CHAPTER 1

5G Network Architecture

5G network architecture has been designed to support fast and reliable connectivity as well as diverse applications and services, enabling flexible deployments using new concepts, such as network function virtualization (NFV), software-defined networking (SDN), and network slicing. The 5G system supports a service-oriented architecture with modularized network services. The service-oriented 5G core (5GC) network is built on the principle that 5G systems must support wide range of services with different characteristics and performance requirements. The service-oriented architecture and interfaces in the 5G systems make the future networks flexible, customizable, and scalable. Network service providers can leverage service-oriented architecture design in 5G to manage and adapt the network capabilities, for example, by dynamically discovering, adding, and updating network services while preserving the performance and backward compatibility.

The main difference in the service-based architecture is in the control plane where, instead of predefined interfaces between entities, a service model is used in which components request a new network entity to discover and communicate with other entities over application programming interfaces (APIs). This notion is closer to the cloud networking concept and more attractive to the operators that demand flexibility and adaptability in their networks. The challenge is that it is harder to implement using today's cloud platforms and it is likely to be part of future deployments. It is also important for the 5G network to enable each network function (NF) to directly interact with other network functions. The architecture design does not preclude the use of an intermediate function to help route control-plane messages. It is also desirable to minimize dependencies between the access network (AN) and the core network.

There are some new concepts that have fundamentally changed the framework of 5G networks and made them differentiated from the previous generations. 5G network architecture leverages structural separation of hardware and software, as well as the programmability offered by software-defined network (SDN) and network function virtualization (NFV). As such, 5G network architecture is a native SDN/NFV architecture covering mobile/fixed terminals, infrastructure, NFs, enabling new capabilities and management and orchestration (MANO) functions. One of the most innovative concepts that has been incorporated into the design of the next-generation networks is the separation of user-plane and control-plane

5G NR. DOI: https://doi.org/10.1016/B978-0-08-102267-2.00001-4

functions, which allows individually scalable and flexible centralized or distributed network deployments. This concept forms the basis of the SDN. Other schemes include modularized functional design, which enables flexible and efficient network slicing. Having such requirements in mind, third-generation partnership project (3GPP) has developed a flat architecture where the control-plane functions are separated from the user plane in order to allow them to scale independently. Another central idea in the design of 5G networks has been to minimize dependencies between the AN and the core network with a unified access-agnostic core network and a common AN/core network interface which integrates different 3GPP and non-3GPP access types.

In order to further support multi-radio access, the network architecture was required to provision a unified authentication framework. The support of stateless NFs, where the compute resource elements are decoupled from the storage resource elements, is intended to create a disaggregated architecture. To support low-latency services and access to local data networks, the user-plane functions (UPFs) can be deployed close to the edge of the AN which further requires support of capability exposure and concurrent access to local and centralized services.

The combination of SDN and functional virtualization enables dynamic, flexible deployment, and on-demand scaling of NFs, which are necessary for the development of 5G mobile packet core networks. 5G network design requires a common core network associated with one or more ANs to be part of a network slice (e.g., fixed and mobile access within the same network slice). A network slice may include control-plane functions associated with one or more UPFs, and/or service or service-category-specific control-plane and user-plane functional pairs (e.g., user-specific multimedia application session). A device may connect to more than one slice. When a device accesses multiple network slices simultaneously, a control-plane function or a set of control-plane functions should be in common and shared among multiple network slices, and their associated resources. In order to enable different data services and requirements, the elements of the 5GC, also called NFs, have been further simplified with most of them being software-based so that they can be adapted and scaled on a need basis.

Today's static measurements of network and application performance are neither extensible to the dynamic nature of SDN/NFV-based 5G networks and functionalities, nor capable of creating any form of automation to create self-adapting behavior. The pace at which these environments change requires sophisticated analysis of real-time measurements, telemetry data, flow-based information, etc., in combination with user profile and behavior statistics. Creating a dynamic model to analyze the resulting big data requires artificial intelligence/machine learning techniques that will pave the way for migration

from today's process-based analytics toward predictive, descriptive, and ultimately cognitive analytics required for self-organizing, self-optimizing, and self-healing networks.

3GPP has been working on the standardization of 5G access and core networks since 2015 with a goal of large-scale commercialization in 2020 + . 3GPP system architecture group finalized the first study items in December 2016 and published the 3GPP TR 23.799 specification as an outcome of the study. The normative specifications of the 5G network architecture and services have been published in numerous 3GPP standards documents [6].

In this chapter we discuss 5G network architecture design principles from 3GPP perspective and the innovative solutions that have formed the foundation of the 5G networks. We will further study the access/core network entities, interfaces, and protocols as well as the quality of service (QoS), security, mobility, and power management in 5G networks.

1.1 Design Principles and Prominent Network Topologies

The 5G system supports a service-based architecture and interfaces with modularized network services, enabling flexible, customizable, and independently deployable networks. Network service providers can leverage 5G service-oriented architecture to manage and customize the network capabilities by dynamically discovering, adding, and updating network services while preserving performance and compatibility with the existing deployments. 5GC and ANs were required to be functionally decoupled to create a radio technology agnostic architecture in order to realize the 5G performance targets for different usage scenarios. As an example, reduction in network transport latency requires placement of computing and storage resources at the edge of the network to enhance service quality and user experience. The tactile Internet is a forward-looking usage scenario under the category of ultra-reliable low-latency communication (URLLC) services. A notable requirement for enabling the tactile Internet is to place the content and context-bearing virtualized infrastructure at the edge of the AN [mobile edge computing (MEC)]. This relocation provides a path for new business opportunities and collaborative models across various service platforms. Improved access to the content, context, and mobility are vital elements to address the demands for reliability, availability, and low latency [62].

While much has been written and speculated about the next-generation radio standards that are going to form the basis of the forthcoming 5G systems, the core network is also an essential piece in achieving the goals set forth for these systems and in helping to ensure the competitiveness and relevance of network operations in the future. With the advent of heterogeneous ANs, that is, deployment of different radio access technologies with different

coverage footprints, seamless connectivity, and service continuity can be provided in various mobility classes. The availability of different types of footprints for a given type of wireless access technology characterizes heterogeneous access, for example, a radio network access node such as a base station with large to small coverage area is referred to as macro-, pico-, and femtocell, respectively. A combination of these types of base stations offers the potential to optimize both coverage and capacity by appropriately distributing smaller-size base stations within a larger macro-base station coverage area. Since the radio access technology is common across these different types of base stations, common methods for configuration and operation can be utilized, thereby enhancing integration and operational efficiencies. The diversity of coverage, harnessing of spectrum (e.g., licensed and unlicensed spectrum), and different transmission power levels based on coverage area provide strategies for optimizing the allocation and efficient utilization of radio resources.

The expanding diversity of deployment options while considering the ultra-low latency, high reliability, availability, and mobility requirements demands a significant reduction in the overhead and complexity associated with the frequent setup and teardown of the access/core network bearers and tunneling protocols. However, the changes in the geographical location of point of attachment of a device to the AN, as a result of mobility, would inevitably add more overhead with tunneling, in a functionally virtualized network, which could adversely affect the delay-sensitive service experience. The 5G networks support multiple radio access mechanisms including fixed and mobile access, making fixed/mobile convergence an important consideration. 5G systems further support the use of non-3GPP access for off-loading and maintaining service continuity.

The logical/physical decomposition of radio NFs is required to meet the diverse information transport demands and to align them with the requirements of next-generation services in various use cases. The decomposition of the radio network protocols/functions across layer-1, layer-2, and layer-3 would depend on the degree of centralization or distribution required. It includes placing more functions corresponding to the upper layers of the radio network protocol stack in the distributed entities when high-performance transport (e.g., high bandwidth, high capacity, low latency, low jitter, etc.) is available. Optimized scheduling at a centralized entity is critical for high-performance transport across multiple distributed entities (e.g., base stations, remote radio heads (RRHs),[1] etc.). For relatively low-performance transport options, more functions corresponding to the upper layer of the radio network protocol stack is moved to the central entity to optimize the cost/performance metrics, associated with the distributed entities. The choice of functional split will determine the fronthaul/backhaul capacity requirements and associated latency specifications and

[1] The terms “remote radio head” abbreviated as RRH and “remote radio unit” abbreviated as RRU have the same meaning and will be used interchangeably in this book.

performance. This will impact the network architecture planning, since it determines the placement of nodes and permissible distance between them.

The core network in the 5G systems allows a user to access network services, independent of the type of access technology. The network service provider utilizes a common framework for authentication and billing via a unified customer database to authorize the access to a service independent of the type of access. The 5G system provides termination points or points of attachment to the core network for control-plane and user-plane entities. These points are selected based on location, mobility, and service requirements. They may dynamically change during the lifetime of a service flow, based on the aforementioned requirements. To achieve a unified core network, common mechanisms of attachment are supported for both 3GPP and non-3GPP ANs. The 5G system will allow simultaneous multiple points of attachment to be selected per device on a per-service flow basis. Control-plane functions and UPFs are clearly separated with appropriate open interfaces.

Device types are characterized by a variety of attributes including three broad categories of interfaces, namely human−human (H−H), human−machine (H−M), and machine−machine (M−M). Examples of devices that belong to these categories include smartphones (H−H), robots (H−M) or (M−M), drones (H−M) or (M−M), wearable devices (H−M), smart objects and sensors (M−M), etc. The attributes and capabilities associated with these devices are varying such as high power/low power, energy constraint/non-energy constraint, high cost/low cost, high performance/low performance, delay sensitive/delay tolerant, high reliability, and precision sensitive. These devices are distinguished in terms of diverse media types, such as audio, visual, haptic, vestibular, etc. The devices may be connected to a network either via a wired connection (e.g., Ethernet or optical transport) or a wireless connection (e.g., cellular, Wi-Fi, or Bluetooth). The cloud radio access model includes both composite and heterogeneous types of access, where moving the computational complexity and storage from the device to the edge of the network would enable diverse services using a variety of device types (e.g., H−H, H−M, and M−M) and would enable energy conservation in the devices with limited computing/storage resources.

Flexibility applies not only to network hardware and software but also to network management. An example would be the automation of network instance setup in the context of network slicing that relies on optimization of different NFs to deliver a specific service satisfying certain service requirements. Flexible management will enable future networks to support new types of service offerings that previously would have made no technical or economic sense. Many aspects of the 5G network architecture need to be flexible to allow services to scale. It is likely that networks will need to be deployed using different hardware technologies with different feature sets implemented at different physical locations in the

network depending on the use case. In some use cases, the majority of user-plane traffic may require only very simple processing, which can be run on low-cost hardware, whereas other traffic may require more advanced/complex processing. Cost-efficient scaling of the user plane to handle the increasing individual and aggregated bandwidths is a key component of a 5GC network.

As we mentioned earlier, supporting the separation of the control-plane and user-plane functions is one of the most significant principles of the 5GC network architecture. The separation allows control- and user-plane resources to scale independently and supports migration to cloud-based deployments. By separating user- and control-plane resources, the user-plane/control-plane entities may also be implemented/instantiated in different logical/physical locations. For example, the control plane can be implemented in a central site, which makes management and operation less complex and the user plane can be distributed over a number of local sites, moving it closer to the user. This is beneficial, as it shortens the round-trip time between the user and the network service, and reduces the amount of bandwidth required between sites. Content caching is an example of how locating functions on a local site reduces the required bandwidth between sites. Separation of the control and user planes is a fundamental concept of SDN, as the flexibility of 5GC networks will improve significantly by adopting SDN principles. User-plane protocols, which can be seen as a chain of functions, can be deployed to suit a specific use case. Given that the connectivity needs of each use case varies, the most cost-efficient deployment can be uniquely created for each scenario. For example, the connectivity needs for a massive machine type communication (mMTC) service characterized by small payload and low mobility are quite different from the needs of an enhanced mobile broadband (eMBB) service with large payload and high mobility characteristics. An eMBB service can be broken down into several subservices, such as video streaming and web browsing, which can in turn be implemented by separate functional chains within the network slice. Such additional decomposition within the user-plane domain further increases the flexibility of the core network. The separation of the control and user planes enables the use of different processing platforms for each one. Similarly, different user planes can be deployed with different run-time platforms within a user plane, all depending on the cost efficiency of the solution. In the eMBB use case, one functional chain of services may run on general-purpose processors, whereas the service that requires simple user-data processing can be processed on low-cost hardware platforms. It is obvious that enabling future expansions requires greater flexibility in the way that the networks are built. While network slicing is a key enabler to achieving greater flexibility, increasing flexibility may lead to greater complexity at all levels of the system, which in turn tends to increase the cost of operation and delay the deployments.

Traditional radio access network (RAN) architectures consist of several stand-alone base stations, each covering relatively a small area. Each base station processes and transmits/receives its own signal to/from the mobile terminals in its coverage area and forwards the user data payloads from the mobile terminal to the core network via a dedicated backhaul link. Owing to the limited spectral resources, network operators reuse the frequency among different base stations, which can cause interference among neighboring cells.

There are several limitations in the traditional cellular architecture, including the cost and the operation and maintenance of the individual base stations; increased inter-cell interference level due to proximity of the other base stations used to increase network capacity; and variation of the amount of loading and user traffic across different base stations. As a result, the average utilization rate of individual base stations is very low since the radio resources cannot be shared among different base stations. Therefore, all base stations are designed to handle the maximum traffic and not the average traffic, resulting in overprovisioning of radio resources and increasing power consumption at idle times.

In earlier generations of cellular networks, the macro-base stations used an all-in-one architecture, that is, analog circuitry and digital processing hardware were physically co-located. The radio frequency (RF) signal generated by the base station transported over the RF cables up to the antennas on top of a tower or other mounting points. In more recent generations, a distributed base station architecture was introduced where the radio unit, also known as the RRH was separated from the digital unit, or baseband unit (BBU) through a fronthaul transport mechanism such as optical fiber. Complex-valued I/Q samples were carried over fiber using Common Public Radio Interface (CPRI)[2] between the RRH and the BBU. The RRH was installed on top of a tower close to the antenna, reducing the cable loss compared to the traditional base stations where the RF signal has to travel through a long cable from the base station cabinet to the antenna. The fiber link between RRH and BBU also allows more flexibility in network planning and deployment as they can be placed a few hundred meters or a few kilometers away. Most modern base stations now use this decoupled architecture [47].

The cloud-RAN (C-RAN) may be viewed as an architectural evolution of the distributed base station system (Fig. 1.1). It takes advantage of many technological advances in wireless and optical communication systems. For example, it uses the latest CPRI specifications,

[2] Common Public Radio Interface, http://www.cpri.info/.

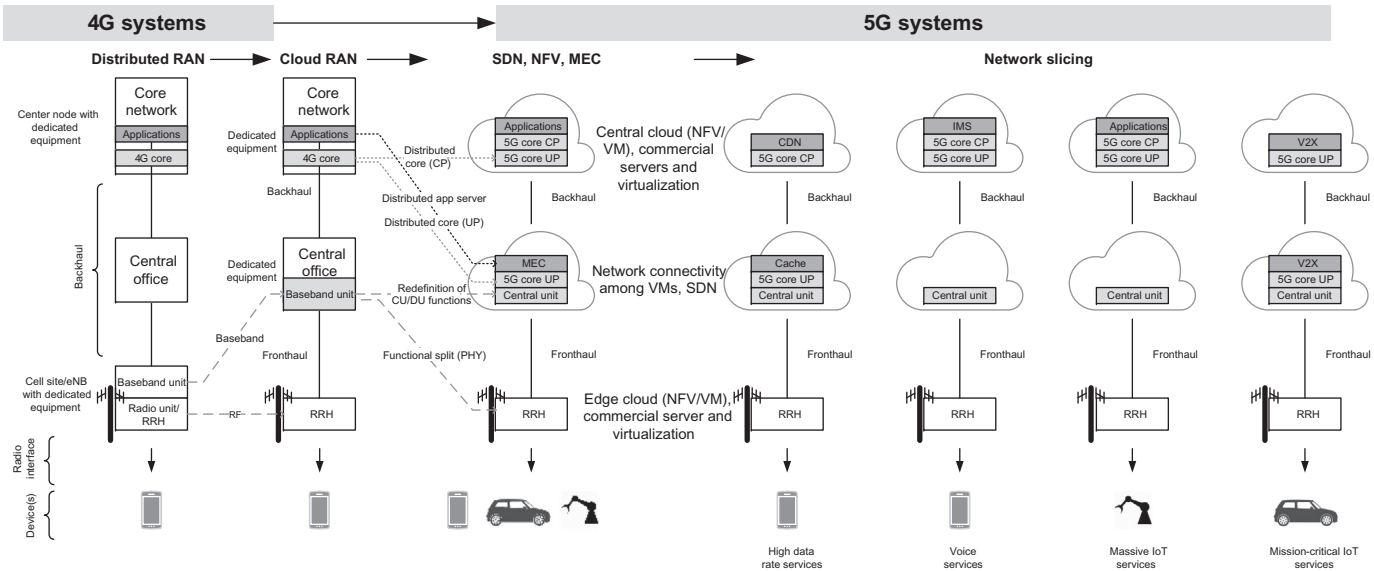
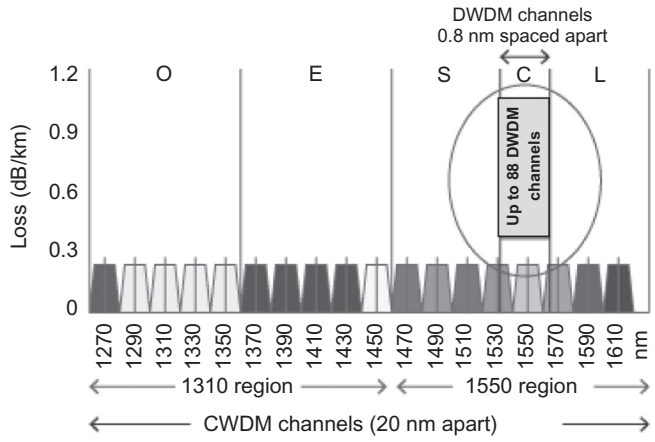


Figure 1.1
Network architecture evolution from 4G to 5G [60].

low-cost coarse/dense wavelength division multiplexing (CWDM/DWDM)[3] technology, and mmWave to allow transmission of baseband signals over long distance, thus achieving large-scale centralized base station deployment. It applies recent data center network technology to allow a low cost, high reliability, low latency, and high bandwidth interconnect network in the BBU pool. In the run up to 5G networks, the C-RAN utilizes open platforms and real-time virtualization technology rooted in cloud computing to achieve dynamic shared resource allocation and support of multi-vendor, multi-technology environments. Fig. 1.1 illustrates the evolution stages of 4G to 5G networks, where the distributed architectures evolved to centralized architectures, NFs have been virtualized, and later the

[3] Wavelength division multiplexing allows different data streams to be sent simultaneously over a single optical fiber network. There are two main types of wavelength division multiplexing technologies in use: Coarse wavelength division multiplexing and dense wavelength division multiplexing. Coarse wavelength division multiplexing allows up to 18 channels to be transported over a single dark fiber, while dense wavelength division multiplexing supports up to 88 channels. Both technologies are independent of transport protocol. The main difference between coarse wavelength division multiplexing and dense wavelength division multiplexing technologies lies in how the transmission channels are spaced along the electromagnetic spectrum. Wavelength division multiplexing technology uses infrared light, which lies beyond the spectrum of visible light. It can use wavelengths between 1260 and 1670 nm. Most fibers are optimized for the two regions 1310 and 1550 nm, which allow effective channels for optical networking. Coarse wavelength division multiplexing is a convenient and low-cost solution for distances up to 70 km. But between 40 and its maximum distance of 70 km, coarse wavelength division multiplexing tends to be limited to eight channels due to a phenomenon called the water peak of the fiber. Coarse wavelength division multiplexing signals cannot be amplified, making the 70 km estimate an absolute maximum. Dense wavelength division multiplexing works on the same principle as coarse wavelength division multiplexing, but in addition to the increased channel capacity, it can also be amplified to support much longer distances. The following figure shows how the dense wavelength division multiplexing channels fit into the wavelength spectrum compared to coarse wavelength division multiplexing channels. Each coarse wavelength division multiplexing channel is spaced 20 nm apart from the adjacent channel (www.Smartoptics.com).



control-plane and user-plane functions were separated, and ultimately network slicing and edge computing have been introduced to further advance the network architectures toward flexibly supporting various 5G use cases and applications.

