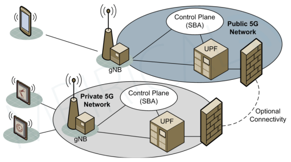
Non-Public Networks

Owned by David Cherney DISH ···
Last updated: Jul 26, 2023 • Add Workflow

Contents

What is a public network? Recall that each network operator is assigned (by the International Telecommunications Union, ITU) a public land mobile network ID. That PLMN is comprised of a mobile country code (MCC) and a mobile network code (MCC); PLMN is MCC concatenated with MNC. (e.g. DISH Wireless has MCC 313 and MNC 340, and thus DISH has PLMN 313340). To answer the question, a network operator with a PLMN is called a public mobile network operator.

The idea of a non-public network is that it has some components within or connected to a public network, and some components that are not in that public network. Here we refer to the latter set of components as "the private network".



The 3GPP term "non-public network" refers to a mobile network that

- does not have its own PLMN
- is associated with a PLMN in a way by using some of its infrastructure
- has a private network component
- is dedicated for use by a single organization

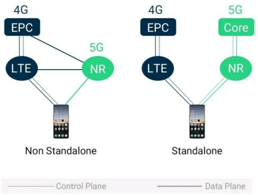
Thus, a non-public network has two parts, a private network part and a public network part.

Kinds of NPNs

3GPP makes a distinction between kinds of non-public networks. The primary distinction is standalone NPN vs non-stand alone NPN. To briefly describe the difference before going into details

- In a standalone NPN,
  - the private network contains
    - access network
    - core network user plane and control plane
  - there is a connection to a data network outside the private network
- If a NPN has any of its parts (access network, user plane, control plane) in the public network, then it is a non-stand alone NPN.

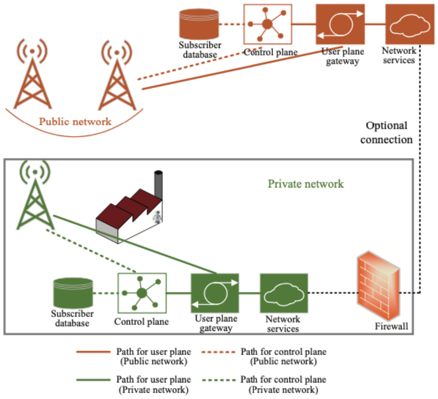
(Note: This is a different distinction than standalone 5G vs non-stand alone 5G. In a non-standalone NPN all parts are 5g as shown in the diagram above. In non-standalone 5G a 5G network is interwoven with a 4G network as shown in the diagram below.)



(Non-)Standalone 5G

Stand Alone NPN

In a standalone NPN, the private network contains all elements for RAN, control plane, and user plane. The only connection between the private network and the public network is for public network services. That is, the private network accesses data networks that are external to it.



A stand-alone non-public network is thus an almost entirely isolated mobile network. The only connection between the private network and public network is controlled by a firewall within the private network.

As an example, a factory might wish to have have an on-premises network for communication between all of the following.

- Between factory devices via a private data network
- From factory workers to devices on that same private data network
- Between factory workers
- From factory workers to the internet

The factory can then have on-premise RAN, on premises private core, an on premises private data network, and firewall protected access to the data network known as the internet.

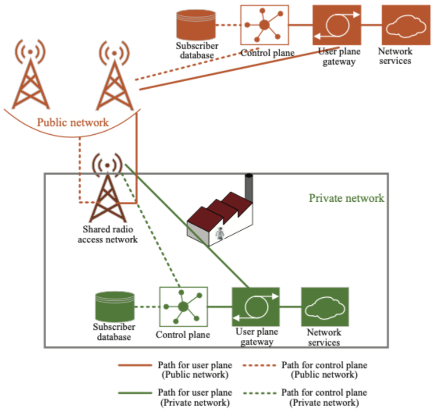
Public Network Integrated NPNs

When a public network serves the RAN, control plane, or user plane for a NPN, the NPN is called a public network integrated NPN (PNI-NPN). There are three kinds of public integrated NPN options corresponding to which of these components are served by the public network.

