End-to-End Private Network Deployment Explained

Provided by: the Alliance for private netorks (MFA)

Introduction

Private networks enable entities other than traditional Mobile Network Operators (MNOs) to deploy networks for a variety of use cases, removing the need to provide services like voice, SMS, etc., to general subscribers. These networks can operate in unlicensed or licensed spectrum owned by, for example, the enterprise or factory that has access.

In 3GPP, private networks are known as Non-Public Networks (NPNs). 3GPP specifications support 5G technology-based private network deployments, which offer numerous connectivity benefits. They enable a high degree of control and customization, allowing businesses to tailor the network to meet specific needs. This flexibility is partially provided by supporting different radio frequency bands and allowing dedicated radio resources for private networks. 5G also supports enhanced security features and sophisticated Quality of Service (QoS) control for data connections, including high bit rate, high reliability, and low-latency communication; critical for applications such as real-time data analytics, automation, and Internet of Things (IoT) devices. One of the most relevant use cases for 3GPP Release 16 NPNs is industrial automation, also known as Industrial Internet of Things (IIoT).

This paper provides an overview of the 5G architecture for private networks, presents some of the most important features supported by 5G technology, and concludes with a summary of the advantages of 5G-based private networks.

3GPP Architecture Overview for Private Networks

The 5G System (5GS) architecture was initially defined by 3GPP in Release 15 to enable MNOs to provide communication between a User's Equipment (UE) and a Data Network (DN) via services like voice, SMS, data, etc. The 5GS architecture is based on concepts such as separation between user and control plane functions, definitions of procedures as services, and direct interaction between network functions enabled by the Service Based Architecture (described in detail in 3GPP TS 23.501 [1]), etc.

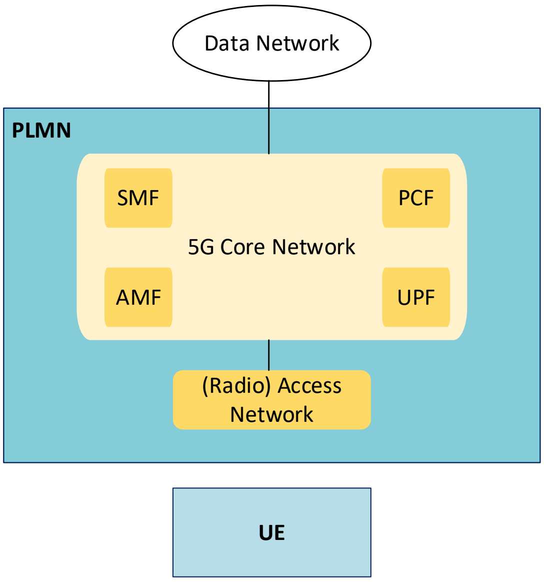

Figure 1: Simplified 5GS Architecture.

Figure 1 represents a simplified 5GS architecture which shows only the essential system structure. The 5GS can be split into UE, Radio Access Network (RAN), Core Network (CN), and DN. Some example CN Functions are also shown: 1. the Access and Mobility management Function (AMF), which manages, among other things, connection, registration, access authentication and authorization of the UE; 2. the Session Management Function (SMF), which establishes, modifies, and releases sessions between the UE and User Plane Function (UPF); 3. the Policy Control Function (PCF), which supports a unified policy framework to govern network and UE behavior and also provides related rules to other control plane functions and UE; 4. the UPF, which is the anchor point for mobility and the external point of interconnect to a DN and allocates User Plane IP addresses/prefixes.

The CN in 5G can exist entirely as software and supports a wide range of deployment models. For example, individual network functions running servers in an existing data center on premises or in the cloud can scale up or down as the number of devices on the network changes.

5G specifications also have added features to support edge-computing to the 5G CN via Multi-Access Edge Computing (MEC). Services that need low latency performance or require critical data to stay within the network operator’s direct control can now be deployed at the edge of the network.

This paper is centered on the 5G standalone deployment option as only 5G standalone deployment offers a complete end-to-end 5G solution, including the support of NPNs. Non-standalone deployment is only important when an existing 4G network is enhanced with 5G radio.