Having the above principles and requirements in mind, 3GPP 5G system (5GS) architecture has been designed to support data connectivity and new services by enabling deployments to use SDN/NFV methods. The 5GS architecture leverages service-based interactions between control-plane NFs and supports separation of user-plane functions from control-plane functions. The modularized functional design would allow flexible and efficient network slicing. It defines procedures, that is, set of interactions between NFs, as services so that their reuse is possible. It enables each NF to directly interact with other NFs. The 5GS design minimizes dependencies between the access and the core networks. It further supports a unified authentication framework, stateless NFs, where compute resources are decoupled from storage resources, and capability exposure, as well as concurrent access to local and centralized services. The 5GS supports roaming with both home-routed traffic as well as local breakout traffic in the visited network. In 5GS, the interactions between NFs are represented either through a service-based representation, where NFs within the control plane enable other authorized NFs to access their services which may include point-to-point reference points; or a reference-point representation, where the interactions between the NFs are described by point-to-point reference points between any two NFs. The NFs within the 5GC network control plane use service-based interfaces for their interactions [3].

The general principles that guided the definition of 3GPP 5G radio access network (NG-RAN) and 3GPP 5GC network architecture and network interfaces are based on logical separation of signaling and data transport networks, as well as separation of NG-RAN and 5GC functions from the transport functions. As a result, the addressing schemes used in NG-RAN and 5GC are decoupled from the addressing schemes of the transport functions. The protocols over the air interface and the NG interfaces are divided into user-plane protocols, which are the protocols implementing the actual protocol data unit (PDU) session service, carrying user data through the access stratum (AS); and control-plane protocols, which are the protocols for controlling the PDU sessions and the connection between the user equipment (UE) and the network from different aspects, including requesting the service, controlling different transmission resources, handover, etc. [15].

1.1.1 Network and Service Requirements

The service-centric 5G network architecture has been designed to flexibly and efficiently meet diverse requirements of the emerging applications/services. With SDN and NFV supporting the underlying physical infrastructure, 5G network systematically centralizes access, transport, and core network components. Migration to cloud-based architectures is meant to support wide-ranging 5G services and enables key technologies, such as network slicing, on-demand deployment of service anchors, and component-based NFs.

The design principles of 3GPP next-generation system architecture have deviated from those of the long-term evolution (LTE) evolved packet core (EPC) network in order to address the challenging requirements of 5G applications/services. While the design of 5G network started from a clean slate, the requirements for support of the new radio access technologies (RATs) as well as the evolved LTE, legacy systems, and non-3GPP radio access have caused the new design to borrow a large amount of concepts from the predecessor networks. Some of the key tenets of 5G network design include the requirement for logically independent network slicing based on a single network (physical) infrastructure to meet the 5G service requirements; and to provide dual-connectivity-based cloud architecture to support various deployment scenarios. The network design further relies on C-RAN architecture to deploy different radio access technologies in order to provide multi-standard connectivity and to implement on-demand deployment of RAN functions required by 5G services. It simplifies core network architecture to implement on-demand configuration of NFs through control and user-plane separation, component-based functions, and unified database management. It further implements automatic network slicing service generation, maintenance, and termination for various services to reduce operating expenses through agile network operation and management.

3GPP TS 22.261 specification, service requirements for the 5G system, contains performance targets and basic capabilities prescribed for the 5G networks. Among those requirements, one can distinguish support for fixed, mobile, wireless, and satellite access technologies; scalable and customizable network that can be tailored to serve multiple services and vertical markets (e.g., network slicing, NFV); resource efficiency for services ranging from low-rate Internet of things (IoT) services to high-bandwidth multimedia services; energy efficiency and network power optimization; network capability exposure to allow third party Internet service providers and Internet content providers to manage network slices, and deploy applications in the operator's service hosting environment; indirect connectivity from a remote UE via a relay UE to the network; and service continuity between indirect connections and direct connections. 3GPP TS22.261 defines performance targets for different scenarios (e.g., urban macro, rural macro, and indoor hotspot) and applications (e.g., remote control, monitoring, intelligent transport systems, and tactile communications).

The general requirements that led the design of NG-RAN architecture and interfaces included logical separation of signaling and data transport networks and separation of access and core NFs from transport functions, regardless of their possible physical co-location. Other considerations included independence of addressing scheme used in NG-RAN and 5GC from those of transport functions and control of mobility for radio resource control (RRC) connection via NG-RAN. The functional division across the NG-RAN interfaces has limited options and the interfaces are based on a logical model of the entity controlled through the corresponding interface. As was the case with LTE, one physical network element can implement multiple logical nodes.

1.1.2 Virtualization of Network Functions

NFV is an alternative approach to design, deploy, and manage networking services as well as a complement to SDN for network management. While they both manage networks, they rely on different methods. SDN separates the control and forwarding planes to offer a centralized view of the network, whereas NFV primarily focuses on optimizing the network services themselves.

NFV transforms the way that network operators architect networks by evolving standard server-based virtualization technology to consolidate various network equipment types into industrial-grade high-volume servers, switches,[4] and storage, which could be located in data centers, network nodes, and in the end-user premises. The NFV involves implementation of NFs in software that can run on a range of network server hardware that can be moved to or instantiated in various locations in the network as required, without the need for installation of new equipment. The NFV is complementary to SDN, but not dependent on it or vice versa. It can be implemented without an SDN being required, although the two concepts/solutions can be combined to gain potentially greater value. NFV goals can be achieved using non-SDN mechanisms, relying on the techniques currently in use in many data centers. But approaches relying on the separation of the control and data forwarding planes as proposed by SDN can enhance performance, simplify compatibility with the existing deployments, and facilitate operation and maintenance procedures. The NFV is able to support SDN by providing the infrastructure upon which the SDN software can be run. Furthermore, NFV aligns closely with the SDN objectives to use commodity servers and switches. The latter is applicable to any user-plane or control-plane functional processing in mobile and fixed networks. Some example application areas include switching elements, mobile core network nodes, functions contained in home routers and set top boxes, tunneling gateway elements, traffic analysis, test and diagnostics, Internet protocol (IP) multimedia subsystem, authentication, authorization, and accounting (AAA) servers,[5] policy control and charging platforms, and security functions [48].

[4] Switch is a device that typically transports traffic between segments of a single local area network. Internal firmware instructs the switch where to forward each packet it receives. Typically, a switch uses the same path for every packet. In a software-defined networking environment, the switches' firmware that dictates the path of packets would be removed from the device and moved to the controller, which would orchestrate the path based on a macro-view of real-time traffic patterns and requirements.

[5] Authentication, authorization, and accounting is a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. An authentication, authorization, and accounting server is a server program that handles user requests for access to computer resources and, for an enterprise, provides authentication, authorization, and accounting services. The authentication, authorization, and accounting server typically interacts with network access and gateway servers and with databases and directories containing user information.

NFV leverages modern technologies such as those developed for cloud computing. At the core of these cloud technologies are virtualization mechanisms. Hardware virtualization is realized by means of hypervisors[6] as well as the usage of virtual Ethernet switches (e.g., vSwitch[7]) for connecting traffic between virtual machines (VMs) and physical interfaces. For communication-oriented functions, high-performance packet processing is made possible through high-speed multi-core CPUs with high I/O bandwidth, smart network interface cards for load sharing and transmission control protocol (TCP) offloading, routing packets directly to VM memory, and poll-mode Ethernet drivers (rather than interrupt driven; e.g., Data Plane Development Kit[8]). Cloud infrastructures provide methods to enhance resource availability and usage by means of orchestration and management mechanisms, which is applicable to the automatic instantiation of virtual appliances in the network, management of resources by properly assigning virtual appliances to the CPU cores, memory and interfaces, reinitialization of failed VMs,[9] snapshot of VM states, and the migration of VMs. As shown in Fig. 1.2, containers and VMs are two ways to deploy multiple, isolated services on a single platform [42–44].

The decision whether to use containers or VMs depends on the objective. Virtualization enables workloads to run in environments that are separated from their underlying hardware by a layer of abstraction. This abstraction allows servers to be divided into virtualized machines that can run different operating systems. Container technology offers an alternative method for virtualization, in which a single operating system on a host can run many

[6] A hypervisor is a function which abstracts or isolates the operating systems and applications from the underlying computer hardware. This abstraction allows the underlying host machine hardware to independently operate one or more virtual machines as guests, allowing multiple guest virtual machines to effectively share the system's physical compute resources, such as processor cycles, memory space, and network bandwidth.

[7] A virtual switch is a software program that allows one virtual machine to communicate with another. Similar to its counterpart, the physical Ethernet switch, a virtual switch does more than just forwarding data packets. It can intelligently direct communication on the network by inspecting packets before forwarding them. Some vendors embed virtual switches into their virtualization software, but a virtual switch can also be included in a server's hardware as part of its firmware. Open vSwitch is an open-source implementation of a distributed virtual multilayer switch. The main purpose of Open vSwitch is to provide a switching stack for hardware virtualization environments, while supporting multiple protocols and standards used in computer networks.

[8] Data plane development kit is a set of data-plane libraries and network interface controller drivers for fast packet processing from Intel Corporation. The data plane development kit provides a programming framework for x86-based servers and enables faster development of high-speed data packet networking applications. The data plane development kit framework creates a set of libraries for specific hardware/software environments through the creation of an environment abstraction layer. The environment abstraction layer conceals the environmental-specific parameters and provides a standard programming interface to libraries, available hardware accelerators, and other hardware and operating system (Linux, FreeBSD) elements.

[9] A virtual machine is an operating system or application environment that is installed on software, which imitates dedicated hardware. The end user has the same experience on a virtual machine as they would have on dedicated hardware.

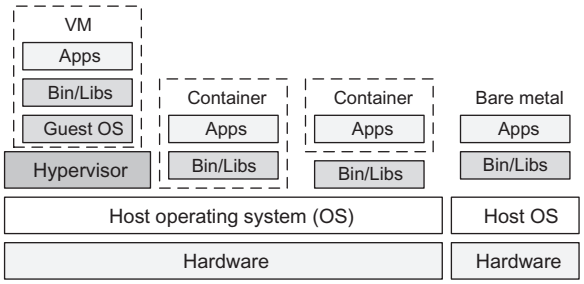


Figure 1.2
NFV software/hardware architecture models.

different applications from the cloud. One way to think of containers versus VMs is that VMs run several different operating systems on one compute node, whereas container technology offers the opportunity to virtualize the operating system itself. A VM is a software-based environment geared to simulate a hardware-based environment, for the benefit of the applications it will host. Conventional applications are designed to be managed by an operating system and executed by a set of processor cores. Such applications can run within a VM without any rearchitecture. On the contrary, container technology has been around for more than a decade and is an approach to software development in which pieces of code are packaged in a standardized way so that they can quickly be plugged in and run on the Linux operating system. This enables portability of code and allows the operating system to be virtualized and share an instance of an operating system in a same way that a VM would divide a server. Therefore instead of virtualizing the hardware like a VM, a container virtualizes at the operating system level. Containers run at a layer on top of the host operating system and they share the kernel. Containers have much lower overhead relative to the VMs and much smaller footprint.

NFV decouples software implementations of NFs from the compute, storage, and networking resources they use. It thereby expands options for both enterprises and service providers, enabling both to create new capabilities and new services for their customers. With new opportunities come new challenges. By tradition, NF implementations are packaged with the infrastructure they utilize; however, this may not be the case anymore. As the physical network is decoupled from the infrastructure and network services, it is necessary to create both new management tools and orchestration solutions for providers to realize the benefits of NFV-based solutions. There are a number of challenges to implement NFV, which need to be addressed by the industry. Some of the main challenges include the following [43]:

- *Portability/interoperability:* This is the ability to load and execute virtual appliances in different but standardized data center environments, which can be provided by different vendors for different operators. The challenge is to define a unified interface which clearly decouples the software instances from the underlying hardware, as represented

by VMs and their hypervisors. Portability and interoperability are very important as they create different ecosystems for virtual appliance vendors and data center vendors, while both ecosystems are clearly coupled and depend on each other. Portability also provides the operator with the freedom to optimize the location and required resources of the virtual appliances without constraints.

- *Performance trade-off:* Since the NFV approach is based on conventional hardware as opposed to customized hardware, there could be a possible decrease in performance. The challenge is how to limit the performance degradation by using appropriate hypervisors, hardware accelerators, and advanced software technologies such that the effects on latency, throughput, and processing overhead are minimized.
- *Migration, coexistence, and compatibility with the existing platforms:* Implementations of NFV must coexist with network operators' legacy network equipment, and further it must be compatible with their existing element management systems (EMSs),[10] network management systems (NMSs), operations support system (OSS),[11] and business support system (BSS),[12] and potentially existing IT orchestration systems, if NFV orchestration and IT orchestration need to converge. The NFV architecture must support a migration path from today's proprietary physical network appliance-based solutions to more open standards-based virtual network appliance solutions. In other words, NFV must work in a hybrid network composed of classical physical network appliances and virtual network appliances. Virtual appliances must therefore use existing north-bound interfaces (for management and control) and interwork with physical appliances implementing the same functions.
- *Management and orchestration:* NFV presents an opportunity through the flexibility afforded by software network appliances operating in an open and standardized infrastructure to rapidly align MANO north-bound interfaces to well-defined standards and abstract specifications. Therefore, a consistent MANO architecture is required. This will greatly reduce the cost and time to integrate new virtual appliances into a network

[10] Element management system consists of systems and applications for managing network elements on the network element management layer. An element management system manages a specific type of telecommunications network element. The element management system typically manages the functions and capabilities within each network element but does not manage the traffic between different network elements in the network. To support management of the traffic between network elements, the element management system communicates upward to higher-level network management systems, as described in the telecommunications management network layered model.

[11] Operations support system is a platform used by service providers and network operators to support their network systems. The operations support system can help the operators to maintain network inventory, provision services, configure components, and resolve network issues. It is typically linked with the business support system to improve the overall customer experience.

[12] Business support systems (BSS) are platforms used by service providers, network operator delivery product management, customer management, revenue management (billing) and order management applications that help them run their business operations. Business support system platforms are often linked to operations support system platforms to support the overall delivery of services to customers.

operator's operating environment. The SDN further extends this concept to streamlining the integration of packet and optical switches into the system, for example, a virtual appliance or NFV orchestration system may control the forwarding behavior of physical switches using SDN. Note that NFV will only scale, if all of the functions can be automated.

- *Security and resilience:* Network operators need to be assured that the security, resilience, and availability of their networks are not compromised when VNFs are introduced. The NFV improves network resilience and availability by allowing NFs to be recreated on demand after a failure. A virtual appliance should be as secure as a physical appliance if the infrastructure, particularly the hypervisor and its configuration, is secure. Network operators will be seeking tools to control and verify hypervisor configurations. They will also require security-certified hypervisors and virtual appliances.
- *Network stability:* It is important to ensure that the stability of the network is not impacted when managing and orchestrating a large number of virtual appliances created by different hardware and hypervisor vendors. This is particularly important when virtual functions are relocated or during reconfiguration events (e.g., due to hardware and software failures) or due to a cyber attack. This challenge is not unique to NFV systems and such unsteadiness might also occur in current networks. It should be noted that the occurrence of network instability may have adverse effects on performance parameters or optimized use of resources.
- *Complexity:* It must be ensured that virtualized network platforms will be simpler to operate than those that exist today. A significant focus area for network operators is simplification of the plethora of complex network platforms and support systems which have evolved over decades of network technology evolution, while maintaining continuity to support important revenue-generating services.
- *Integration:* Seamless integration of multiple virtual appliances into existing industrial-grade servers and hypervisors is a major challenge for NFV schemes. Network operators need to be able to combine servers, hypervisors, and virtual appliances from different vendors without incurring significant integration costs. The ecosystem offers integration services and maintenance and third-party application support. It must be possible to resolve integration issues between several suppliers. The ecosystem will require mechanisms to validate new NFV products. Tools must be identified and/or created to address these issues.

1.1.2.1 Architectural Aspects

The NFV initiative began when network operators attempted to accelerate deployment of new network services in order to advance their revenue and growth plans. They found that customized hardware-based equipment limited their ability to achieve these goals. They studied standard IT virtualization technologies and found NFV helped accelerate service innovation and provisioning in that space [48].

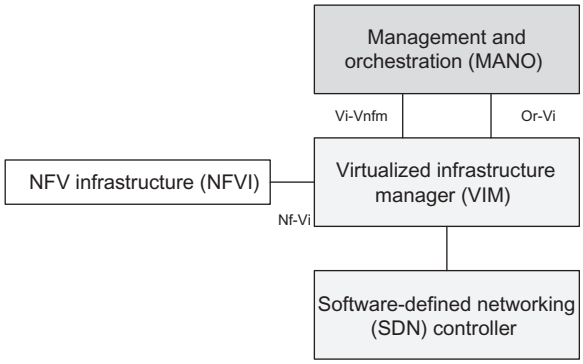


Figure 1.3
High-level concept of a virtualized network.

Fig. 1.3 illustrates the conceptual structure of a virtualized network and its main components. Following conversion of physical NFs to software, that is, virtual network functions (VNFs), the software applications need a platform to run. The NFV infrastructure (NFVI) consists of physical and virtual compute, storage, and networking resources that VNFs need to run. The NFVI layer primarily interacts with two other NFV framework components: VNFs and the virtual infrastructure manager (VIM). As we mentioned earlier, the VNF software runs on NFVI. The VIM, on the other hand, is responsible for provisioning and managing the virtual infrastructure. As shown in Fig. 1.4, the VNF to NFVI interface (Vn−Nf) constitutes a data path through which network traffic traverses, while the NFV to VIM interface (Nf−Vi) creates a control path that is used solely for management but not for any network traffic. The NFVI consists of three distinct layers: physical infrastructure, virtualization layer, and the virtual infrastructure. The VIM manages the NFVI and acts as a conduit for control path interaction between VNFs and NFVI. In general, the VIM provisions, de-provisions, and manages virtual compute, storage, and networking while communicating with the underlying physical resources. The VIM is responsible for operational aspects such as logs, metrics, alerts, analytics, policy enforcement, and service assurance. It is also responsible for interacting with the orchestration layer and SDN controller. Unlike the NFVI which consists of several technologies that can be assembled independently, the VIM comes in the form of complete software stacks. OpenStack[13] is the main VIM software stack which is very common in NFV realization.

[13] OpenStack software controls large pools of compute, storage, and networking resources throughout a data center, managed through a dashboard or via the OpenStack application programming interface. OpenStack works with popular enterprise and open source technologies, making it ideal for heterogeneous infrastructure (https://www.openstack.org/).