Shared RAN NPN

Say a company wishes use the radio equipment of a public network (like DISH). Say that further, the company wishes to use a 5G core that is isolated from the core of the public network. A shared RAN NPN is the solution. In the strongest version of this setup, all of the RAN is from the public network. However it is also possible for the private network to contain some of the radio equipment as well.

In the diagram below, the color of the shared RAN is a combination of brown and green to indicate that it is part of both the private and part of the public network; it is shared.


Subscriber database
Control plane
User plane gateway
Network services
Public network
Shared radio access network
Private network
Subscriber database
Control plane
User plane gateway
Network services
Path for user plane (Public network)
Path for control plane (Public network)
Path for user plane (Private network)
Path for control plane (Private network)

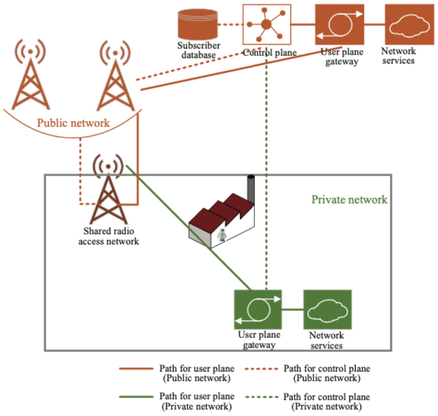
For example, a shipping logistics company might wish to use 5G mobile technology for tracking of trucks and pallets. While the trucks are on the road the existing RAN infrastructure of the public network might be sufficient. However, within the shipping yard where trucks are loaded with pallets, the public network's wireless signal might not be strong enough to reliably keep track of all the sensors on pallets. The logistics company might then place radio equipment, including one or several base stations, in the shipping yard. The company has exclusive ability to use the on premises radio equipment, and non-exclusive ability to use the RAN from the public network. No control plane or user plane information for the private network passes through the public network's core; all application servers that are accessed are servers within the private network.

3GPP specifications cover the RAN sharing situations needed for RAN sharing NPNs.

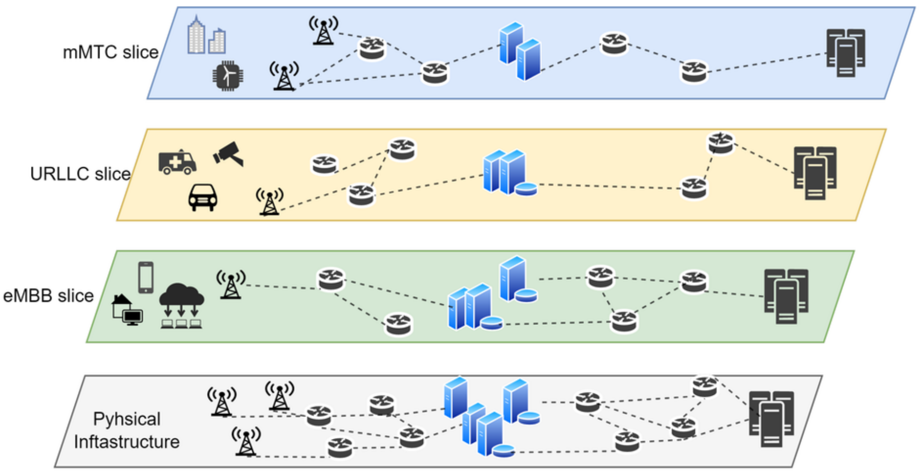
Shared RAN and Control Plane NPN

Say a company wants control plane functions of a NPN to always reside in a public network while the user plane functions remain in the private network. Then a shared RAN and control plane NPN is in order.

In the diagram below, the private network control plane traffic (dotted green) is visualized as not passing through the RAN. This is, of course, not possible, and is a indicator of a concept; the control plane messaging passes through the RAN without alteration. Note also that the user plane traffic does not leave the private network. Thus, this configuration is ideal for companies who wish to protect information passing through the user plane from inspection by the public network operator.


