运营商的边缘云中时，专用网和公网共享“逻辑上分离的5G RAN和核心”（GNB、UPF、5GC、MEC、UDM）（端到端网络切片）。

与UPF和MEC位于企业中的3、4不同，在这种情况下，企业中只有gNB。私有5G设备与Intranet（LAN）设备（PC或本地Intranet服务器）之间没有本地流量路径，因此流量必须到达运营商边缘云中的UPF，然后通过专线回到企业内部，与局域网设备进行通信。

此外，为企业中的5G设备提供5G应用服务的MEC位于移动运营商边缘云中。

在这种架构中，网络延迟（RTT）可能是一个主要问题，延迟的时间取决于企业（5G设备）和运营商边缘云（UPF、MEC）之间的距离。

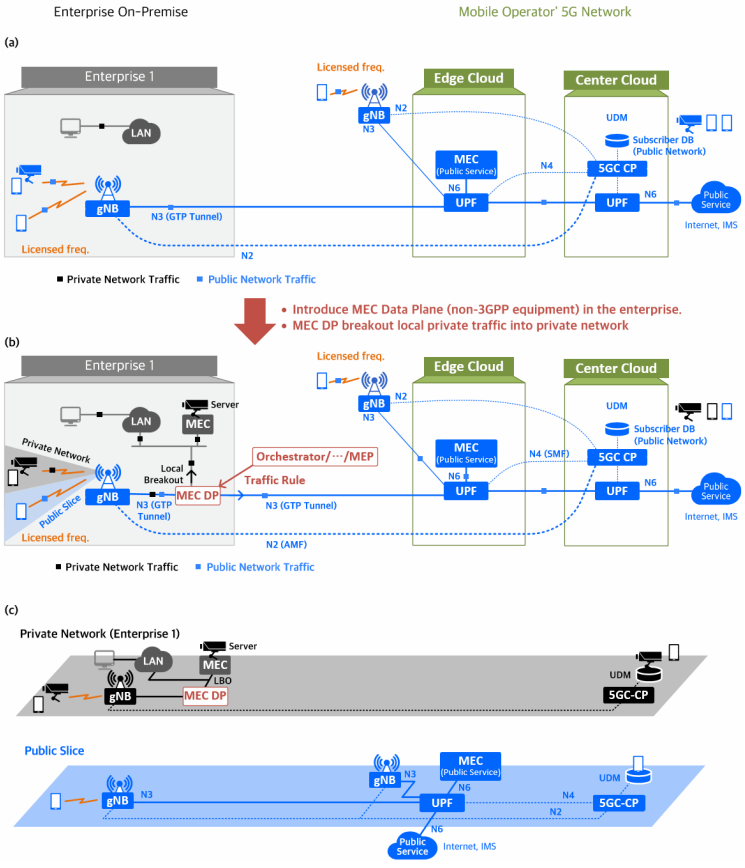
由于专用网络设备的流量是从企业转移到移动运营商的网络，因此存在数据流量安全的问题。虽然移动运营商将在其边缘云上分割UPF和MEC，以使我们的私有网络流量与公共和其他私有网络流量分开，但企业内部的私密流量外泄是令人担忧的。

与case 4一样，对于企业来说，将运营和订阅信息存储在移动运营商的网络上而不是公司的专用网络上，这让企业感到不安。

与需要在企业内部部署UPF或5GC CP的case 2、3和4相比，这种架构的成本最低。

但是，企业关注的是安全方面（从专用网络终端生成的数据流量，专用网络设备的订阅信息和操作信息）和网络延迟（专用5G设备与MEC应用程序服务器之间，以及专用5G设备与内网/局域网设备之间）。

6.N3 LBO(Local Breakout)：韩国SK Telecom的案例



如上图（a）所示，与case 5一样，gNB部署在企业中。N3 GTP隧道是在gNB和UPF之间连接设备时创建的，无论

是闭路监控摄像头还是智能手机，这些设备都是公共网络设备。

如上图（b）所示，企业引入了MEC数据平面（非3GPP设备，ETSI MEC）和MEC应用（MEC应用）。移动运营商的编排器中的移动边缘平台（MEP）通过Mp2接口将流量规则发送到MEC DP（如果目标IP地址是本地网络-专用5G设备，本地有线LAN设备，本地MEC应用程序服务器-然后Local Breakout！）。

MEC DP查看来自gNB的所有GTP隧道的数据包的目标IP地址（GTP Decap），并将用户IP包路由到内部专用网络(如果它是本地通信流)。

尽管此方法不是3GPP的标准方法，但是将私有网络流量从公共流量中分离出来是可能的。

与case 5相比，专用网络流量不会传输到移动运营商的网络，因此专用网络数据流量的安全性也与case 3和4一样明确。

与case 3和case 4不同的是，通过添加低成本的MEC DP（实际上是SDN/P4交换机），可以大大降低构建专用5G网络的成本，而无需购入昂贵的UPF设备（UPF是5G标准设备中最昂贵的设备）。

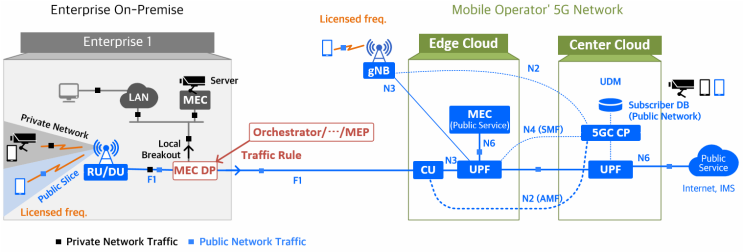
此外，由于MEC还存在于企业中，并处理MEC DP breakouts流量，因此它将能够提供超低延迟的应用程序服务。

但是，由于MEC DP不是3GPP UPF，因此MEC DP无法为专用网络设备执行移动性管理和计费功能。

（当然，由于运营商可以制定实现这些功能的专有规范，因此MEC DP可以实现其中一些功能）

与case 4和5一样，对于企业来说，将运营和订阅信息存储在移动运营商的网络上而不是公司的专用网络上也是令人不安的。

7.F1 LBO（Local Breakout）：韩国KT案例



与case 6相同，但区别在于仅部署了企业中的RU/DU，并且CU放置在移动网络的边缘云中，专用网络流量是从F1接口本地断开,而不是从N3接口。

最后，上述专用5G网络架构各有优缺点，没有一种架构能够适合所有情况。每个企业都可以根据自己的要求以及实施/运营预算来选择最适合自己的架构。

原文链接：https://www.netmanias.com/en/?m=view&id=blog&no=14500