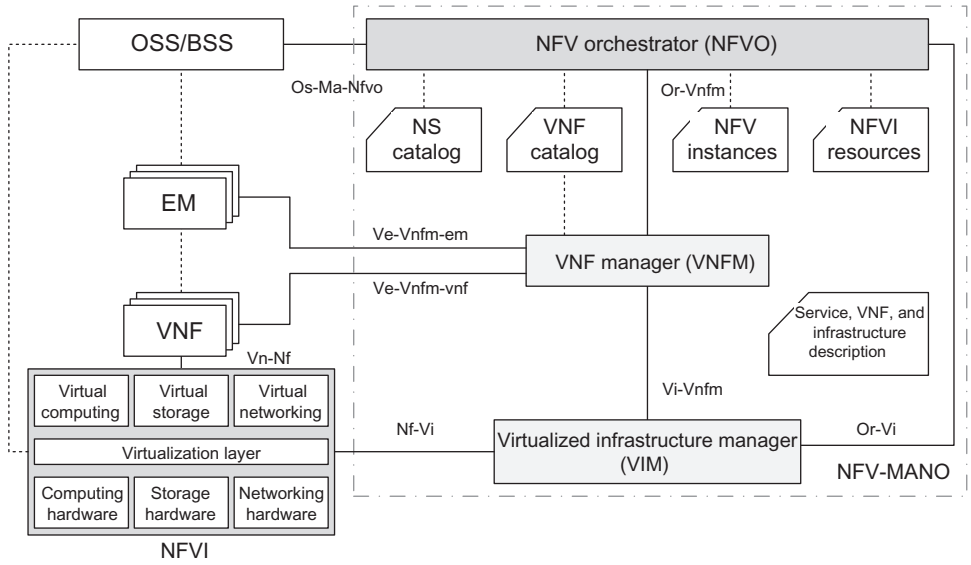


Figure 1.4
NFV architecture [37,40].

As we mentioned earlier, NFV defines standards for compute, storage, and networking resources that can be used to build VNFs. The NFVI is a key component of the NFV architecture that describes the hardware and software components on which virtual networks are built. The NFV leverages the economies of scale of the IT industry. The NVFI is based on widely available and low-cost, standardized computing components. The NFVI works with different types of servers, for example, virtual or bare metal, software, hypervisors, VMs, and VIMs in order to create a platform for VNFs to run. The NFVI standards help increase the interoperability of the components of the VNFs and enable multivendor environments [42–44].

The NFV architecture comprises major components including VNFs, NFV-MANO, and NFVI that work with traditional network components like OSS/BSS. The NFVI further consists of NFVI points-of-presence (NFVI-PoPs[14]), which are the sites at which the VNFs are deployed by the network operator, including resources for computation, storage, and networking. NFVI networks interconnect the computing and storage resources contained in an NFVI-PoP. This may include specific switching and routing devices to allow external connectivity. The NFVI works directly with VNFs and VIMs and in concert with the NFV orchestrator (NFVO). NFV services are instantiated and instructed by the NFVO, which utilizes VIMs that manage the resources from the underlying infrastructure. The NFVI is

[14] Network function virtualization infrastructure points-of-presence is a single geographic location where a number of network function virtualization infrastructure nodes are situated.

critical to realizing the business benefits outlined by the NFV architecture. It delivers the actual physical resources and corresponding software on which VNFs can be deployed. NFVI creates a virtualization layer on top of the hardware and abstracts the hardware resources, so they can be logically partitioned and allocated to the VNF in order to perform their functions. NFVI is also critical to building more complex networks without geographical limitations of traditional network architectures.

A network service can be viewed architecturally as a forwarding graph of NFs interconnected by the supporting network infrastructure. These NFs can be implemented in a single operator network or inter-work between different operator networks. The underlying NF behavior contributes to the behavior of the higher level service. Therefore, the network service behavior is a combination of the behavior of its constituent functional blocks, which can include individual NFs, NF sets, NF forwarding graphs, and/or the infrastructure network. The end points and the NFs of the network service are represented as nodes and correspond to devices, applications, and/or physical server applications. An NF forwarding graph can have NF nodes connected by logical links that can be unidirectional, bidirectional, multicast, and/or broadcast. Fig. 1.4 shows the NFV architectural framework depicting the functional blocks and reference points in the NFV framework. The main reference points and execution reference points are shown by solid lines and are in the scope of European Telecommunications Standards Institute (ETSI) NFV specification [37–41]. The dotted reference points are available in present deployments but may need extensions for handling NFV. However, the dotted reference points are not the main focus of the NFV at present. The illustrated architectural framework focuses on the functionalities necessary for the virtualization and the resulting operation of the network. It does not specify which NFs should be virtualized, as that is solely a decision of the network operator.

1.1.2.2 Functional Aspects

The NFV architectural framework, shown in Fig. 1.4, identifies functional blocks and the main reference points between the blocks. Some of these blocks are already present in current deployments, whereas others might be necessary additions in order to support the virtualization process and the subsequent operation. The functional blocks are as follows [37]:

- VNF is a virtualization of a network function in a legacy non-virtualized network.
- Element management (EM) performs the typical management functionality for one or several VNFs. NFV elements are the discrete hardware and software requirements that are managed in an NFV installation to provide new communication services and application services on commodity-based hardware. NFV services are deployed on commercial off-the-shelf hardware platform, typically run on x86-based or ARM-based computing platform and standard switching hardware. The early model of NFV, ETSI MANO, is a common reference architecture. The NFV architecture developed by ETSI

MANO includes EMSs, which describe how individual VNFs are managed on a commodity hardware platform.

- NFVI represents the entire hardware and software components which create the environment in which VNFs are deployed, managed, and executed. The NFVI can span across several locations, that is, places where NFVI-PoPs are operated. The network providing connectivity between these locations is regarded as part of the NFVI.
- Virtualization layer abstracts the hardware resources and decouples the VNF software from the underlying hardware, thus ensuring a hardware independent life cycle for the VNFs. The virtualization layer is responsible for abstracting and logically partitioning physical resources; enabling the software that implements the VNF to use the underlying virtualized infrastructure; and providing virtualized resources to the VNF. The virtualization layer ensures VNFs are decoupled from hardware resources, thus the software can be deployed on different physical hardware resources. Typically, this type of functionality is provided for computing and storage resources in the form of hypervisors and VMs. A VNF can be deployed in one or several VMs.
- VIM(s) comprises the functionalities that are used to control and manage the interaction of a VNF with computing, storage, and network resources under its authority as well as their virtualization.
- NFVO is in charge of the orchestration and management of NFVI and software resources and realizing network services on NFVI.
- VNF manager(s) is responsible for VNF life cycle management (e.g., instantiation, update, query, scaling, and termination). Multiple VNF managers may be deployed where a VNF manager may be deployed for each VNF or multiple VNFs.
- Service, VNF and infrastructure description is a data set which provides information regarding the VNF deployment template, VNF forwarding graph, service-related information, and NFVI information models. These templates/descriptors are used internally within NFV-MANO. The NFV-MANO functional blocks handle information contained in the templates/descriptors and may expose (subsets of) such information to applicable functional blocks.
- Operations and Business Support Systems (OSS/BSS)

The management and organization working group of the ETSI[15] has defined the NFV-MANO architecture. According to ETSI specification, NFV-MANO comprises three major functional blocks: VIM, VNF manager, and NFVO [37,40]. The VIM is a key component of the NFV-MANO architectural framework. It is responsible for controlling and managing the NFVI compute, storage, and network resources, usually within one operator's infrastructure domain (see Fig. 1.4). These functional blocks help standardize the functions of virtual

[15] European Telecommunications Standards Institute, http://www.etsi.org/.ETSI, network function virtualization specifications are listed and can be found at http://www.etsi.org/technologies-clusters/technologies/nfv.

networking to increase interoperability of SDN elements. The VIMs can also handle hardware in a multi-domain environment or may be optimized for a specific NFVI environment. The VIM is responsible for managing the virtualized infrastructure of an NFV-based solution. The VIM operations include the following:

- It maintains an inventory of the allocation of virtual resources to physical resources. This allows the VIM to orchestrate the allocations, upgrade, release, and retrieval of NFVI resources and optimize their use.
- It supports the management of VNF forwarding graphs by organizing virtual links, networks, subnets, and ports.
- The VIM also manages security group policies to ensure access control.
- It manages a repository of NFVI hardware resources (compute, storage, and networking) and software resources (hypervisors), along with the discovery of the capabilities and features to optimize the use of such resources.
- The VIM performs other functions as well, such as collecting performance and failure information via notifications; managing software images (add, delete, update, query, or copy) as requested by other NFV-MANO functional blocks; and managing catalogs of virtualized resources that can be used by NFVI.

In summary, the VIM is a management layer between the hardware and the software in an NFV domain. VIMs are critical to realizing the business benefits that can be provided by the NFV architecture. They coordinate the physical resources that are necessary to deliver network services. This is particularly noticeable by infrastructure-as-a-service providers, where their servers, networking, and storage resources must work smoothly with the software components running on top of them. They must ensure that resources can be appropriately allocated to fulfill the dynamic service requirements.

The NFVI consists of three distinct layers: physical infrastructure, virtualization layer, and the virtual infrastructure, as shown in Fig. 1.4. The NFVI hardware consists of computing, storage, and networking components. OpenStack is often used in conjunction with NFV technology in data centers to deploy cloud services, especially communication services offered by large service providers and cloud providers. OpenStack is an open source virtualization platform. It enables the service providers to deploy VNFs using commercial off-the-shelf hardware. These applications are hosted in a data center so that they could be accessed via the cloud, which is the underlying model to use NFV. The VIM manages the NFVI and serves as a conduit for control path interaction between VNFs and NFVI. The VIM assigns, provisions, de-provisions, and manages virtual computing, storage, and networking resources while communicating with the underlying physical resources. The VIM is responsible for operational aspects, such as logs, metrics, alerts, root cause analysis, policy enforcement, and service assurance. It is also responsible for interacting with the orchestration layer (MANO) and SDN controller.

NFV is managed by NFV-MANO, which is an ETSI-defined framework for the management and orchestration of all resources in the cloud data center. This includes computing, networking, storage, and VM resources. The main focus of NFV-MANO is to allow flexible on-boarding and to avoid the possible disorder that can arise during transition states of network components. As we mentioned earlier, the NFV-MANO consists of three main components:

1. NFVO is responsible for on-boarding of new network services and VNF packages; network service life cycle management; global resource management; and validation and authorization of NFVI resource requests. The NFVO is a key component of the NFV-MANO architectural framework, which helps standardize the functions of virtual networking to increase interoperability of SDN-controlled elements. Resource management is important to ensure there are adequate compute, storage, and networking resources available to provide network services. To meet that objective, the NFVO can work either with the VIM or directly with NFVI resources, depending on the requirements. It has the ability to coordinate, authorize, release, and engage NFVI resources independent of any specific VIM. It can also control VNF instances sharing resources of the NFVI.
2. VNF manager oversees life cycle management of VNF instances; coordination and adaptation role for configuration; and event reporting between NFVI and EMs.
3. VIM controls and manages the NFVI compute, storage, and networking resources.

1.1.2.3 Operational Aspects

A VNF may be composed of one or multiple VNF components (VNFC). A VNFC may be a software entity deployed in the form of a virtualization container. A VNF realized by a set of one or more VNFCs appears to the outside as a single, integrated system; however, the same VNF may be realized differently by each VNF provider. For example, one VNF developer may implement a VNF as a monolithic, vertically integrated VNFC, and another VNF developer may implement the same VNF using separate VNFCs, for example, one for the control plane, one for the user plane, and one for the EM. VNFCs of a VNF are connected in a graph. For a VNF with only a single VNFC, the internal connectivity graph is a null graph [37].

A VNF can assume a number of internal states to represent the status of the VNF. Transitions between these states provide architectural patterns for some expected VNF functionality. Before a VNF can start its life cycle, it is a prerequisite that the VNF was onboarded (process of registering the VNF with the NFVO and uploading the VNF descriptor). Fig. 1.5 provides a graphical overview of the VNF states and state transitions. Each VNFC of a VNF is either parallelizable or nonparallelizable. If it is parallelizable, it may be instantiated multiple times per VNF instance, but there may be a constraint on the minimum and maximum number of parallel instances. If it is nonparallelizable, it is instantiated once per VNF instance. Each VNFC of a VNF may need to handle the state information, where it can be either stateful or stateless. A VNFC that does not have to handle state information is

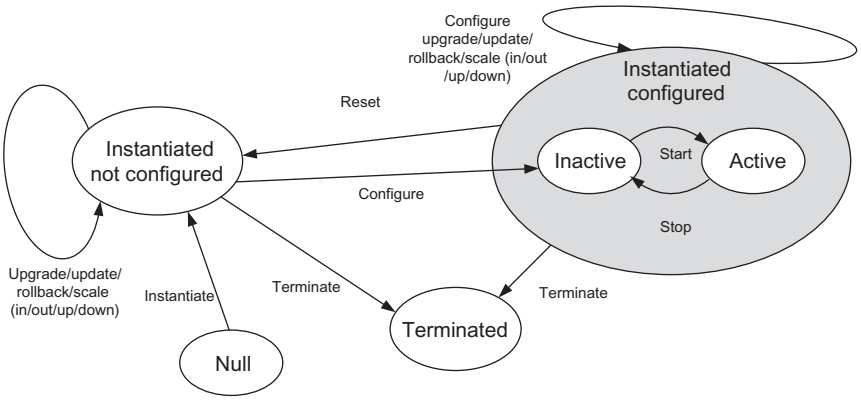


Figure 1.5
VNF instance and state transitions [37].

a stateless VNFC. A VNFC that needs to handle state information may be implemented either as a stateful VNFC or as a stateless VNFC with an external state where the state information is held in a data repository external to the VNFC.

Depending on the type of VNF, the instantiation can be more or less complex. For a simple VNF consisting of a single VNFC, the instantiation based on VNF descriptor is straightforward, while for a complex VNF consisting of several VNFCs connected via virtual networks, the VNF manager may require support from an internal function that is implemented by VNF to facilitate the process of instantiation. As an example, the VNF manager could boot a predefined number of VNFCs, leaving booting of the remaining VNFCs and the configuration of the VNF to an internal VNF provider-specific process that may also involve an EM.

The VNF descriptor is a specification template provided by the VNF developer for describing virtual resource requirements of a VNF. It is used by the NFV-MANO functions to determine how to execute VNF life cycle operations such as instantiation. The NFV-MANO functions consider all VNF descriptor attributes to check the feasibility of instantiating a given VNF. There are several options for how the instances of individual VNFCs can be created, which can be fully or partially loaded virtualization containers; or empty virtualization containers prepared for booting and loading. It is then the responsibility of the VNF MANO functions to instruct the VIM to create an empty virtualization container with an associated interface that is ready for use.

To instantiate a VNF, the VNF manager creates the VNF's set of VNFC instances as defined in the VNF descriptor by executing one or more VNFC instantiation procedures. The VNF descriptor defines which VNFC instances may be created in parallel or sequentially as well as the order of instantiation. The set of created VNFC instances may already

correspond to a complete VNF instance. Alternatively, it may contain only a minimal set of VNFC instances needed to boot the VNF instance. The VNF manager requests a new VM and the corresponding network and storage resources for the VNFC instance according to the definition in the VNF descriptor or uses a VM and the corresponding network and storage resources previously allocated to it. Following successful completion of this process, the VNF manager requests to start the VM [37].

1.1.2.4 Legacy Support and Interworking Aspects

In general, the behavior of a complete system can be characterized when the constituent functional blocks and their interconnections are specified. An inherent property of a functional block (in traditional sense) is that its operation is autonomous. The behavior of a functional block is characterized by the static transfer function of the functional block, the dynamic state of the functional block, and the inputs/outputs received/generated at the corresponding reference points. If a functional block is disconnected from an immediately preceding functional block, it will continue to function and generate outputs; however, it will process a null or invalid input. As we mentioned earlier, the objective of NFV is to separate software that defines the NF (the VNF) from the hardware and the generic software that creates the hosting NFVI on which the VNF runs. Therefore, it is a requirement that the VNFs and the NFVI be separately specified. However, this is a requirement that is not immediately satisfied by traditional method of functional blocks and associated interfaces. Fig. 1.6 shows an example where a traditional network comprising three functional blocks is evolved into a hypothetical case where two of the three functional blocks have been virtualized. In each case, the functional block is implemented as a VNF that runs on a host function in the NFVI. However, in this process, there are two important differences with the standard functional block representation that must be noted. The VNF is not a functional block independent of its host function, because the VNF cannot exist autonomously in the way that a functional block can exist. The VNF depends on the host function for its

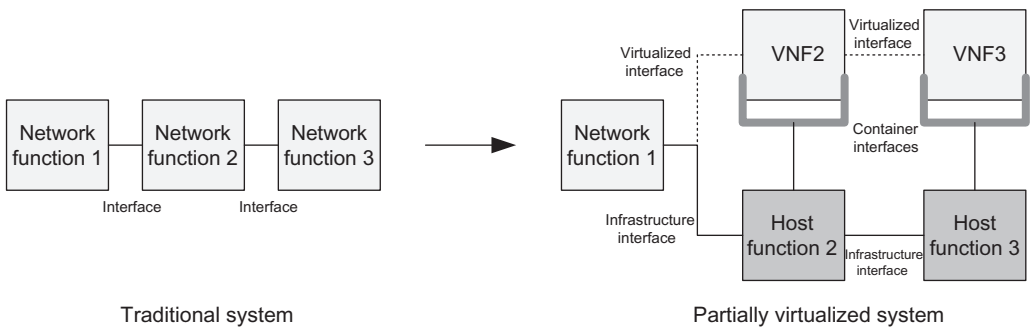


Figure 1.6
Traditional and virtualized network functions [40].

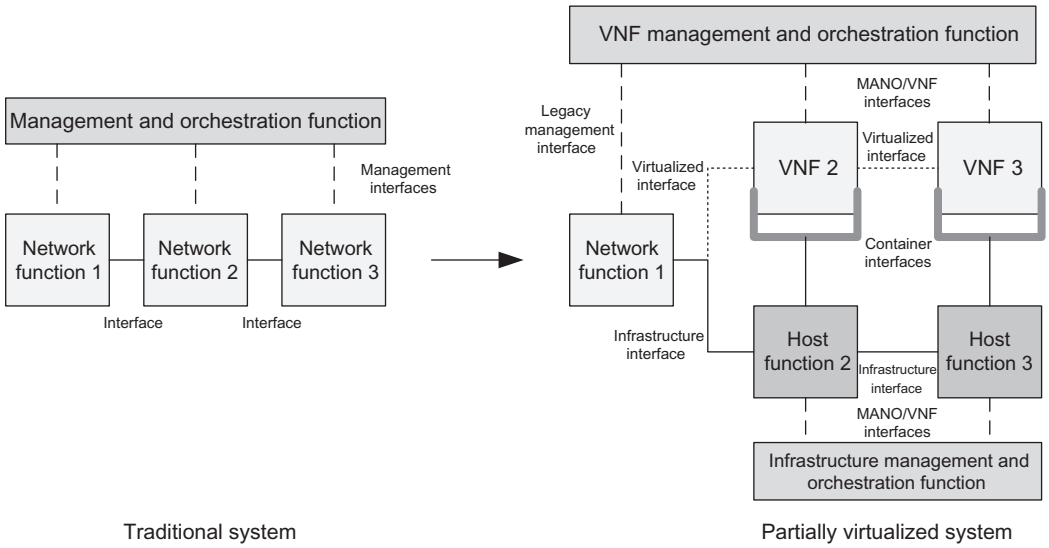


Figure 1.7
MANO of traditional and virtualized network functions [40].

existence and if the host function is interrupted, or disappears, then the VNF will be interrupted or disappear. Similarly, the container interface reflects this existence dependency between a VNF and its host function. The relationship between the VNF and its host function can be described as follows: the VNF is a configuration of the host function and the VNF is an abstract view of the host function when the host function is configured by the VNF. Therefore a host function, when configured with a VNF, has the external appearance as a functional block in traditional sense, implementing the VNF specification. It is the host function that is the functional block, but it externally appears to be the VNF. Equivalently, the VNF is an abstract view of the host function.

In an operator's network, NFs can be remotely configured and managed. For this purpose, the NFs have an interface, often referred to as a north-bound interface, to the MANO function. The MANO function is often complex and includes a large number of distributed components. However, it can be characterized using the same system model comprising functional blocks and their interfaces (see Fig. 1.7). The objective of NFV is to separate the VNFs from the infrastructure including their management. As shown in Fig. 1.7, the MANO functions are divided between the MANO of the NFVI and the MANO of the VNFs.