There is one aspect where the baseline 3GPP specifications are tailored to MNOs: network identification. In the baseline specifications it is assumed that networks can be identified by a Public Land Mobile Network (PLMN) Identifier (ID), which consists of a 3-digit Mobile Country Code (MCC) and a 2- or 3-digit Mobile Network Code (MNC). A PLMN ID is a globally unique identifier assigned by telecommunication authorities to service providers and has a maximum of six decimal digits which only enables the differentiation of no more than one million networks. Due to the general guidelines of assigning PLMN IDs only to public service providers, it is not realistic to assume that all private networks have access to a globally unique PLMN ID.

To address this issue 3GPP introduced the concept of Standalone Non-Public Networks (SNPN) (see details in clause 5.30.2 of 3GPP TS 23.501 [3]) for private network deployments independent from MNO deployments. An SNPN is a 3GPP 5G network deployment where the network is identified based on a PLMN ID and an additional 32-bit identifier - referred to as a Network Identifier (NID) - as depicted in “Figure 2.” It is expected that a PLMN ID and a NID together can identify an SNPN, but this can only be assured if the NID allocation is coordinated. A private network may use a locally assigned NID, but the global uniqueness would not be guaranteed even with the use of NID. It is possible to use Private Enterprise Numbers assigned by Internet Assigned Numbers Authority (IANA) as NID to guarantee the globally unique network identification independently from the PLMN ID.

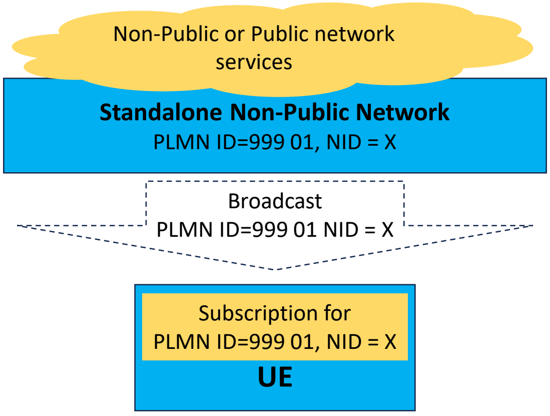

Figure 2: Example of Standalone Non-Public Network and Network Identification

The introduction of NIDs enables the use of PLMN IDs that are shared among private networks. There are several options for shared PLMN IDs:

1) ITU-T (International Telecommunication Union Telecommunication Standardization Sector) allocated MCC 999 to be used within any private network deployment. The usage of this MCC is not coordinated, meaning users can select any MCN and any NID with this country code. Therefore, there is no guarantee that two private networks will not have the same PLMN ID and NID unless a globally unique NID is used.

2) A second option would be a shared PLMN ID assigned for private networks by a local authority in the country or region of operation. In this case, the use of a PLMN ID is regulated by the local authority and limited to the given country or region.

3) The Alliance has acquired a globally unique PLMN ID which is available to any operator deploying a private network without any regional restriction through our PLMN ID Program. The advantage of employing this PLMN ID is that usage is coordinated by the Alliance (e.g., NID allocation), resolving the problems of shared PLMN ID application.

Use of an SNPN requires UE support due to the new network identifier type. Identification and authentication of UEs happens similarly to identification and authentication of a PLMN: a Subscription Permanent Identifier of the same format is used to identify the subscription; there is no change in the authentication procedure.

3GPP Features for Private Networks

Security

SNPN security is like that of PLMNs in that the UE and network must mutually authenticate and generate the security material used to protect confidentiality and integrity of the user and control plane data.

The support for SNPN authentication differs from legacy PLMNs given that - in addition to the SIM-based authentication mechanisms such as 5G AKA (Authentication and Key Agreement) and EAP-AKA (Extensible Authentication Protocol) - other non-SIM based, authentication mechanisms based on EAP can be used (e.g., EAP-TLS (Transport Layer Security). Non-SIM-based EAP mechanisms enable SNPNs to plug their existing authentication infrastructure and identity management system into the SNPN system, limiting the impact to only the UE and Authentication Server Function (AUSF). Configuration of the SNPN determines which authentication mechanism(s) can be used.