Subscriber database
Control plane
User plane gateway
Network services
Public network
Shared radio access network
Private network
User plane gateway
Network services
Path for user plane (Public network)
Path for control plane (Public network)
Path for user plane (Private network)
Path for control plane (Private network)

If a company wishes to use a public network, but wishes to avoid the possibility that user plane congestion might affect performance, then the company might wish for the public network operator to set up a slice with user plane resources dedicated to the company.

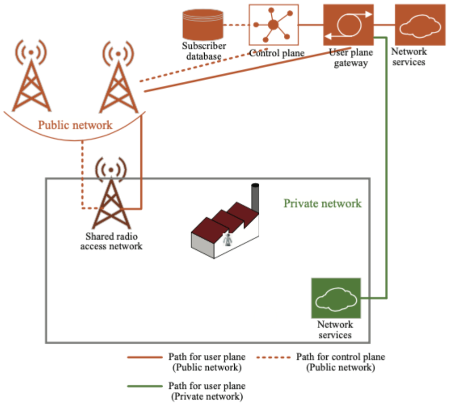


No matter whether the public network operator or the company manages the user plane infrastructure, the setup is considered a “public network integrated shared RAN and control plane NPN”.

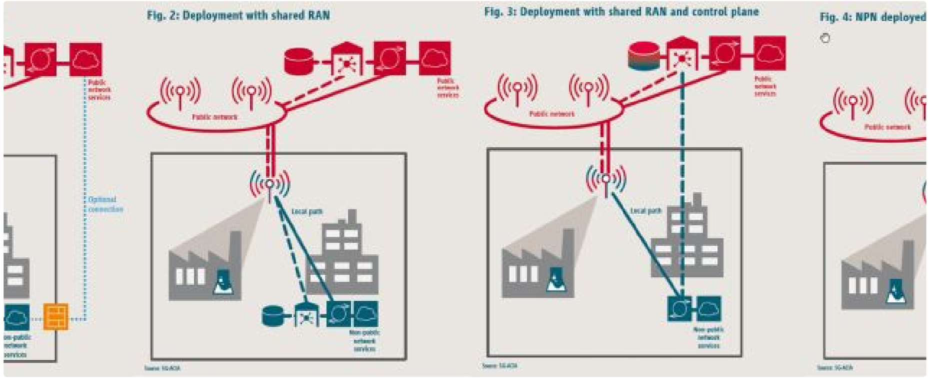
Public Network Hosted NPN

In situations where the applications accessed by UE on a NPN are to run privately, but the RAN and core are to run on a public network, a public hosted non-public network can be used.

In general, applications are available through data networks as network services. Often, the data network is the internet. However, the data network is sometimes an edge data network constructed by the public network operator. Customers may also use private data networks, and these are in essence private edge data centers. NPN customers looking for this combination of public and private data networks are covered by public network hosted NPNs.



Four options were presented above for NPN setups. The following image puts them side by side.



Why go NPN 5G?

The advantages of 5G mobile networks over other options are substantial.

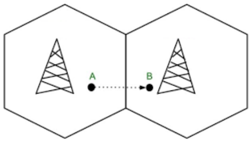
Why Wireless?

IoT applications like smart factories can (and have) been run with wires. However, deployment with wireless allows more flexibility; If equipment is to be moved from one place to another within the factory as changes are made in the factory environment, dealing with wires makes the process considerably more complicated.

Note that 5G can support wired ethernet connections, so mixed wireless-wired deployments can be served through 5G; starting with wireless provides the most flexibility.

Why Mobile?

Recall that mobility refers to the ability of connections between UE and core to be sustained throughout spatial movement of the UE via handoff from one access network node to another.



WiFi is a connection option for private networks. It usually does not support mobility by handoff between WiFi routers, but rather uses repeaters to provide service to a larger area. In cases where WiFi does support handoff between access points, the security checks can be time consuming (as they are in DISH Riverfront.) SIM cards facilitate faster handoff by facilitating fast security checks.