The MANO of the NFVI is an integral part of the NFV framework. One possible scenario is the management of the existing NFs that are partially virtualized by an NFV deployment. Managing the VNFs using the existing systems can be used for the deployment of NFV in the transition period as illustrated in Fig. 1.7. The removal of the hardware from the VNFs eliminates the requirement of managing hardware aspects. The flexibility provided by NFV can only

be fully achieved, if the MANO implements efficient VNF life cycle management process adapted to new requirements such as fast order delivery, fast recovery, and auto-scaling.

1.1.3 Separation of Control and User Planes (Software-Defined Networks)

SDN is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions, enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The OpenFlow protocol is a fundamental element for building SDN solutions. The OpenFlow standard, created in 2008, was recognized as the first SDN architecture that defined how the control- and data-plane elements would be separated and communicate with each other using the OpenFlow protocol. The Open Networking Foundation (ONF)[16] is the body in charge of managing OpenFlow standards, which are open-source specifications. However, there are other standards and open-source organizations with SDN resources, thus OpenFlow is not the only protocol that makes up SDN framework. SDN is a complementary approach to NFV for network management. While they both manage networks, both rely on different methods. SDN offers a centralized view of the network, giving an SDN controller the ability to act as the intelligence of the network. As shown in Fig. 1.8, the SDN controller communicates with switches and routers via south-bound APIs and to the applications with north-bound APIs. In the SDN architecture, the splitting of the control and data forwarding functions is referred to as disaggregation because these components can be sourced separately, rather than deployed as a single integrated system. This architecture provides the applications with more information about the state of the entire network from the controller's perspective compared to the traditional networks where the network is application aware. The SDN architectures generally consist of three functional groups, as follows:

- *SDN applications:* The application plane consists of applications such as routing and load balancing, which communicates with the SDN controller in the control plane through north-bound interfaces (e.g., REST[17] and JSON[18]). SDN applications are programs that communicate behaviors and needed resources with the SDN controller via APIs. In addition, the applications can build an abstracted view of the network by collecting information from the controller for decision-making purposes. These

[16] Open Networking Foundation (https://www.opennetworking.org).

[17] A REST application programming interface, also referred to as a RESTful web service, is based on Representational State Transfer (REST) scheme that is an architectural style and approach to communications often used in web services development. REST-compliant web services allow requesting systems to access and manipulate textual representations of web resources using a uniform and predefined set of stateless operations. A RESTful API is an application program interface that uses HTTP requests to GET, PUT, POST, and DELETE data.

[18] JSON or JavaScript Object Notation, is a minimal, readable format for structuring data. It is used primarily to transmit data between a server and web application, as an alternative to XML.

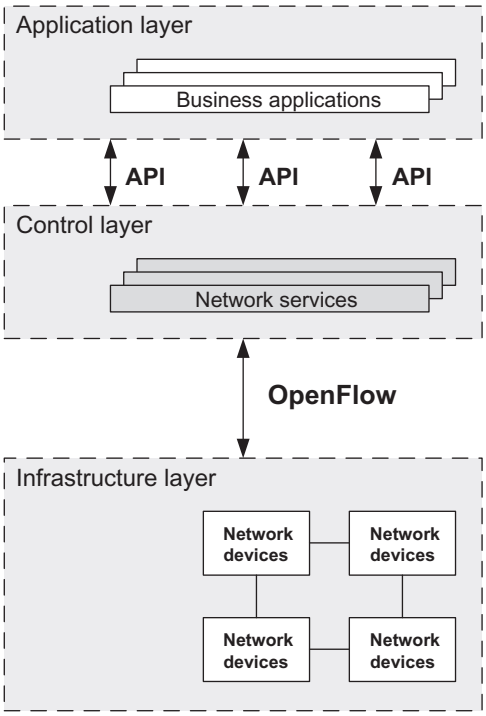


Figure 1.8
Illustration of the SDN concept [49].

applications include network management, analytics, or business applications that are used to run large data centers. For example, an analytics application might be built to recognize suspicious network activity for security purposes.

- *SDN controller:* The SDN controller is a logical entity that receives instructions or requirements from the SDN application layer and relays them to the networking components. The controller also extracts information about the network from the hardware devices and communicates back to the SDN applications with an abstract view of the network, including statistics and events. The control plane consists of one or a set of SDN controllers (e.g., Open Network Operating System[19] or OpenDayLight[20]), which logically maintain a global and dynamic network view, and provide control tasks to manage the network devices in the user plane via south-bound

[19] Open Network Operating System is an open-source software-defined network operating system (https://wiki.onosproject.org/).

[20] OpenDaylight is an open-source software-defined networking project hosted by Linux Foundation, which was created in order to advance software-defined networking adoption and to create a strong basis for network function virtualization. It was created as a community-led and industry-supported open-source framework. The goal of the OpenDaylight project is to offer a functional software-defined networking platform that can provide the users with directly deployable software-defined networking platform without the need for other components. In addition to this, contributors and vendors can deliver add-ons and other pieces that will offer more value to OpenDaylight (https://www.opendaylight.org/).

interfaces (e.g., OpenFlow or ForCES[21]) based on requests from the applications. The controllers communicate with each other using east−west-bound interfaces.

- *SDN networking devices:* The SDN networking devices on the infrastructure layer control the forwarding and data processing capabilities of the network. This includes forwarding and processing of the data path. The user plane is composed of data forwarding elements, such as virtual/physical switches and routers, which forward and route the data packets based on the rules prescribed by the SDN controllers. This plane is responsible for all activities related to provisioning and monitoring of the networks.

The SDN architecture APIs are often referred to as north-bound and south-bound interfaces, defining the communication between the applications, controllers, and networking systems. A north-bound interface is defined as the connection between the controller and applications, whereas the south-bound interface is the connection between the controller and the physical networking hardware. Since SDN is a virtualized architecture, these elements do not have to be physically co-located. An SDN controller platform typically contains a collection of pluggable modules that can perform different network functions such as tracking device inventory within the network along with maintaining information about device capabilities, network statistics and analytics, etc. Extensions can be inserted in the SDN controller to enhance its functionality in order to support more advanced capabilities such as running algorithms to perform analytics and orchestrating new rules throughout the network.

The centralized, programmable SDN environments can easily adjust to the rapidly evolving needs of enterprise networks. The SDN can lower the cost and limit the uneconomical provisioning and can further provide flexibility in the networks. As already mentioned above, SDN and NFV are set to play key roles for operators as they prepare to migrate from 4G to 5G and to gradually scale their networks. NFVO and NFVI, along with SDN, are critical to the success of 5G rollouts, enabling agile infrastructure that can adapt to network slicing, low latency, and high-capacity requirements of major 5G use cases.

One of the key architectural enhancements in 3GPP's 5G network is control- and user-plane separation (CUPS) of EPC nodes, which enables flexible network deployment and operation

[21] Forwarding and control element separation defines an architectural framework and associated protocols to standardize information exchange between the control plane and the user/forwarding plane in a forwarding and control element separation network element. IETF RFC 3654 and RFC 3746 have defined the forwarding and control element separation requirements and framework, respectively (see https://tools.ietf.org/html/rfc5810).

by distributed or centralized deployment and the independent scaling between control-plane and user-plane functions. In other words, the network equipment is now changing from closed and vendor-specific to open and generic with SDN architectural model, which enables the separation of control and data planes, and allows networks to be programmed through open interfaces. With NFV, network functions that were previously realized in costly customized-hardware platforms are now implemented as software appliances running on low-cost commodity hardware or running in cloud computing environments. By splitting the network entities in this manner (i.e., from serving gateway (SGW) to SGW-C and SGW-U and from packet gateway (PGW) to PGW-C and PGW-U), it is possible to scale these components independently and to enable a range of deployment options. The protocol used between the control and user planes can be either an extension of the existing OpenFlow protocol or new interfaces which have been specified as part of 3GPP CUPS work item [1].

1.1.3.1 Architectural Aspects

Next-generation networks are experiencing an increase in use of very dense deployments where user terminals will be able to simultaneously connect to multiple transmission points. It is a significant advantage for the next-generation access networks to design the architecture on the premises of separation of the control-plane and user-plane functions. This separation would imply allocation of specific control-plane and user-plane functions between different nodes. As we stated earlier, the goal of SDN is to enable cloud and network engineers and administrators to respond quickly to changing business requirements via a centralized control platform. SDN encompasses multiple types of network technologies designed to make the networks more flexible and agile to support the virtualized server and storage infrastructure of the modern data centers. The SDN was originally defined as an approach to designing, building, and managing networks that separates the network's control and forwarding planes, enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. All SDN models have some version of an SDN controller, as well as south-bound APIs and north-bound APIs. As shown in Fig. 1.9, an SDN controller is interfaced with the application layer and the infrastructure layer via north-bound and south-bound APIs, respectively. As the intelligence of the network, SDN controllers provide a centralized view of the overall network and enable network administrators to instruct the underlying systems (e.g., switches and routers) on how the forwarding plane should route/handle network traffic. SDN uses south-bound APIs to relay information to the switches and routers. OpenFlow, considered the first standard in SDN, was the original south-bound API and remains as one of the most commonly used protocols. Despite some belief considering OpenFlow and SDN to be the same, OpenFlow is merely one piece of the larger SDN framework. SDN uses north-bound APIs to communicate with the

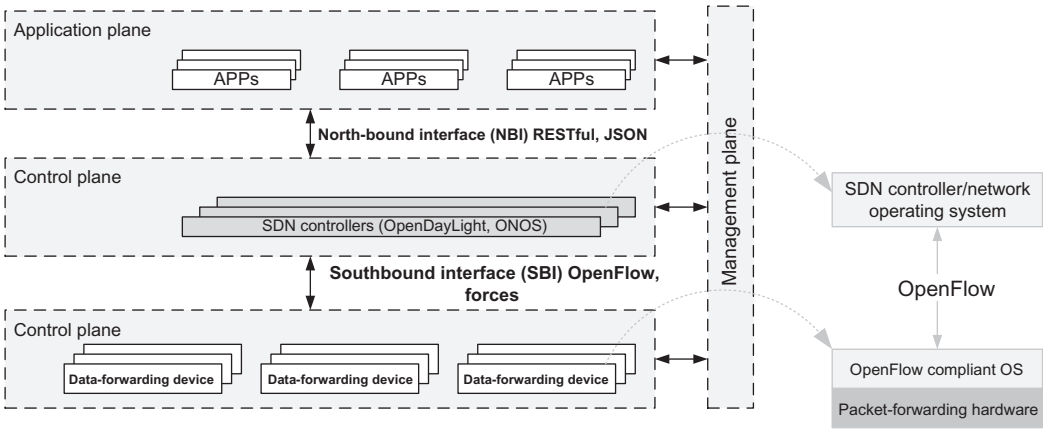


Figure 1.9
SDN framework and its main components [71].

applications in the application layer. These help network administrators to programmatically shape the traffic and deploy services.

In the SDN architecture for 5G networks, shown in Fig. 1.9, there are notably three layers: an infrastructure layer (user plane), a control layer (control plane), and an application layer (application plane). The infrastructure layer mainly consists of forwarding elements (e.g., physical and virtual switches, routers, wireless access points) that comprise the data plane. These devices are mainly responsible for collecting network status, storing them temporarily in local network devices, and sending the stored data to the network controllers and for managing packets based on the rules set by the network controllers or administrators. They allow the SDN architecture to perform packet switching and forwarding via an open interface. The control layer/control plane maintains the link between the application layer and the infrastructure layer through open interfaces. Three communication interfaces allow the controller to interact with other layers: the south-bound interface for interacting with the infrastructure layer, the north-bound interface for interacting with the application layer, and east−west-bound interfaces for communicating with groups of controllers. Their functions may include reporting network status and importing packet-forwarding rules and providing various service access points (SAPs) in various forms. The application layer is designed mainly to fulfill user requirements. It consists of the end-user business applications that utilize network services and resources. The SDN applications are able to control and access switching devices at the data layer through the control-plane interfaces. The SDN applications include network visualization, dynamic access control, security, mobility, cloud computing, and load balancing.

The functionalities of an SDN controller can be classified into four categories: (1) a high-level language for SDN applications to define their network operation policies; (2) a rule update process to install rules generated from those policies; (3) a network status

collection process to gather network infrastructure information; and (4) a network status synchronization process to build a global network view using the network status collected by each individual controller. One of the basic functions of the SDN controller is to translate application specifications into packet-forwarding rules. This function uses a protocol to address communication between its application layer and control layer. Therefore, it is imperative to utilize some high-level languages (e.g., C++, Java, and Python) for the development of applications between the interface and the controllers. An SDN controller is accountable for generating packet-forwarding rules as well as clearly describing the policies and installing the rules in relevant devices. The forwarding rules can be updated with policy changes. Furthermore, the controller should maintain consistency for packet forwarding by using either the original rule set/updated rule set or by using the updated rules after the update process is completed. The SDN controllers collect network status to provide a global view of the entire network to the application layer. The network status includes time duration, packet number, data size, and flow bandwidth. Unauthorized control of the centralized controller can degrade controller performance. Generally, this can be overcome by maintaining a consistent global view of all controllers. Moreover, SDN applications play a significant role in ensuring application simplicity and guaranteeing network consistency.

In most SDNs, OpenFlow is used as the south-bound interface. OpenFlow is a flow-oriented protocol and includes switches and port abstraction for flow control. The OpenFlow protocol is currently maintained by ONF and serves as a fundamental element for developing SDN solutions. The OpenFlow, the first standard interface linking the forwarding and controls layers of the SDN architecture, allows management and control of the forwarding plane of network devices (e.g., switches and routers) both physically and virtually. The OpenFlow helps SDN architecture to adapt to the high bandwidth and dynamic nature of user applications, adjust the network to different business needs, and reduce management and maintenance complexity. It must be noted that OpenFlow is not the only protocol available or in development for SDN. To work in an OpenFlow environment, any device that wants to communicate to an SDN controller must support the OpenFlow protocol. The SDN controller sends changes to the switch/router flow table through south-bound interface, allowing network administrators to partition traffic, control flows for optimal performance, and start testing new configurations and applications (see Fig. 1.10).

The OpenFlow features support a number of commonly used data-plane protocols, ranging from layer-2 to layer-4, with packet classification being performed using stateless match tables, and packet processing operations, known as actions or instructions, ranging from header modification, metering, QoS, packet replication (e.g., to implement multicast or link aggregation), and packet encapsulation/de-encapsulation. Various statistics are defined per port, per table, and per table entry. Information can be retrieved on demand or via notifications. OpenFlow is, however, not merely an interface. It also defines the expected behavior of the switch and how the behavior can be customized using the interface. An OpenFlow controller is an SDN controller that uses the OpenFlow protocol to connect and

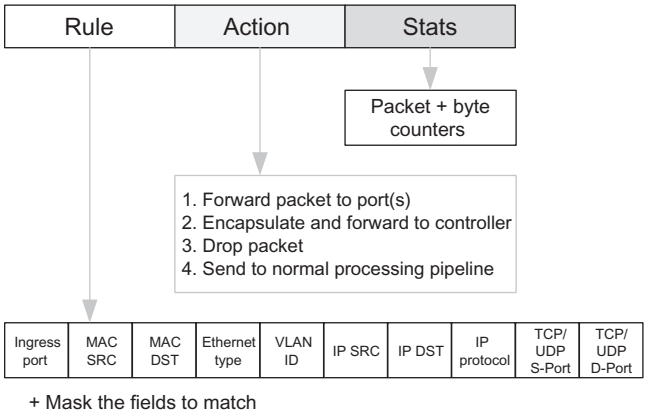


Figure 1.10
Example of OpenFlow flow table entries [48,49].

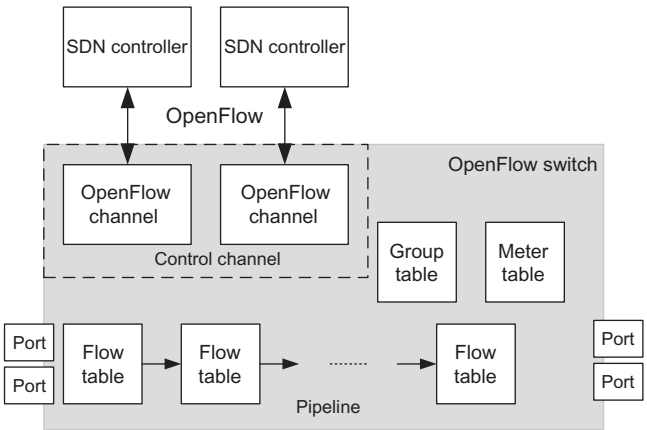


Figure 1.11
Main components of an OpenFlow switch [49].

configure the network devices in order to find the best path for application traffic. OpenFlow controllers create a central control point to manage OpenFlow-enabled network components.

An OpenFlow logical switch (see Fig. 1.11) consists of one or more flow tables and a group table, which perform packet lookups and forwarding, and one or more OpenFlow channels to an external controller. The switch communicates with the controller and the controller manages the switch via the OpenFlow switch protocol. Using the OpenFlow switch protocol, the controller can add, update, and delete flow entries in flow tables, both reactively (in response to packets) and proactively. As shown in Fig. 1.10, each flow table in the switch contains a set of flow entries; each flow entry consists of match fields, counters, and a set of instructions to apply to matching packets. Matching starts at the first

flow table and may continue to additional flow tables of the pipeline. Flow entries match packets in priority order, with the first matching entry in each table being used. If a matching entry is found, the instructions associated with the specific flow entry are executed. If no match is found in a flow table, the outcome depends on configuration of the table-miss flow entry, for example, the packet may be forwarded to the controllers over the OpenFlow channel, dropped, or may continue to the next flow table. Instructions associated with each flow entry either contain actions or modify pipeline processing. Actions included in instructions describe packet forwarding, packet modification, and group table processing. Pipeline processing instructions allow packets to be sent to subsequent tables for further processing and allow information, in the form of meta-data, to be communicated between tables. Table pipeline processing stops when the instruction set associated with a matching flow entry does not specify a next table; at this point the packet is usually modified and forwarded [49].

We now change our focus to 3GPP CUPS and discuss the efforts within 3GPP to enable SDN control of networks. 3GPP completed Rel-14 specification of control- and user-plane separation work item in June 2014, which is a key core network feature for many operators. Control- and user-plane separation of EPC nodes provides architecture enhancements for the separation of functionalities in the EPC's SGW, PGW, and traffic detection function (TDF).[22] This enables flexible network deployment and operation, distributed or centralized architecture, as well as independent scaling between control-plane and user-plane functions without affecting the functionality of the existing nodes as a result of the split. The user data traffic in operators' networks have been doubling on an annual basis in recent years due to increasing use of smart devices, proliferation of video streaming, and other broadband applications. At the same time, there is a strong consumer demand for improved user experience, higher throughput, and lower latency. The CUPS scheme allows for reducing the latency of application/service by selecting user-plane nodes which are closer to the RAN or more appropriate for the intended usage type without increasing the number of control-plane nodes. It further supports increase of data traffic by enabling addition of user-plane nodes without changing the number of control-plane nodes (SGW-C, PGW-C, and TDF-C) in the network. The CUPS scheme further allows locating and scaling control-plane and user-plane resources of the EPC nodes independently as well as enabling independent evolution of the control-plane and user-plane functions. The CUPS paradigm is a precursor

[22] Traffic detection function has become an important element in the mobile networks due to the increasing complexities in managing data services, demand for personalization, and service differentiation. Traffic detection function provides communication service providers the opportunity to capitalize on analytics for traffic optimization, charging and content manipulation, working in conjunction with policy management and charging system. Traffic detection function enforces traffic policies based on predetermined rules or dynamically determined rules by the policy and charging rules function on data flows in real time. Traffic detection function was introduced together with Sd reference point as a means for traffic management in the 3GPP Rel-11 specifications using layer-7 traffic identification.