Depending upon the selected authentication mechanism, different credentials may be employed. For example, considering the EAP-TLS mechanism, the UE is configured with the necessary certificate(s) to authenticate the network and the UE (either self-signed or issued by the Certification Authority (CA)). Concurrently, the AUSF is configured with the UE public key (for self-signed UE certificate) or with the necessary certificate(s) (in a CA-issued case) to authenticate the UE. Once the UE and the network are mutually authenticated, they derive the root session key (called K_{AUSF} in 3GPP specifications) which is used in turn to derive the necessary keys to protect the traffic between the UE and the network.

Packet Data Service and QoS

The 5G data service is implemented via Packet Data Unit (PDU) sessions. A PDU session refers to a connection established between a user's device and a data network (DN) via the 5G network for data transmission. A DN is the network that provides services to the users. It can be a public network like the Internet, a private network, or a specific service network.

A PDU session carries user data, which can be IP packets, Ethernet packets, or Unstructured data. Each PDU session can have one or more associated Quality of Service (QoS) flows. Each QoS flow has a specific bit rate requirement and QoS characteristics (e.g., priority level, packet delay budget, and packet error rate) which is identified by a 5G QoS Identifier (5QI).

RAN Sharing

To enable cost-effective deployments, the 5G system supports sharing of the RAN among different operators. It is possible for a single gNodeB (gNB) to provide access for multiple private networks (e.g., to different factories sharing the same geographical location) or to some private and public networks (e.g., a public network operator may allow a private network to use its RAN infrastructure). Even though RAN sharing does not require sharing subscriber level information (subscriber credentials and data remains in the control of its home service provider), some special arrangements are needed to ensure the appropriate level of network security. The fair use of shared radio resources also requires business level agreements among the participating operators and entities.

Ethernet / TSN support and URLLC

One of the main motivations for NPNs is the industrial automation use case, which demands ultra-low latency, ultra reliability, and time sensitive communication. To support this, 3GPP developed a standard to adapt to IEEE Time Sensitive Networking (TSN) and specified two aspects: time synchronization based on generalized precision time protocol (gPTP) and time-deterministic ethernet frame forwarding (for details, see IEEE 802.AS [2] and IEEE 802.1Q [3]).

For gPTP based time synchronization, to compensate for the variable delays resulting from forwarding gPTP messages via 5GS, each gPTP frame is time-stamped when entering the 5GS. The related time information is then corrected depending upon the time the gPTP frame spent in the 5GS before being forwarded to the nodes beyond the UE. In that sense, the 5GS is “seen” by the TSN network as a set of one or more TSN bridges. A 5GS bridge has ethernet ports on a network-side TSN translator (NW-TT) (located in the UPF), ethernet ports on the device-side TSN translator (DS-TT) (co-located with the UE), and a user plane tunnel between UE and UPF. A more detailed overview on the integration of 5G and TSN for industrial communication can be found in the white paper developed by 5G-ACIA [4].

For time-deterministic ethernet frame forwarding, the 5GS bridge delay is provided by the 5GS bridge to the Centralized Network Configuration (CNC) entity of the IEEE TSN system for each DS-TT/NW-TT port pair and traffic class. The CNC entity then uses such delays to calculate the forwarding path as well as the scheduling information then forwards this information to each bridge of the TSN network.

Integration with Wi-Fi

5G-based SNPNs can also support the integration of non-3GPP access technologies such as Wi-Fi. The integration of non-3GPP access technologies enables the use of existing WLAN deployments with SNPN deployment and can provide security, service control, and mobility across the different access technologies. 3GPP has specified two types of non-3GPP interworking: trusted and untrusted.

Untrusted non-3GPP interworking refers to the scenario where the non-3GPP access network is connected to a special security gateway, called Non-3GPP InterWorking Function (N3IWF) in 3GPP specifications. In this scenario the UEs establish a secure tunnel to this gateway using their SNPN credentials to access the services of the SNPN. The secure tunnel ensures security and service control for the SNPN. The deployment of this type of interworking is simple as it does not require special functions from the non-3GPP access networks and does not interfere with services provided in the non-3GPP access network.