More generally, since the problems typically faced by WiFi deployments are simple relative to the problems faced in mobile wireless connections, the technology built out for mobile is significantly more advanced. In particular, wireless mobile has

- Latency reducing features like carrier sub-spacing
- the ability to connect a huge number of devices (3,300 on a single 5G channel with multiple channels available, whereas a WiFi router can support 250)
- the benefits of 5G antenna technology like
  - transmission power control (for energy efficiency)
  - spread spectrum to combat interference
  - multiple input multiple output advantages
    - spatial, temporal, and frequency diversity for transmission correction mechanisms
    - beam forming, which greatly reduce energy use and boosts transmission distance
- the resulting capacity for 5G mobile systems to give extremely low error rates (one packet error per billion packets for URLLC)
- Whats more, non-mobile things can be added to a mobile network, but not vice versa.

Why 5G?

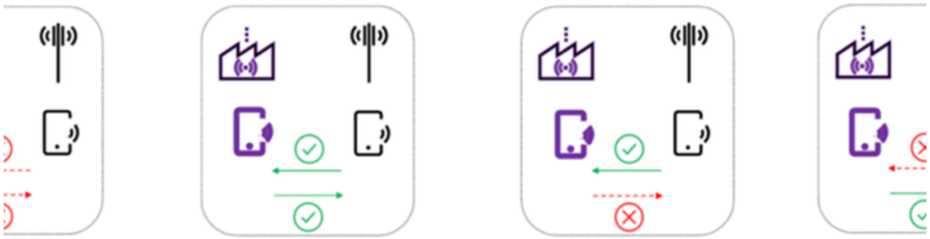
4G mobile technology has many of the capacities of 5G since it's latest stage (LTE-Advanced) was developed while the earliest stages of 5G (release 15) was developed. However, 4G was designed as an expansion of 3G mobile phone technology, whereas 5G was designed to support a wide range of use cases beyond mobile phones. For this reason, many things are much more easily done in 5G than in 4G.

- Support of user plane data sessions for unspecified data packets, for IoT applications where the devices do not transmit IP or ethernet packets
- Capacity for a much larger number of connections via variation in transmission time intervals (TTI); 4G has a TTI of 1ms with 14 symbols per TTI, whereas 5G introduces mini-slots giving TTI down to 1/8ms and the options for 2, 4, or 7 symbols. Because of this, 5G can support 3,300 connections on the same frequency range that 4G can support 300.
- much bigger spectrum ranges: 5G includes high frequencies, above 6GHz, that give 5G a much bigger bandwidth.
- optional always on: 4G was designed to reduce the time needed to establish a data session in 3G, and so has an always on (as in always connected) feature. This is wasteful, especially for IoT devices that might transmit at low data rates like a few bytes per day. 5G has been designed to support a wide range of always, sometimes, and rarely on options to allows for overall reduction in energy use, and in particular energy use for IoT devices that might need to last for years on a single AA battery.
- beam forming of synchronization signals
- Integration with time sensitive networking (TSN) for guarantee of low latency, low delay variation, and very low loss of packets
- Grant free access; in grant based access, a scheduling request must be sent before data transmission. 5G has considerable grant free technology built to reduce control plane signaling time.
- Support for high density deployments and heterogeneous network deployments; 5G has been designed to support a very diverse array of radio technologies, including high spatial density of antennas which allows for low path loss.
- Network slicing, which enables using parts of a well built out 5G network; 4G's comparable technology (dedicated cores) is much more complicated by contrast
- native support for edge computing; whereas edge computing was invented in the era of 4G, the 5G edge technology is built on lessons learned and supports breakout edge computing via UL-CL/BP UPFs, change of MEC host in support of mobility, service and session continuity modes, and intermediate UPFs while 4G has none of these things.
- localization and tracking capabilities that are far superior to 4G

P5G Roaming

Roaming is the maintenance of connection as a device moves from one administrative domain to another, including between a PLMN and an NPN.

An enterprise like a hospital might want to set up a NPN such that the users of the network can maintain connectivity when they leave (or enter) the hospital. In this process, the connection is handed over from a public network (PLMN) to the NPN, or vice versa. Then again, an enterprise like a military unit might not want to allow roaming onto a public network. There are four possibilities, depicted below.



ase 1
Roaming
n Enterprise
d MNO

Case 2
Full Roaming
between
Enterprise and MNO

Case 3
MNO allowed to
roam into
Enterprise

Case
Enterprise
To roar
MN