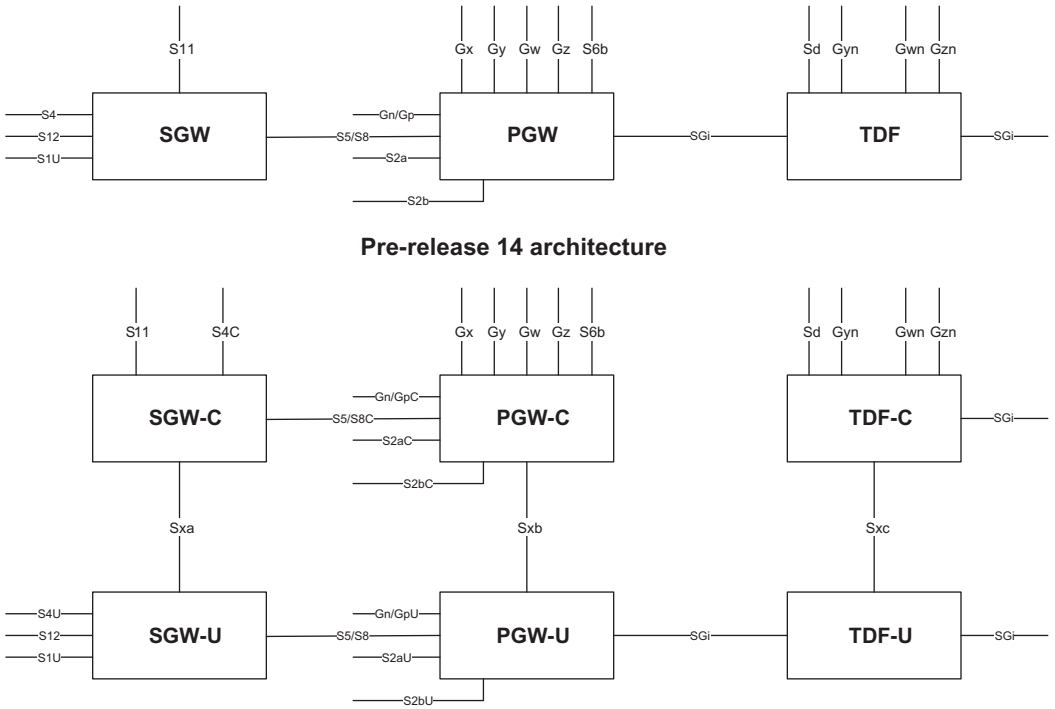


Figure 1.12
Separation of control plane and user plane in EPC [1].

to the use of SDN concept in 3GPP networks. The following high-level principles were incorporated in the CUPS framework [8,36]:

- As shown in Fig. 1.12, the control-plane functions terminate control-plane protocols such as GTP-C, Diameter[23] (Gx, Gy, Gz) and a control-plane function can interface multiple user-plane functions, as well as a user-plane function can be shared by multiple control-plane functions.
- A UE is served by a single SGW-C but multiple SGW-U can be selected for different packet data network (PDN) connections. A user-plane data packet may traverse multiple user-plane functions.

[23] Diameter is an application-layer protocol for authentication authorization and accounting. It is a message-based protocol, where authentication authorization and accounting nodes receive positive or negative acknowledgment for each message exchanged. For message exchange, Diameter uses the transmission control protocol and stream control transmission protocol, which makes it more reliable. Diameter base protocol is specified in IETF RFC 6733 (https://tools.ietf.org/html/rfc6733).

- The control-plane functions control the processing of the packets in the user-plane by provisioning a set of rules in Sx sessions, that is, packet detection, forwarding, QoS enforcement, and usage reporting rules.
- While all 3GPP features impacting the user-plane functions (e.g., policy and charging control, lawful interception, etc.) are supported, the user-plane functions are designed to be 3GPP agnostic as much as possible.
- A legacy SGW, PGW, and TDF can be replaced by a split node without effecting connected legacy nodes.

As shown in Fig. 1.12, CUPS introduces three new interfaces, namely Sxa, Sxb, and Sxc between the control-plane and user-plane functions of the SGW, PGW, and TDF, respectively.

3GPP evaluated candidate protocols such as OpenFlow, ForCES, and Diameter. The criteria identified for the selection process included ease of implementation on simple forwarding devices, no transport blocking, low latency, and capabilities to support the existing 3GPP features, ease of extension and maintenance of the protocols to support 3GPP features, and backward compatibility across releases. Based on these criteria, it was decided to define a new 3GPP native protocol with type-length value-encoded messages over user datagram protocol (UDP)/IP, called packet-forwarding control protocol (PFCP), for Sxa, Sxb, and Sxc interfaces [3gpp]. The protocol stack for the control-plane/user-plane over Sxa, Sxb, Sxc, and combined Sxa/Sxb reference points are depicted in Fig. 1.13.

The PFCP is a new protocol layer, which has the following properties:

- One Sx association is established between a control-plane function and a user-plane function before being able to establish Sx sessions on the user-plane function. The Sx association may be established by the control-plane function or by the user-plane function.
- An Sx session is established in the user-plane function to provision rules instructing the user-plane function on how to process certain traffic. An Sx session may correspond to

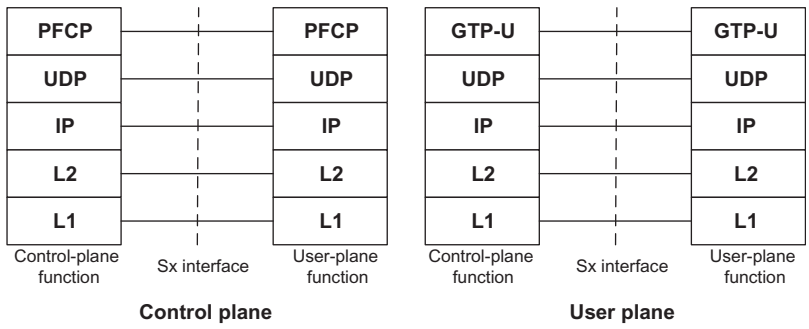


Figure 1.13
Control-plane/user-plane protocol stack over Sxa, Sxb, Sxc, and combined Sxa/Sxb [8].

an individual PDN connection, TDF session, or this can be a standalone session and not tied to any PDN connection/TDF session, for example, for forwarding DHCP/RADIUS/Diameter signaling between the PGW-C and PDN over SGi.

- Sx node–related procedures include Sx association setup/update/release procedures, monitoring peer PFCP, load and overload control procedures to balance loading across user-plane functions, and to reduce signaling toward user-plane function under overload conditions, Sx packet flow description (PFD) management procedure to provision PFDs for one or more application identifiers in the user-plane function.
- Sx session–related procedures include Sx session establishment/modification/deletion procedures; Sx session report procedure to report traffic usage or specific events.

Data forwarding between the control-plane function and user-plane function is supported by GTP-U encapsulation on the user plane and PFCP on the control plane where the latter protocol supports reliable delivery of messages. A set of new domain name system (DNS)[24] procedures are defined for user-plane function selection. The control-plane function selects a user-plane function based on DNS or local configuration, the capabilities of the user-plane function and the overload control information provided by the user-plane function. Figs 1.14 and 1.15 show two [example] deployment scenarios based on higher layer functional split between the central unit and the distributed unit (DU) of the base station reusing Rel-12 dual-connectivity concepts. The control-plane/user-plane separation permits flexibility for different operational scenarios such as moving the PDCP to a central unit while retaining the radio resource management (RRM) in a master cell; moving the RRM to a more central location where it has oversight over multiple cells, allowing independent scalability of user plane and control plane; and centralizing RRM with local breakout of data connections of some UEs closer to the base station site. During the establishment of an Sx session, the control plane function and the user-plane function select and communicate to each other the IP destination address at which they expect to receive subsequent request messages related to that Sx session. The control-plane function and the user-plane function may change this IP address subsequently during an Sx session modification procedure. Typically, Ethernet should be used as a layer-2 protocol, but the network operators may use any other technologies.

[24] Domain name system is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical Internet protocol addresses needed for locating and identifying computer hosts and devices with the underlying network protocols. The domain name system delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain. Network administrators may delegate authority over subdomains of their allocated name space to other name servers. This mechanism provides distributed and fault-tolerant service and was designed to avoid a single large central database. The domain name system also specifies the technical functionality of the database service that is at its core. It defines the domain name system protocol, a detailed specification of the data structures and data communication exchanges used in the domain name system, as part of the Internet protocol suite.

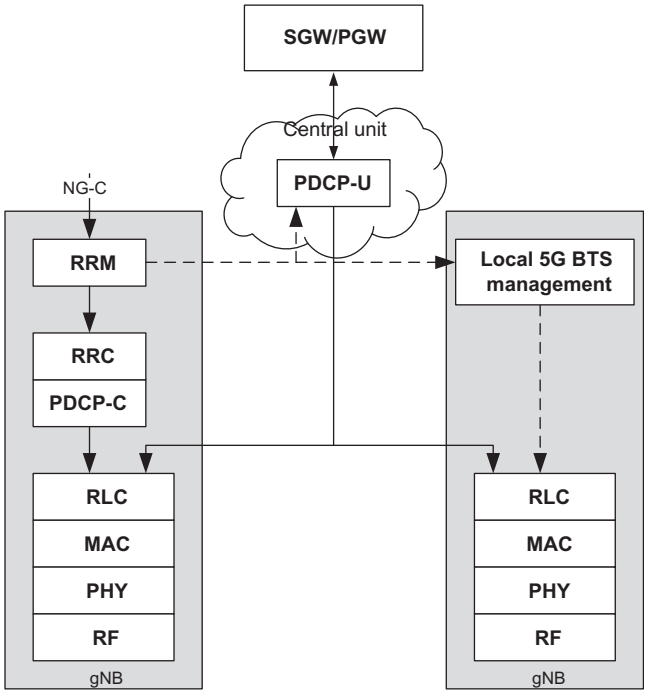


Figure 1.14
Centralized PDCP-U with local RRM [34].

1.1.4 Network Slicing

The combination of SDN and NFV enables dynamic, flexible deployment and on-demand scaling of NFs, which are necessary for the development of the 5G packet core network. Such characteristics have also encouraged the development of network slicing and service function chaining. From a UE perspective, slicing a network is to group devices with similar performance requirements (transmission rate, delay, throughput, etc.) into a slice. From network perspective, slicing a network is to divide an underlying physical network infrastructure into a set of logically isolated virtual networks. This concept is considered as an important feature of a 5G network, which is standardized by 3GPP. Service function chaining (SFC)[25] or network service chaining allows traffic flows to be routed through an ordered

[25] Network service chaining or service function chaining is a capability that uses software-defined networking capabilities to create a service chain of connected network services and connect them in a virtual chain. This capability can be used by network operators to set up suites or catalogs of connected services that enable the use of a single network connection for many services, with different characteristics. The primary advantage of network service chaining is the way virtual network connections can be set up to handle traffic flows for connected services. For example, a software-defined networking controller may use a chain of services and apply them to different traffic flows depending on the source, destination, or type of traffic.

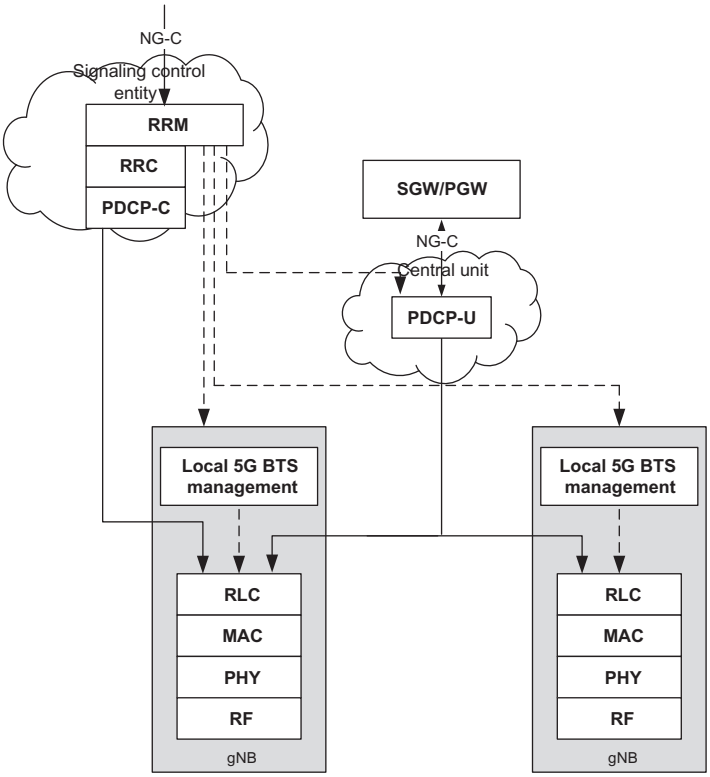


Figure 1.15
Centralized PDCP with centralized RRM in separate platforms [34].

list of NFs (e.g., firewall, load balancers, etc.). The best practical use case of SFC is to chain NFs (i.e., middle boxes in this case) placed in the interface between PGW and the external networks.

As depicted in Fig. 1.16, the network slicing architecture comprises three layers: (1) service instance layer, (2) network slice instance (NSI) layer, and (3) resource layer. The service instance layer represents the services (end-user or business services) which are supported by the network where each service is represented by a service instance. The services are typically provided by network operator or a third party. A service instance can either represent an operator service or a third-party service. A network operator uses a network slice blueprint[26] to create an NSI. An NSI provides the network characteristics which are required by

[26] Network slice blueprint is a complete description of the structure, configuration, and the plans/workflows for how to instantiate and control a network slice instance during its lifecycle. A network slice blueprint enables the instantiation of a network slice, which provides certain network characteristics (e.g., ultralow latency, ultrareliability, and value-added services for enterprises). A network slice blueprint refers to required physical and logical resources and/or to sub-network blueprint(s).

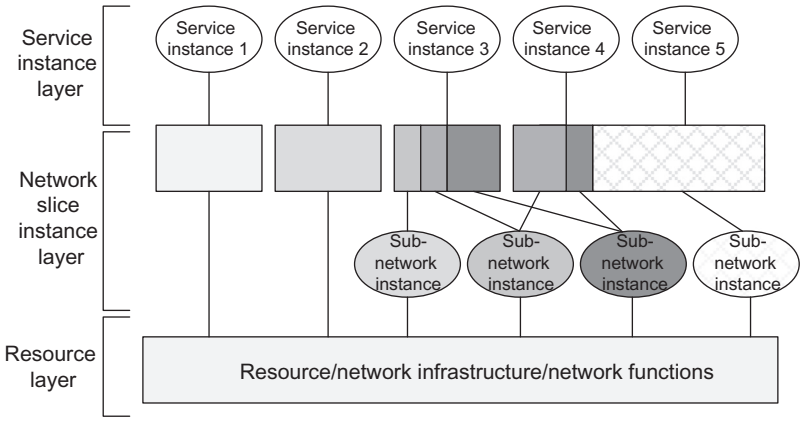


Figure 1.16
Network slicing conceptual architecture [6].

a service instance. An NSI may also be shared across multiple service instances provided by the network operator. The NSI may be composed of zero or more sub-network instances, which may be shared by another NSI. Similarly, the sub-network blueprint[27] is used to create a sub-network instance to form a set of NFs, which run on the physical/logical resources. The sub-network instance is a set of NFs, which run on the physical or logical resources. The network slice is a complete logical network providing telecommunications services and network capabilities. Network slices vary depending on the features of the service they need to support.

Fig. 1.17 shows an example of logical architecture of network slicing in a radio access network. In this example, different NSIs[28] can either share the same functions or have dedicated functions. The new RAT features flexible air interface design and a unified medium access control (MAC) scheduling to support different network slice types. Such a combination allows time-domain and frequency-domain resource isolation without compromising resource efficiency. The protocol stack can be tailored to meet the diverse service requirements from different NSIs. For instance, layer-3 RRC functions can be customized in network slice design phase. Layer-2 can have various configurations for different NSIs to meet specific requirements for radio bearers. In addition, layer-1 uses flexible numerology to support different

[27] Sub-network blueprint: a description of the structure (and contained components) and configuration of the sub-network instances and the plans/workflows for how to instantiate it. A sub-network blueprint refers to physical and logical resources and may refer to other sub-network blueprints.

[28] Network slice instance is the realization of network slicing concept. It is an end-to-end logical network, which comprises a group of network functions, resources, and connections. A network slice instance typically covers multiple technical domains, which includes terminal, access network, transport network, and core network, as well as dual-connectivity domain that hosts third-party applications from vertical industries. Different network slice instances may have different network functions and resources. They may also share some of the network functions and resources.

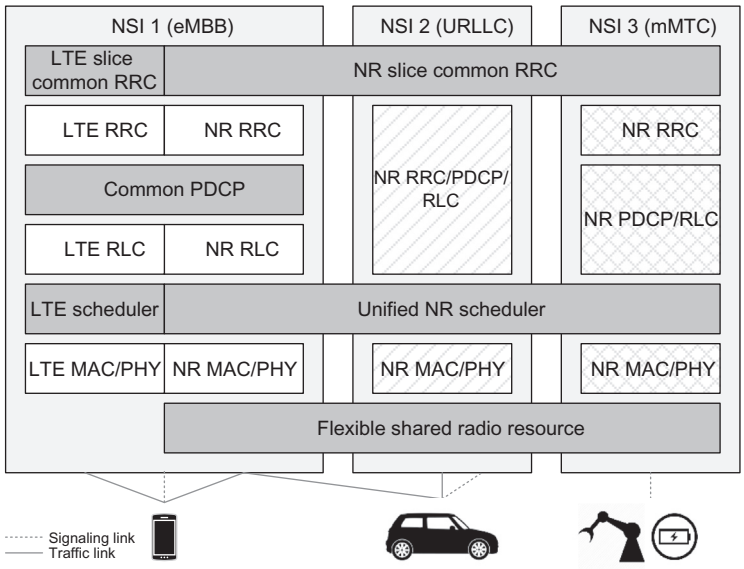


Figure 1.17
Example of RAN architecture with network slicing support [74].

network slice types. An NSI may contain different types of access nodes, such as 3GPP new RAT and a non-3GPP RAT. Consolidating fixed and wireless access in 5G is a desirable approach, which also requires further enhancements in the architecture design [74].

According to 3GPP specifications [3,16], a network slice always consists of an access and a core network part. The support of network slicing relies on the principle that traffic for different slices is handled by different PDU sessions. Network can create different network slices by scheduling and also by providing different L1/L2 configurations. The UE should be able to provide assistance information for network slice selection in an RRC message. While the network can potentially support a large number of slices, the UE does not need to support more than eight slices in parallel. As we mentioned earlier, network slicing is a concept that allows differentiated network services depending on each customer requirements. The mobile network operators can classify customers into different tenant types each having different service requirements that control in terms of what slice types each tenant is authorized to use based on service-level agreement and subscriptions.

Network slices may differ depending on the supported features and optimization of the network functions. An operator may opt to deploy multiple NSIs delivering exactly the same features but for different groups of UEs. A single UE can simultaneously be served by one or more NSIs via NG-RAN. A single UE may be served by a maximum of eight network slices at any time. The access and mobility management function (AMF) instance serving the UE logically belongs to each of the NSIs serving the UE, that is, this AMF instance is common

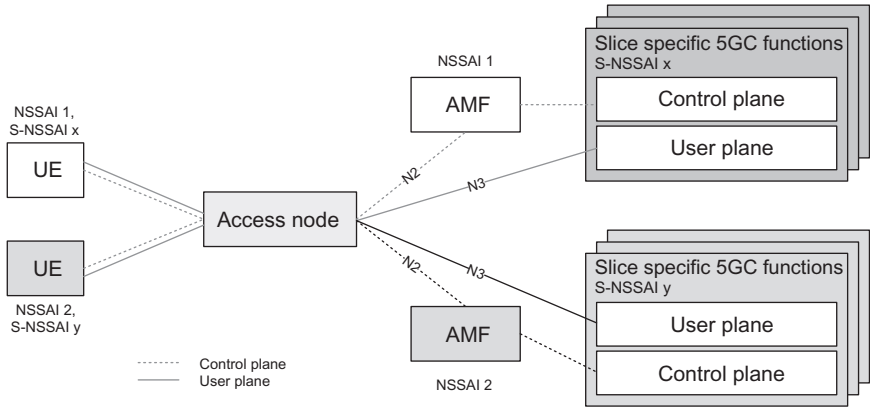


Figure 1.18
Slice selection and identifiers [55].

to the NSIs serving a UE. The selection of the set of NSIs for a UE is triggered by the first associated AMF during the registration procedure typically by interacting with the network slice selection function (NSSF), which may lead to change of AMF.