In Trusted non-3GPP interworking the non-3GPP access network has a direct interface to the 5GS core network. As this requires a higher level of system integration, including the support of special functions in the non-3GPP access networks, deployment of this type of interworking is more complex than untrusted non-3GPP interworking.

Neutral Host Networks

5G networks can be deployed as private networks, only providing services to subscribers authorized by the network owner. They can also be used to extend the coverage of public networks, like roaming. In this mode, subscribers to the public network can access their home network without even knowing they aren't on the public network's infrastructure. Such Neutral Host Networks (NHNs) require coordination with the public network operators to agree on access terms and are a great way to address poor indoor coverage. A network can even be deployed as hybrid – providing NHN service while at the same time creating a private network that only authorized subscribers are able to access.

Summary

In this paper, we presented an overview of 5G architecture and some key features of 5G that make it very attractive for private networks. We focused on the standalone private network deployment option, which is called SNPN in 3GPP specifications.

5G technology, originally developed for public network deployments, is also a viable option for private networks due to its flexibility and ability to support a variety of features. An important characteristic of 5G is that most of its features are optional and allow for easy network deployment that addresses specific use-cases and services. A basic deployment can only provide the best effort services, while an advanced deployment version offers high reliability and low latency communications. Moreover, the support of multiple services can happen concurrently within a single deployment as it is possible to allocate resources within a network for specific services or service classes.

References

[1] 3GPP TS 23.501: “System Architecture for the 5G System; Stage 2”

[2] IEEE Std 802.1AS-2020: “IEEE Standard for Local and metropolitan area networks—Timing and Synchronization for Time-Sensitive Applications

[3] IEEE Std 802.1Q-2022: “IEEE Standard for Local and metropolitan area networks—Bridges and Bridged Networks”.

[4] 5G-ACIA, Integration of 5G with Time-Sensitive Networking for Industrial Communications, https://5g-acia.org/whitepapers/integration-of-5g-with-time-sensitive-networking-for-industrial-communications/.

Abbreviation and acronym definitions:

3GPP: 3rd Generation Partnership Project

5G-ACIA: 5G Alliance for Connected Industries and Automation

5G AKA: 5G Authentication and Key Agreement

5GS: 5G System

5QI: 5G QoS Identifier

AMF: Access and Mobility management Function

AUSF: Authentication Server Function

CA: Certification Authority

CNC: Centralized Network Configuration

CN: Core Network

DS-TT: device-side TSN translator

DN: Data Network

EAP: Extensible Authentication Protocol

gNB: gNodeB

gPTP: generalized Precision Time Protocol

IANA: Internet Assigned Numbers Authority

ID: Identifier

IIOT: Industrial Internet of Things

IOT: Internet of Things

IP: Internet Protocol

ITU-T: International Telecommunication Union Telecommunication Standardization Sector

MEC: Multi-Access Edge Computing

MNC: Mobile Network Code

MNOs: Mobile Network Operators

MCC: Mobile Country Code

N3IWF: Non-3GPP Interworking Function

Neutral Host Networks (NHNs)

NID: Network Identifier

NPNs: Non-Public Networks

NW-TT: network-side TSN translator

PCF: Policy Control Function

PDU: Packet Data Unit

PLMN: Public Land Mobile Network

QoS: Quality of Service

Rel-15: 3GPP Specifications Release 15

Rel-16: 3GPP Specifications Release 16

RAN: Radio Access Network

SMF: Session Management Function

SMS: Short Message Service

TLS: Transport Layer Security

TSN: Time Sensitive Networking

UE: User Equipment

UPF: User Plane Function

UP: User Plane

SIM: Subscriber Identity Module

SNPN: Standalone Non-Public Networks

SPI: Subscription Permanent Identifier

WLAN: Wireless Local Area Network

About the Alliance for private networks: We are an industry alliance supporting private network adoption. The Alliance provides resources that simplify the path to optimized, reliable and secure private networks in locally licensed, shared, or unlicensed spectrum. We enable the ecosystem with our Uni5G™ technology blueprints and unique global PLMN-ID program. Uni5G, based on 3GPP specifications, identifies the key 5G features needed for enterprises to successfully deploy their own private network. The Alliance is a 3GPP Market Representation Partner. Learn more at www.mfa-tech.org.