A network slice is identified by an identifier known as single-network slice selection assistance information (S-NSSAI). The S-NSSAI identity consists of a slice/service type (SST), which refers to the expected network slice behavior in terms of features and services and a slice differentiator (SD), which is an optional information element that complements the SST(s) to differentiate among multiple network slices of the same SST. The support of all standardized SST values by a public land mobile network (PLMN)[29] is not required. The S-NSSAI can have standard values or PLMN-specific values. The S-NSSAI identifiers with PLMN-specific values are associated with the PLMN ID of the PLMN that assigns them. An S-NSSAI cannot be used by the UE in AS procedures in any PLMN other than the one to which the S-NSSAI is associated. Standardized SST values provide a way for establishing global interoperability for slicing so that PLMNs can support the roaming use case more efficiently for the most commonly used SSTs. Currently, the SST values of 1, 2, and 3 are associated with eMBB, URLLC, and mMTC slice types [16]. The NSSAI is a collection of S-NSSAI. There can be at most eight S-NSSAIs in the NSSAI sent in signaling messages between the UE and the network. Each S-NSSAI assists the network in selecting a particular NSI. The same NSI may be selected via different S-NSSAIs. NSSAI includes one or more S-NSSAIs. Each network slice is uniquely identified by an S-NSSAI [3] (see Fig. 1.18).

[29] Public land mobile network is a mobile wireless network that is centrally operated and administrated by an organization and uses land-based RF transceivers or base stations as network hubs. This term is generally used to refer to an operator network.

NG-RAN supports differentiated handling of traffic for different network slices which have been preconfigured. The support of slice capabilities in terms of the NG-RAN functions (i.e., the set of NFs that comprise each slice) is implementation dependent. The NG-RAN supports the selection of the RAN part of the network slice by assistance information provided by the UE or the 5GC which unambiguously identifies one or more preconfigured network slices in the PLMN. The NG-RAN supports policy enforcement between slices according to service-level agreements. It is possible for a single NG-RAN node to support multiple slices. The NG-RAN can apply the best RRM policy depending on the service agreements for each supported slice. The NG-RAN further supports QoS differentiation within a slice. For initial attach, the UE may provide assistance information to support the selection of an AMF and the NG-RAN uses this information for routing the initial NAS to an AMF. If the NG-RAN is unable to select an AMF using this information or the UE does not provide such information, the NG-RAN sends the NAS signaling to a default AMF. For subsequent accesses, the UE provides a Temp ID, which is assigned to the UE by the 5GC, to enable the NG-RAN to route the NAS message to the appropriate AMF as long as the Temp ID is valid. Note that the NG-RAN is aware of and can reach the AMF which is associated with the Temp ID.

The NG-RAN supports resource isolation between slices via RRM policies and protection mechanisms that would avoid conditions such as shortage of shared resources in one slice resulting in under-service issues in another slice. It is possible to fully dedicate the NG-RAN resources to a certain slice. Some slices may be available only in certain parts of the network. Awareness in the NG-RAN of the slices supported in the cells of its neighbors may be beneficial for inter-frequency mobility in the connected mode. It is assumed that the slice configuration does not change within the UE's registration area. The NG-RAN and the 5GC can manage service requests for a slice that may or may not be available in a given area. Admission or rejection of access to a slice may depend on certain factors such as support for the slice, availability of resources, and support of the requested service by other slices. In the case where a UE is simultaneously associated with multiple slices, only one signaling connection is maintained. For intra-frequency cell reselection, the UE always tries to camp on the best cell, whereas for inter-frequency cell reselection, dedicated priorities can be used to control the frequency on which the UE camps. Slice awareness in NG-RAN is introduced at PDU session level by indicating the S-NSSAI corresponding to the PDU session in all signaling containing PDU session resource information. 5GC validates whether the UE is authorized to access a certain network slice. The NG-RAN is informed about all network slices for which resources are being requested during the initial context setup [3,15].

Resource isolation enables specialized customization of network slices and prevents adverse effects of one slice on other slices. Hardware/software resource isolation is up to implementation; nevertheless, RRM procedures and service agreements determine whether each slice

may be assigned to shared or dedicated radio resources. To enable differentiated handling of traffic for network slices with different service agreements, NG-RAN is configured with a set of different configurations for different network slices and receives relevant information, indicating which of the configurations applies to each specific network slice. The NG-RAN selects the AMF based on a Temp ID or assistance information provided by the UE. In the event that a Temp ID is not available, the NG-RAN uses the assistance information provided by the UE at RRC connection establishment to select the appropriate AMF instance (i.e., the information is provided after random access procedure). If such information is not available, the NG-RAN routes the UE to a default AMF instance [3,15].

Enabling network slicing in 5G requires native support from the overall system architecture. As shown in Fig. 1.16, the overall architecture consists of three fundamental layers: the infrastructure layer, network slice layer, and network management layer. The infrastructure layer provides the physical and virtualized resources, for instance, computing resource, storage resource, and connectivity. The network slice layer is located above the infrastructure layer and provides necessary NFs, tools and mechanisms to form end-to-end logical networks via NSIs. The network management layer contains the generic BSS/OSS and network slice management (NSM) system, which manages network slicing and ensures satisfaction of the SLA requirements. The overall architecture has the following key features:

- *Common infrastructure:* Network slicing is different than a dedicated network solution that uses physically isolated and static network resources to support tenants. Network slicing promotes the use of a common infrastructure among tenants operated by the same operator. It helps to achieve higher resource utilization efficiency and to reduce the service time to market. Moreover, such design is beneficial for long-term technology evolution as well as for maintaining a dynamic ecosystem.
- *On-demand customization:* Each technical domain in an NSI has different customization capabilities, which are coordinated through the NSM system during the process of network slice template (NST) design, NSI deployment, and operation and management. Each technical domain can perform an independent customization process in terms of design schemes to achieve an effective balance between the simplicity needed by commercial practice and architectural complexity.
- *Isolation:* The overall architecture supports the isolation of NSIs, including resource isolation, operation and management isolation, and security isolation. The NSIs can be either physically or logically isolated at different levels.
- *Guaranteed performance:* Network slicing seamlessly integrates different domains to satisfy industry-defined 5G performance specifications and to accommodate vertical industry requirements.
- *Scalability:* Owing to virtualization, which is one of the key enabling technologies for network slicing, resources occupied by an NSI can dynamically change.

- *Operation and management capability exposure:* Tenants may use dedicated, shared, or partially shared NSIs. Furthermore, different tenants may have independent operation and management demands. The NSM system provides access to a number of operation and management functions of NSIs for the tenants, which for instance allows them to configure NSI-related parameters such as policy.
- *Support for multi-vendor and multi-operator scenarios:* Network slicing allows a single operator to manage multiple technical domains, which may be composed of network elements supplied by different vendors. In addition, the architecture needs to support a scenario, where the services from the tenants may cover different administrative domains owned by different operators.

As we mentioned earlier, an NSI is a managed entity in the operator's network with a life cycle independent of the life cycle of the service instance(s). In particular, service instances are not necessarily active through the entire duration of the run-time phase of the supporting NSI. The NSI life cycle typically includes an instantiation, configuration and activation phase, a run-time phase, and a decommissioning phase. During the NSI life cycle the operator manages the NSI. As shown in Fig. 1.19, the network slice life cycle is described by a number of phases as follows [7]:

- *Preparation:* In this phase, the NSI does not exist. The preparation phase includes the creation and verification of NST(s), on-boarding, preparing the necessary network environment which is used to support the life cycle of NSIs, and any other preparations that are needed in the network.
- *Instantiation, configuration, and activation:* During instantiation/configuration, all shared/dedicated resources associated with the NSI have been created and configured and the NSI is ready for operation. The activation step includes any actions that make the NSI active such as routing traffic to it, provisioning databases (if dedicated to the network slice, otherwise this takes place in the preparation phase), and instantiation, configuration, and activation of other shared and/or non-shared NF(s).
- *Run-time:* In this phase, the NSI is capable of traffic handling and supports certain types of communication services. The run-time phase includes supervision/reporting, as well as activities related to modification. Modification of the workflows related to runtime tasks may include upgrade, reconfiguration, NSI scaling, changes of NSI capacity, changes of NSI topology, and association and disassociation of NFs with NSI.
- *Decommissioning:* This step includes deactivation by taking the NSI out of active state as well as the retrieval of dedicated resources (e.g., termination or reuse of NFs) and configuration of shared/dependent resources. Following this phase, the NSI does not exist anymore.

An NSI is complete in the sense that it includes all functionalities and resources necessary to support certain set of communication services. The NSI contains NFs belonging to the access and the core networks.

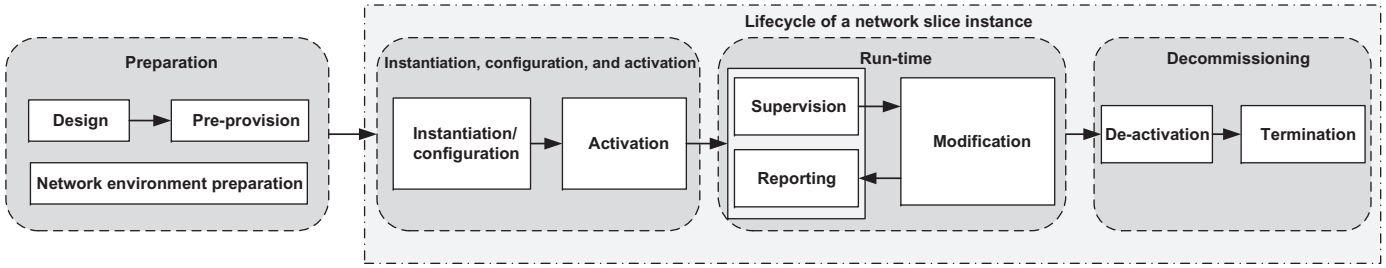


Figure 1.19
Life cycle phases of an NSI [7].

If the NFs are interconnected, the 3GPP management system contains the information relevant to connections between these NFs including the topology of connections, and individual link requirements such as QoS attributes. The NSI is realized via the required physical and logical resources. A network slice is described by an NST. The NSI is created using the NST and instance-specific information. The concept of network slice subnet instance management is introduced for the purpose of NSI management. For example, for instantiation of an NSI that contains radio access and core network components, these components can be defined and instantiated as two NSSIs denoted by NSSI1 (RAT1) in RAN and NSSI3 in the core network. The targeted NSI will be instantiated by combining the NSSI1 and NSSI3. Another NSI can be instantiated by combining NSSI3 with another RAN NSSI denoted by NSSI2 (RAT2).

Depending on the communication service requirements, a communication service can use an existing NSI or trigger the creation of a new NSI. The new NSI may be created exclusively for this communication service or it may be created to support multiple communication services with similar network slice requirements. The life cycle of a communication service is related but not dependent on an NSI. The NSI may exist before the communication service uses the NSI and may exist after the communication service stopped using the NSI. An NSI can be created using one or more existing NSSI(s) or initiate the creation of one or more new NSSI(s) depending on the NSI requirements. The new NSSI(s) may be created just for this NSI or it may be created to support multiple NSIs. The life cycle of an NSI is related but not dependent on that of an NSSI. The NSSI may exist before the NSI is created and may exist after the NSI is no longer needed.

1.1.5 Heterogeneous and Ultra-dense Networks

Effective network planning is essential to support the increasing number of mobile broadband data subscribers and bandwidth-intensive services competing for limited radio resources. Network operators have addressed this challenge by increasing the capacity through new spectrum, multi-antenna techniques, and implementing more efficient modulation and coding schemes. However, these measures are not adequate in highly populated areas and at the cell edges where performance can significantly degrade. In addition to the above remedies, the operators have integrated small cells into their macro-networks to efficiently distribute network loading, and to maintain performance and service quality while reusing spectrum more efficiently.

One solution to expanding an existing macro-network, while maintaining it as homogeneous, is to add more sectors per base station or deploying more macro-base stations. However, reducing the site-to-site distance in the macro-cell layout can only be pursued to a certain extent because finding new macro-sites becomes increasingly difficult and can be expensive, especially in dense urban areas. An alternative is to introduce small cells through addition of low-power

access nodes or RRH to the existing [overlaid] macro-cells due to their more economical site acquisition and equipment installation. Small cells are primarily added to increase capacity in hotspots with high user demand and to fill coverage holes in the macro-network in both outdoor and indoor environments. They also improve network performance and service quality by off-loading the overlaid macro-cells. The result is a heterogeneous network topology with large macro-cells in conjunction with small cells providing increased capacity per unit area. Heterogeneous network planning dates back to GSM era where cells were separated through the use of frequency reuse. While this approach could still be taken in LTE, LTE networks primarily use a frequency reuse of one to maximize utilization of the licensed bandwidth. In heterogeneous networks, the cells of different sizes are referred to as macro-cells, micro-cells, pico-cells, and femto-cells in the order of decreasing transmit power. The actual cell size depends not only on the access node power but also on physical antenna positions, as well as the topology of the cells and propagation conditions.

In general, the small cells in an ultra-dense network (UDN) are classified into full-functional base stations (pico-cells and femto-cells) and macro-extension access points (relays and RRHs). A full-functional base station is capable of performing all functions of a macro-cell with a lower power in a smaller coverage area and encompasses the full RAN protocol stack. On the other hand, a macro-extension access node is an extension of a macro-cell to effectively increase the signal coverage, and it performs all or some of the lower protocol layer functions. Moreover, the small cells feature different capabilities, transmission powers, coverage, and deployment scenarios. The UDN deployment scenarios introduce a different coverage environment where any given user would be in close proximity to many cells.

Small-cell architectures using low-power nodes were considered promising to mitigate the substantial increase in network traffic, especially for hotspot deployments in indoor and outdoor scenarios. A low-power node generally means a node whose transmit power is lower than the corresponding macro-node and base station classes, for example, pico-cell and femto-cell access nodes. Small-cell enhancements for LTE focused on additional functionalities for improved performance in hotspot areas for indoor and outdoor using low-power nodes. Network architectures comprising small cells (of various types including non-3GPP access nodes) and macro-cells can be considered as practical realization of the heterogeneous networks. Increasing the density of the 3GPP native or non-indigenous small cells overlaid by macro-cells constitutes what is considered as UDNs.

Small cells can be deployed sparsely or densely with or without overlaid macro-cell coverage as well as in outdoor or indoor environments using ideal or non-ideal backhaul. Small cells deployment scenarios include small-cell access nodes overlaid with one or more macro-cell layer(s)[30] in order to increase the capacity of an already deployed cellular

[30] Note: 3GPP uses the term layer in this context to refer to different radio frequencies or different component carriers.

Table 1.1: Backhaul options for the small cells [12].

Backhaul Type	Backhaul Technology	One-Way Latency (ms)	Throughput (Mbps)
Nonideal	Fiber access 1	10–30	10–10,000
	Fiber access 2	5–10	100–1000
	Fiber access 3	2–5	50–10,000
	DSL access	15–60	10–100
	Cable	25–35	10–100
	Wireless backhaul	5–35	10–100+
Ideal	Fiber access 4	<2.5 μs	Up to 10,000

network. In this context, two scenarios can be considered: (1) UE is simultaneously in coverage of both the macro-cell and the small cell(s); and (2) UE is not simultaneously covered by the macro-cell and small cell(s). The small-cell nodes may be deployed indoors or outdoors, and in either case could provide service to indoor or outdoor UEs, respectively. For an indoor UE, only low UE speeds of 0–3 km/h are considered. For outdoor UEs, in addition to low UE speeds, medium UE speeds up to 30 km/h were targeted. Throughput and mobility (seamless connectivity) were used as performance metrics for low- and medium-speed mobility scenarios. Cell-edge performance (e.g., fifth percentile of user throughput CDF) and network/UE power efficiency were also used as evaluation metrics.

Backhaul is a critical component of heterogeneous networks, especially when the number of small nodes increases. Ideal backhaul, characterized by very high throughput and very low latency link such as dedicated point-to-point connection using optical fiber; and non-ideal backhaul (e.g., xDSL,[31] microwave backhaul, and relaying) for small cells were studied by 3GPP, and performance and cost trade-offs were made. A categorization of ideal and non-ideal backhaul based on operators' data is listed in Table 1.1.

3GPP conducted extensive studies to investigate the interfaces between macro and small cell, as well as between small cells considering the amount and type of information/signaling needed to be exchanged between the nodes in order to achieve the desired performance improvements; and whether a direct interface should be used between macro and small cells or between small cells. In those studies, LTE X2 interface (i.e., inter-eNB interface) was used as a starting point. In small cell enhancements, both sparse and dense small cell deployments were considered. In some scenarios (e.g., indoor/outdoor hotspots), a single or multiple small-cell node(s) are sparsely deployed to cover the hotspot(s), whereas in other

[31] Digital subscriber line is a family of technologies that are used to transmit digital data over telephone lines. The asymmetric digital subscriber line is the most commonly used type of digital subscriber line technology for Internet access. The xDSL service can be delivered simultaneously with wired telephone service on the same telephone line since digital subscriber line uses high-frequency bands for data transmission. On the customer premises, a digital subscriber line filter on each non-digital subscriber line outlet blocks any high-frequency interference to enable simultaneous use of the voice and digital subscriber line services.

scenarios (e.g., dense urban, large shopping mall, etc.), a large number of small-cell nodes are densely deployed to support high-volume traffic over a relatively wide area covered by the small-cell nodes. The coverage of the small-cell layer is generally discontinuous between different hotspot areas. Each hotspot area is typically covered by a group of small cells or a small cell cluster. Furthermore, future extension or scalability of these architectures is an important consideration. For mobility or connectivity performance, both sparse and dense deployments were studied with equal priority.

Network synchronization is an important consideration where both synchronized and unsynchronized scenarios should be considered between small cells as well as between small cells and macro-cell(s). For specific operational features such as interference coordination, carrier aggregation, and coordinated multipoint (CoMP) transmission/reception, small-cell enhancements can benefit from synchronized deployments with respect to small-cell search/measurements and interference/resource management procedures. Small-cell enhancements tried to address deployment scenarios in which different frequency bands are separately assigned to macro-layer and small-cell layer. Small-cell enhancements are applicable to the existing cellular bands and those that might be allocated in the future with special focus on higher frequency bands, for example, the 3.5 GHz band, to take advantage of more available spectrum and wider bandwidths. Small-cell enhancements have considered the possibility of frequency bands that, at least locally, are only used for small cell deployments. The studies further considered cochannel deployment scenarios between macro-layer and small-cell layer. Some example spectrum configurations may include the use of carrier aggregation in the macro-layer with bands X and Y and the use of only band X in the small-cell layer. Other example scenarios may include small cells supporting carrier aggregation bands that are cochannel with the macro-layer; or small cells supporting carrier aggregation bands that are not cochannel with the macro-layer. One potential cochannel scenario may include deployment of dense outdoor cochannel small cells, including low-mobility UEs and non-ideal backhaul. All small cells operate under a macro-cell coverage irrespective of duplex schemes [frequency division duplex/time division duplex (FDD/TDD)] that are used for macro-layer and small-cell layer. Air interface and solutions for small cell enhancement are band-independent [12]. In a small cell deployment, it is likely that the traffic volume and the user distribution are dynamically varying between the small-cell nodes. It is also possible that the traffic is highly asymmetrical and it is either downlink or uplink centric. Both uniform and nonuniform traffic and load distribution in time-domain and spatial-domain are possible. During performance modeling, both non-full-buffer and full-buffer traffic were considered, where non-full buffer traffic was prioritized as it was deemed to be more practical representation of user activity.

Small-cell enhancements target high network energy efficiency and a reasonable system complexity. The small cells can save energy by switching to a dormant mode due to increased likelihood of periods of low or no user activity during operation. The trade-off

between user throughput/capacity per unit area and network energy efficiency is an important consideration for small cell deployments. The small cells can further achieve UE energy efficiency considering the small cell's short-range transmission path, resulting in reduced energy/bit for the uplink transmission, mobility measurements, cell identification, and small cell discovery.

Given that some of the heterogeneous network deployments include user-installed access nodes in indoor environments, a self-organizing mechanism for deployment and operation of the small cell without direct operator intervention is required. 3GPP self-organizing networks (SON) solutions aim to configure and optimize the network automatically, so that the intervention of human can be reduced and the capacity of the network can be increased. These solutions can be divided into three categories [85]:

- *Self-configuration:* This is the dynamic plug-and-play configuration of newly deployed access node. As shown in Fig. 1.20, the access node configures its physical cell identity (PCI), transmission frequency, and power, leading to faster cell planning and rollout.

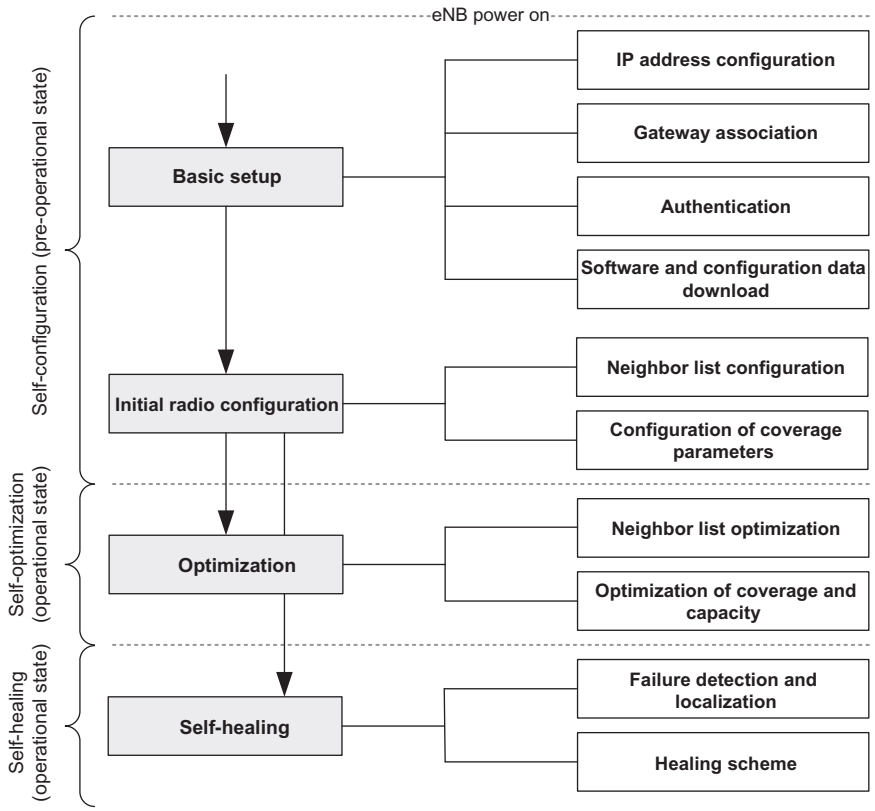


Figure 1.20
SON framework [85].

The network interfaces (e.g., S1 and X2 in the case of LTE) are dynamically configured, and the IP address as well as connection to IP backhaul is established. To reduce manual operation, the automatic neighbor relation (ANR) scheme is used. The ANR configures the neighbor list in newly deployed access nodes and optimizes the list over the course of operation. Dynamic configuration includes the configuration of the physical layer identifier, PCI, and cell global ID (CGID). The PCI mapping attempts to avoid assignment of duplicate identifiers to the access nodes in order to prevent collision. The PCI can be assigned in a centralized or distributed manner. When centralized assignment is used, the operation and management system will have a complete knowledge and control of the PCIs. When the distributed solution is used, the operation and management system assigns a list of possible PCIs to the newly deployed access nodes, but the adoption of the PCI is in control of the eNB. The newly deployed eNB will request a report, sent either by UEs over the air interface or by other eNBs over the X2 interface, including already in-use PCIs. The eNB will randomly select its PCI from the remaining values. The ANR is used to minimize the work required for configuration in newly deployed eNBs as well as to optimize configuration during operation. Correct and up-to-date neighbor lists will increase the number of successful handovers and minimize the number of dropped calls. Before a handover can be executed, the source eNB requires the neighbor information such as PCI and CGID of the target eNB. The PCI is included in normal measurement reports. The mapping between the PCI and CGID parameters can be done by using information from the operation and management or that reported by UEs decoding the target cell CGID on the broadcast channel in the target cell. The capability of decoding CGID is an optional UE feature. A network operator can put a cell on an ANR black list, to block certain handover candidates, for example, from indoor to outdoor cells. 3GPP has also specified LTE inter-frequency and inter-RAT ANR.

- *Self-optimization:* The self-optimization functions were mainly specified in 3GPP Rel-9, which included optimization of coverage, capacity, handover, and interference. Mobility load balancing is a feature where cells experiencing congestion can transfer excess load to other cells which have available resources. Mobility load balancing further allows the eNBs to exchange information about the load level and the available capacity. The report can contain computational load, S1 transport network load, and radio resource availability status. There are separate radio resource status reports for the uplink and downlink, which may include the total allocated resources, guaranteed bit rate (GBR) and non-guaranteed bit rate traffic statistics, the percentage of allocated physical resources relative to total resources, and the percentage of resources available for load balancing. Mobility load balancing can also be used across different radio access technologies. In case of inter-RAT, the load reporting RAN information management protocol will be used to transfer the information via the core network between the base stations of different radio technologies. A cell capacity class value,

set by the operation and management system, is used to relatively compare the capacities of different radio access technologies. A handover due to load balancing is performed as a regular handover; however, it may be necessary to set the parameters such that the UE cannot return to the [congested] source cell. Mobility robustness optimization is a solution for automatic detection and correction of errors in the mobility configuration which may cause radio link failure as a result of unsuccessful handover.

- *Self-healing:* Features for automatic detection and removal of failures and automatic adjustment of parameters were mainly specified in 3GPP Rel-10. Coverage and capacity optimization enables automatic correction of capacity problems due to variations of the environment. The minimization of drive tests was a feature that enables normal UEs to provide the same type of information as those collected during the drive tests with the advantage that UEs can further retrieve and report parameters from indoor environments.

The home eNB (HeNB) concept was introduced in LTE Rel-9, which defines a low-power node primarily used to enhance indoor coverage. Home eNBs and particularly femtocells are privately owned and deployed without coordination with the macro-network; as such, if their operating frequency is the same as the frequency used in the macro-cells and access to them is limited, then there is a risk of interference between the femtocell and the surrounding network. The use of different cell sizes with overlapping coverage and creation of a heterogeneous network adds to the complexity of network planning. In a network with a frequency reuse of one, the UE normally camps on the cell with the strongest received signal power, hence the cell edge is located at a point where the received signal strengths are the same in both cells. In homogeneous network deployments, this also typically coincides with the point of equal path loss of the uplink in both cells, whereas in a heterogeneous network, with high-power nodes in the large cells and low-power nodes in the small cells, the point of equal received signal strengths is not necessarily the same as that of equal uplink path loss. Therefore, a challenge in heterogeneous network planning is to ensure that the small cells actually serve certain number of users. This can be done by increasing the area served by the small cell through the use of a positive cell selection offset which is referred to as cell range extension (Fig. 1.21). A drawback of this scheme is the increased interference in the downlink experienced by the UE located in the extended cell region and served by the base station in the small cell. This effect may impact the quality of reception of the downlink control channels. It is important to highlight that indoor small cells (femtocells) operate in three different access modes: open, closed, and hybrid. In open access mode, all subscribers of a given operator can access the node, while in closed access mode, the access is restricted to a closed subscriber group. In hybrid mode, all subscribers can connect to the femtocell with the priority always given to the designated subscribers. A network comprising small cells and

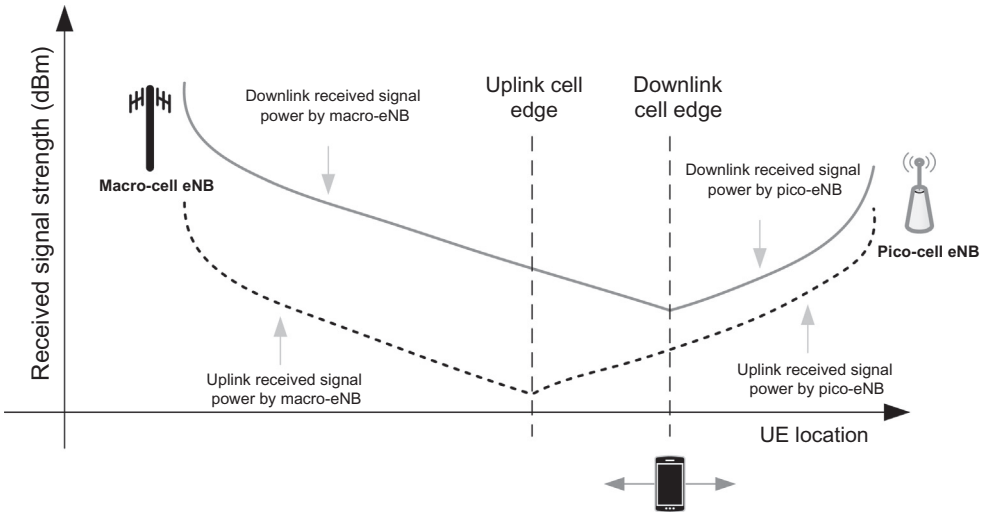


Figure 1.21
Uplink/downlink imbalance issue in HetNet deployments [12].

macro-cells is referred to as HetNet in the literature. HetNets, in general, are considered as a paradigm shift from the classic homogeneous networks.

A number of features were added to the later releases of LTE that can be used to mitigate the inter-cell interference issue in the heterogeneous networks. Inter-cell interference cancelation (ICIC) was introduced in LTE Rel-8, in which the eNBs can coordinate over the X2 interface in order to mitigate inter-cell interference for UEs at the cell edge. Frequency-domain ICIC scheme evolved to enhanced ICIC (eICIC) in LTE Rel-10 where the time-domain ICIC was added through the use of almost blank subframes. Those subframes included only LTE control channels and cell-specific reference signals and no user data, transmitted with reduced power. In that case, the macro-eNB would transmit the almost blank subframes according to a semistatic pattern and the UEs in the extended range of the small cells could better receive downlink control and data channels from the small cell. Further enhancement of ICIC focused on interference handling by the UE through ICIC for control signals, enabling even further cell range extension.

Carrier aggregation (CA) was introduced in LTE Rel-10 to increase the total system bandwidth and the maximum user throughputs. In this scheme, the component carriers (CCs) are aggregated and any CA-capable UE can be allocated resources on all or some component carrier combinations. Cross-carrier scheduling is an important feature in heterogeneous networks supporting CA where the downlink control channels are mapped to different component carriers in the large and small cells (as shown in Fig. 1.22). As an example, when LTE downlink control channel which carries downlink control information along with scheduling

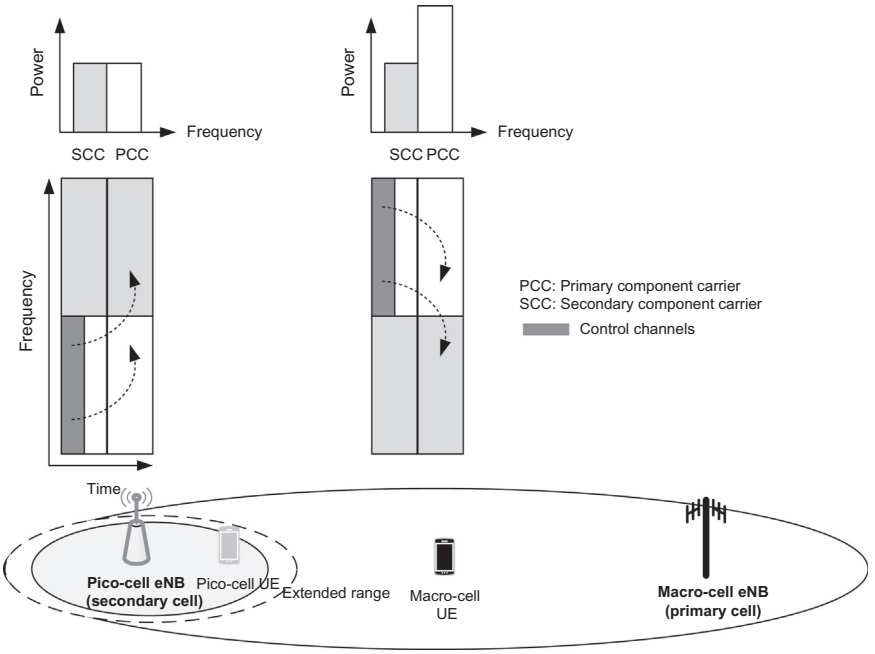


Figure 1.22
Illustration of cross-carrier scheduling and multi-cell operation in LTE [69].

information must be received by the UEs at the cell edge, it may be transmitted with a higher power than the traffic channels. Therefore, using different carriers for the downlink control channels in the large and small cells reduces the risk of inter-cell interference. The latest releases of LTE allow multi-carrier operation with different timing advances, enabling combination of component carriers from macro-eNBs with those of small cells.

The CoMP transmission and reception feature, introduced in LTE Rel-11, is an inter-cell and inter-user interference mitigation scheme that allows coordinated eNBs, relay nodes, or RRHs to simultaneously transmit to or receive from a UE. When CoMP is used in a heterogeneous network, a number of macro-cells and small cells can participate in data transmission to and from a UE. However, this would require that the macro-eNBs and the small cells to be synchronized and coordinated via backhaul links and the content be available almost at the same time at multiple transmission points, which is practically challenging. In the next section, we will see how cloud-RANs with distributed RRHs have made multi-point transmission/reception and data processing practically feasible. In CoMP scheme, a dynamic muting mechanism can be exploited to mute some (radio) resources at certain small cells for the benefit of other small cells. In this manner, the inter-cell coordination function which generates the muting patterns considers an appropriate metric for individual users and a proportional fairness scheduling among all users. The muting technique not

only takes into account the first dominant interferer but also the second dominant interference source for optimal interference mitigation.

Owing to the network traffic load fluctuation, switching off the base stations/access nodes in the cells with low or no traffic load is an essential method for UDNs to improve energy efficiency and to reduce inter-cell interference. In practice, the network load fluctuates over different times and locations due to diversity of user behavior and mobility, which is especially true for UDNs that warrants switching off under-utilized base stations. In a sparse network using frequency reuse of one with idle base stations where access node density is less than user density, the average spectral efficiency can still increase linearly with access node density as in the network without idle mode base stations. In a frequency reuse of one UDN with idle mode base stations where access node density is larger than user density, the spectral efficiency only increases logarithmically with access node density [68].

Optimal utilization of large amount of radio resources in a UDN can become increasingly complex. Improper allocation of abounded radio resources in a UDN can lead to higher inter-cell interference, unbalanced load distributions, and higher power consumption. Furthermore, due to inter-cell interference, local radio resource allocation strategies may have a global impact on a UDN operation. In other words, a localized allocation strategy may not work in a UDN environment, which necessitates the use of a centralized RRM that has a holistic view of the UDN, allowing tight interworking across the network. Providing sufficient bandwidth over direct-wired backhaul to each access node in a UDN may not be practical. As a result, in the last decade several schemes have been devised and studied in the literature such as wireless self-backhauling, which consumes valuable radio resources and may cause additional interference and latency. Recall that a UDN is a densified HetNet. The user association in HetNets follows a load-based association rule, where the users are biased to connect to the nearest small cell to offload their traffic. The small cells are usually lightly loaded due to the limited coverage area; hence, the association of a given user to the nearest small cell gives the user a higher data rate privilege. The biasing of users to small cells is performed via virtual extension of their coverage area. Interference management is a challenging task in densified networks. Various types of small cells are deployed with large densities to provide the users with very high throughput connections. The use of inter-cell coordination to mitigate the interference requires increasing signaling overhead due to the large number of deployed small cells. Thus, distributed control is preferred to mitigate the interference in a UDN.

A UDN can be defined as a network where there are more cells than active users. In mathematical terms, $\rho_{BS} \gg \rho_{user}$, where ρ_{BS} denotes the area density of access nodes and ρ_{user} denotes the area density of users. Another definition of UDN can be solely given in terms of the access node density irrespective of the user density. The access nodes in UDN environments are typically low-power small cells with a small footprint, resulting in a small coverage area. Accordingly, the inter-site distance would be in the range of meters or tens of meters. Strong interference between neighboring cells is a limiting factor in UDN. The

proximity of the small cells to each other in a UDN environment causes strong interference, thus the use of effective interference management schemes is inevitable to mitigate the interference of neighboring cells. Densification of wireless networks can be realized either by deploying an increasing number of access nodes or by increasing the number of links per unit area. In the first approach, the densification of access nodes can be realized in a distributed manner through deployment of small cells (e.g., pico-cells or femto-cells) or via a centralized scheme using distributed antenna system (DAS)[32] in the form of C-RAN architecture. In small-cell networks, femtocells are typically installed by the subscribers to improve the coverage and capacity in residential areas, and the pico-cells are installed by the operators in hotspots. Thus, in small-cell networks the coordination mechanism is often distributed. Compared to relays, DAS transmits the user signals to the base station via fiber links, while the relays use the wireless spectrum either in the form of in-band or out-of-band.

1.1.6 Cloud-RAN and Virtual-RAN

Operators in quest of more efficient ways to accommodate the increasing use of smartphones and other heavy data-consuming wireless devices in their networks face a dilemma when it comes to expanding network capacity and coverage. Optical fiber is typically the first option which is considered when addressing the problem of exponential traffic growth in the network. However, optical fiber is expensive; it takes a long time to install; and in some locations, it cannot be installed. To improve the network capacity and coverage, operators have several options among them small cells, carrier Wi-Fi,[33] and DASs. These and a host of other solutions are being used by network operators as methods of expanding their network to accommodate the exponential user traffic and new applications.

[32] A distributed antenna system is a network of spatially separated antennas which are connected to a common source via a transport mechanism that provides wireless service within a geographic area or structure. Distributed antenna system improves mobile broadband coverage and reliability in areas with heavy traffic and enhances network capacity, alleviating pressure on wireless networks when a large group of people in close proximity are actively using their terminals. Distributed antenna system is an approach to extending outdoor base station signals in indoor environments. It is a network of geographically separated antennas which receive input from a common base station source. Distributed antenna system uses multiple smaller antennas to cover the same area (that otherwise the macro base station would cover) and provides deeper penetration and coverage inside buildings. The RF input to the antennas can be conveyed either by lossy coaxial cables or more expensive optical fiber links. Some in-building distributed antenna systems can support multiple operators and standards at various levels, but advanced equipment is needed to meet a wider range of frequency bands and power outputs. Unwanted signal by-products and interference are serious issues in a shared distributed antenna system environment.

[33] Carrier Wi-Fi provides improved, scalable, robust unlicensed spectrum coverage and is often deployed as a stand-alone solution. It is an easy data offload from the cellular networks with access and policy control capable of supporting large numbers of users. Wi-Fi with new standards, such as Hotspot 2.0, can provide high data rates for users who are continuously streaming content on mobile devices.

In conjunction with the question of network expansion, there are other business imperatives. Mobile data transport architectures must be evaluated based on characteristics such as fastness, time to market, cost-effectiveness, operational and architectural simplicity, expandability, and flexibility. Energy consumption and physical size are also key factors in the deployment of new network architectures considering power and space are expensive and scarce resources at base station sites and central offices (COs).

A centralized-RAN, or C-RAN architecture addresses capacity and coverage issues, while supporting mobile fronthaul and/or backhaul solutions as well as network self-organization, self-optimization, configuration, and adaptation with software control and management through SDN and NFV. Cloud-RAN also provides advantages in controlling ongoing operational costs, improving network security, network controllability, network agility, and flexibility. The application of the C-RAN concept to small-cell architectures provides capacity benefits beyond those achieved through cell virtualization. In a traditional small-cell architecture, each access point provides a fixed amount of capacity within its coverage area. This might work well only if the user traffic is evenly distributed across the coverage area, a condition that is rarely happens in real life. The result is that some access points will be overloaded and others are relatively idle across time. Unlike stand-alone small cells where the addition of the new cells further aggravates the inter-cell interference, C-RAN architectures can be expanded and scaled.

1.1.6.1 Architectural Aspects

Cloud-based processing techniques can be implemented to centralize the baseband processing of multiple small cells and to improve inter-cell mobility and interference management. Small cells can support a variety of applications and services including voice-over-IP and videoconferencing, which can greatly benefit from a centralized architecture. C-RAN architecture comprises distributed RRHs commonly connected to centralized BBUs using optical transport or Ethernet links. The RRHs typically include the radio, the associated RF amplifiers/filters/mixers, and the antenna. The centralized BBU is implemented separately and performs the signal processing functionalities of the RAN protocols. The centralized BBU model enables faster service delivery, cost savings, and improved coordination of radio capabilities across a set of RRHs. Fig. 1.23 shows the migration from distributed RAN architecture to the centralized model. In a V-RAN architecture, the BBU functionalities and services are virtualized in the form of VMs running on general-purpose processor platforms that are located in a centralized BBU pool in the CO that can effectively manage on-demand resource allocation, mobility, and interference control for a large number of interfaces [toward remote radio units (RRUs)] using programmable software layers. The V-RAN architecture benefits from software-defined capacity and scaling limits. It enables selective content caching, which helps to further reduce network deployment and maintenance costs as well as to improve user experience based on its cloud infrastructure.

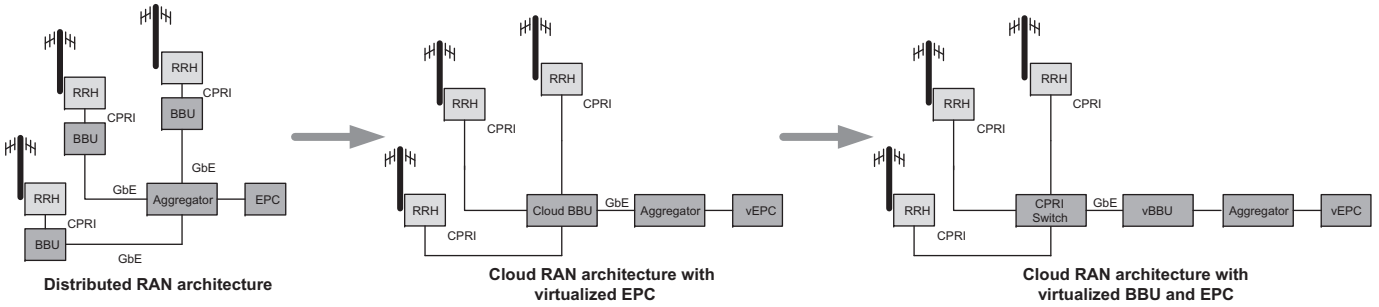


Figure 1.23
Base station architecture evolution and high-level C-RAN architecture [61].

In a traditional cellular network architecture, each physical base station unit encompasses both baseband and radio processing functions. In C-RAN, the baseband processing for a large number of cells is centralized, resulting in improved performance due to the ability to coordinate among multiple cells, and cost reduction as a result of pooling the shared resources. Small cells, when densely deployed across a large indoor environment, create large areas of overlap between neighboring cells. Inter-cell interference occurs at the cell boundaries. Some enterprise small cells use a central service controller to assist in handovers and backhaul aggregation, but it cannot overcome the fact that each cell interferes with its neighbors since some level of interference is inevitable. Creating multiple independent cells further necessitates frequent handovers for mobile terminals, degrading the user experience and creating the potential for handover failures or constant back-and-forth handovers between adjacent cells, a phenomenon known as ping-pong effect. Cell virtualization enables allocation of users' data over the same radio resources but sent to different access nodes for transmission to different users.

In general, a C-RAN architecture consists of three main entities: BBU(s), RRH/units, and the transport network or what is called the fronthaul, as shown in Fig. 1.23. In order to reduce the power consumption across network and to reduce inter-cell interference, the C-RAN architecture allows shutting off idle RRHs. This flexibility provides network adaptation based on traffic profiles that vary temporally and/or geographically that further reduces the interference to neighboring cells in order to optimize overall system performance. From a hardware usage perspective, scheduling baseband resources on-demand to perform communication process for multiple RATs while taking advantage of network virtualization techniques can improve operational efficiency and reduce energy consumption. CoMP, dual connectivity, virtual multiple input and multiple output (MIMO), and coordinated beamforming are effective standard approaches to improve network capacity specified by 3GPP [47]. To support CoMP schemes with joint transmission/processing, the network configures the UEs to measure channel-state information and to periodically report the measurements to a set of collaborating nodes, which results in a large amount of signaling overhead. The logical interface between various RATs in a centralized BBU model would enable signaling exchange among participating nodes and node selection for collaborative transmission and reception.

Since most of the current and the future deployment scenarios are in the form of ultradense heterogeneous networks, multi-RAT coexistence will be a key issue. 3GPP LTE was designed to support inter-RAT handover for GSM, UMTS, and interworking with wireless local area network. As shown in Fig. 1.24, the architecture for interworking between LTE and different RATs requires connection of their core networks for higher layer signaling. This multi-RAT architecture might be feasible but the latency of an inter-RAT handover may be prohibitive for many applications and services. In order to improve the user experience, simplified network architectures have been studied for lower latency based on C-RAN concept. If the BBU

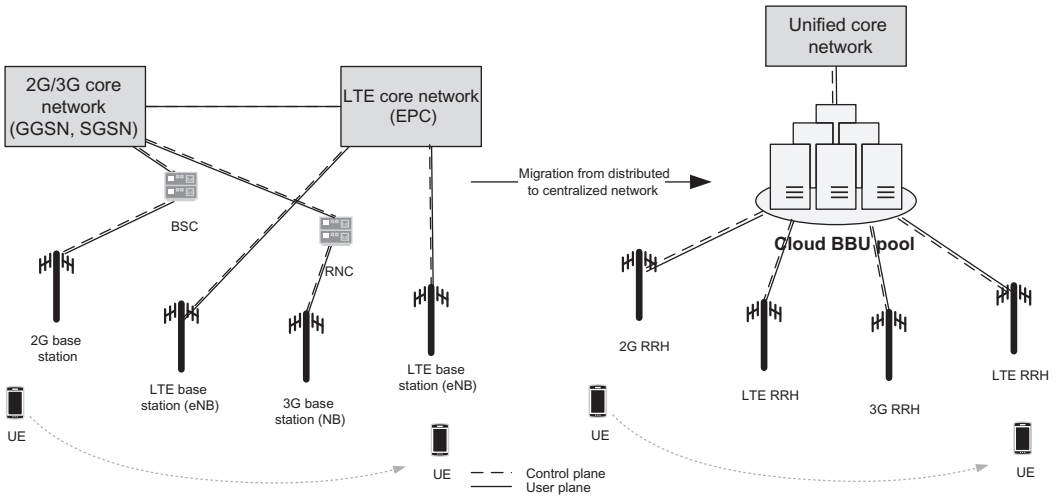


Figure 1.24
Mobility management in multi-RAT scenarios in distributed and centralized RAN architectures [61].

pool, shown in Fig. 1.24, integrates the essential 2G, 3G, and LTE [and later 5G NR (new radio)] network protocols, the inter-RAT handover process can be simplified and the distance between traffic anchor and interface can be reduced, which ultimately reduces the handover interruption time for network services. The inter-RAT handover differs from intra-RAT handover, which is a procedure to select a cell with the strongest received signal. The objective of inter-RAT handover is to select a suitable cell, considering user needs (especially mobility prediction), traffic type, and network property and state, by switching the logical interface between different RATs, which is more manageable in a C-RAN architecture.

Based on the distributed base station architectural model for the C-RAN, all or some of the baseband functions are performed in the centralized unit (CU). The processing resources on the CU can be dynamically managed and allocated. The C-RAN architecture allows improvement of resource utilization rate and energy efficiency as well as support of collaborative techniques. The concept of C-RAN has been evolving in the past decade and numerous architectural and deployment schemes for improving the spectral efficiency, latency, and support of advanced interference mitigation techniques have been studied and trialed by the leading operators. As an example, demarcation of the BBU into a CU and DU(s), functional split, and the next-generation fronthaul interface (NGFI) were introduced under the C-RAN context to meet the 5G requirements. The principle of CU/DU functional split originated from the real-time processing requirements of different applications. As shown in Fig. 1.25, a CU typically hosts non-real-time RAN protocols and functions offloaded from the core network as well as MEC services. Accordingly, a DU is primarily responsible for physical layer processing and real-time processing of layer-2 functions. In order to relax the

transport requirements on the fronthaul link between the DU and the RRUs, some physical layer functions can be relocated from the DU to the RRU(s). From the equipment point of view, the CU equipment can be developed based on a general-purpose platform, which supports RAN functions, functions offloaded from core network, and the MEC services, whereas the DU equipment must be (typically) developed using customized platforms, which can support intensive real-time computations. Network function virtualization infrastructure allows system resources, including those in the CU and the DU, to be flexibly orchestrated via MANO, SDN controller, and traditional network operation and maintenance center, supporting fast service rollout. In order to address the transport challenges between CU, DU, and RRU(s), the NGFI standard has been developed where an NGFI switch network is used to connect the C-RAN entities. Using the NGFI standard, the C-RAN entities can be flexibly configured and deployed in various scenarios. In case of ideal fronthaul, the deployment of DU can also be centralized, which could subsequently support cooperative physical layers. In case of non-ideal fronthaul, the DU can be deployed in a fully or partially distributed manner. Therefore C-RAN architecture in conjunction with the NGFI

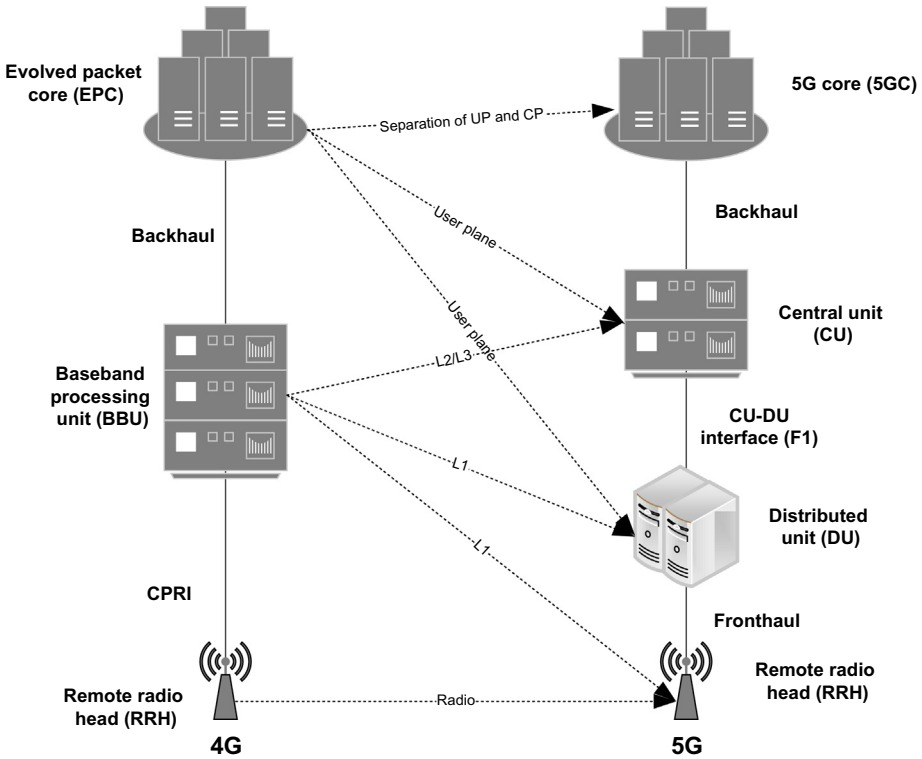


Figure 1.25
BBU architecture and evolution to 5G [47].

standard can support CU and DU deployments [47]. Latency, cost, and distance should be carefully evaluated in determining the proper mode of transport. Some of the available options include dedicated fiber, optical transport network (OTN),[34] passive optical network (PON),[35] microwave, and wavelength-division multiplexing (WDM) schemes. Mobile operators can further leverage low-cost, high-capacity fronthaul solutions using microwave E-band transport as an advanced application of C-RAN architecture. E-band radios are point-to-point, line-of-sight (LoS) microwave radios operating at 71−86 GHz.

1.1.6.2 Fronthaul Transport and Functional Split Options

In a C-RAN architecture, the baseband signal processing is centralized and often moved from individual RRUs to the edge cloud, resulting in a simplified network architecture, smaller form-factor radio units, efficient sharing and use of network resources, reduced costs of equipment installation and site maintenance, and higher spectral efficiency gains from joint processing schemes such as CoMP transmission/reception. However, it is necessary to overcome the constraints of fronthaul network transporting the raw in-phase and quadrature (I/Q) digital radio samples from the radio units to the edge cloud for processing. The fronthaul network is traditionally implemented based on the CPRI standard, which currently supports data rates of up to 24 Gbps per cell, a total fronthaul latency up to 200 μs, low jitter, tight synchronization, and high reliability. These requirements can only be realized with high-capacity fiber or point-to-point wireless links, making the deployment of the fronthaul network very costly, reducing the gains expected from centralization. The most promising approach to reduce the traffic load of the fronthaul interface is through the functional split between the edge cloud BBU and the RRU(s). By adopting only partial radio protocol split, the fronthaul requirements can be significantly relaxed while retaining the main centralization benefits. These functional splits blur the difference between classical fronthaul and backhaul networks, calling for converged transport networks that unify

[34] An optical transport network consists of a set of optical network elements connected by optical fiber links and is able to provide functionality of transport, multiplexing, routing, management, supervision, and survivability of optical channels carrying user signals, according to the requirements given in ITU-T Recommendation G.872. A distinguishing characteristic of the optical transport network is its provision of transport for any digital signal independent of client-specific aspects, that is, client independence. As such, according to the general functional modeling described in ITU-T Recommendation G.805, the optical transport network boundary is placed across the optical channel/client adaptation, in a way to include the server specific processes and leaving out the client-specific processes.

[35] A passive optical network is a communication technology which is used to provide fiber links to the end users. One of the passive optical network's distinguishing features is that it implements a point-to-multipoint architecture where passive fiber-optic splitters are used to enable a single optical fiber to serve multiple endpoints. A passive optical network does not have to provision individual fibers between the hub and customer.

backhaul and fronthaul equipment (i.e., integrated access and backhaul[36]), hence reducing deployment and operational costs. The deployment of these networks can be facilitated by the introduction of NGFI.

Centralizing baseband processing simplifies network management and enables resource pooling and coordination of radio resources. The fronthaul represents the transport network connecting the central site to cell sites when some or the entire baseband functions are hosted in a central site. Point-to-point dark fiber would be the ideal transport medium for fronthaul because of its high bandwidth, low jitter, and low latency. However, dark fiber is not widely available, thus there has been a need to relax the fronthaul requirements in order to enable the use of widely available transport networks such as packet-based Ethernet or E-band microwave. With such transport networks, bandwidth may be limited, jitter may be higher, and latencies may be on the order of several milliseconds. Cloud-RAN architecture is able to support different functional splits. Centralizing only a portion of the baseband functions and leaving the remaining functions at the remote sites would be a way to relax the fronthaul requirements. Depending on which functions are centralized, we will have different bandwidth, latency, and jitter requirements.

In a C-RAN architecture, the RRHs are connected to the BBU pool through high-bandwidth transport links known as fronthaul. There are a few standard interface options between the RRH and BBU including CPRI, radio-over-Ethernet (RoE), and Ethernet. However, CPRI and its most recent version, eCPRI, are currently the most common technologies used by C-RAN equipment vendors. The fronthaul link is responsible for carrying the radio signals, typically over an OTN, using either digitized form based on protocols such as the CPRI, or in analog form through radio-over-fiber technology. The main advantage of digitized transmission is the reduced signal degradation, allowing data transmission over longer distances, offering higher degree of BBU centralization. The common fronthaul solution in C-RAN is to use dedicated fiber. However, centralization requires use of a large number of fiber links which are limited and expensive to deploy. Alternative solutions include the use of other transport technologies such as WDM and OTN, or even the transmission of fronthaul data wirelessly using microwave or mmWave frequency bands. CPRI imposes very strict requirements on the fronthaul network. These requirements make the fronthaul network very expensive to deploy, thereby offsetting the cost saving expected from C-RAN. It can therefore be argued that the fronthaul network could become the bottleneck of 5G mobile networks.

[36] One of the potential technologies targeted to enable future cellular network deployment scenarios and applications is the support for wireless backhaul and relay links enabling flexible and very dense deployment of new radio cells without the need for densifying the transport network proportionately.

The data rates on the fronthaul links are substantially higher compared to the data rates on the radio interface due to CPRI I/Q sampling and additional control information. The centralized BBU and the distributed RRHs exchange uncompressed I/Q samples; therefore, efficient compression schemes are needed to optimize such wideband transmission over capacity-constrained fronthaul links. Possible solutions include digital RF signal sampling rate reduction, use of nonlinear quantization, frequency-domain subcarrier compression, or I/Q data compression. The choice of the most suitable compression scheme is a trade-off between achievable compression ratio, algorithm and design complexity, computational delay, and the signal distortion it introduces, as well as power consumption. Reducing signal sampling rate is a low-complexity scheme with minimal impact on the protocols. Nonlinear quantization improves the signal-to-noise ratio (SNR). Logarithmic encoding algorithms such as μ-law or A-law[37] can also be used to achieve higher transport efficiency on the fronthaul links. Implementation of the orthogonal frequency division multiplexing (OFDM) processing blocks at the RRH allows further reduction in the required fronthaul capacity.

CPRI requires a round-trip latency of 5 μs, excluding propagation delay [75]. More importantly, the total delay including propagation delay is limited by the air-interface hybrid automatic repeat request (HARQ) timing, since HARQ acknowledgments have to be received at the DL/UL transceiver within certain duration and baseband processing would take certain time depending on the air-interface technology. As a result, typically around 200 μs is available for total fronthaul latency. Assuming the speed of light of 200,000 km/s in fiber, CPRI maximum transmission distance is limited to approximately 20 km.

In a fronthaul network which utilizes dark fiber, jitter rarely occurs between BBU and RRH, because this type of optical fiber rarely causes any jitter. On the contrary, in a fronthaul network containing active equipment like WDM or PON, jitter can be introduced to the fronthaul network during signal processing (e.g., mapping/multiplexing in OTN). CPRI I/Q bit streams with such jitter can cause errors in the clock and data recovery process at RRH, subsequently leading to degraded system performance of RRH. Degraded frequency accuracy of the reference clock recovered in RRH can affect the performance of all relevant components that use the reference clock. For example, an inaccurate reference clock may cause errors when converting LTE/NR I/Q samples into analog signals during the digital-to-analog conversion. It can further lead to inaccurate frequency of carrier signals used for radio transmission of the analog signals. Therefore jitter in the fronthaul network can cause significant impacts on the quality of

[37] A-law is a companding algorithm, which is used in European 8-bit PCM digital communications systems to modify the dynamic range of an analog signal for digitization. It is one of the versions of the ITU-T G.711 standard. The μ-law algorithm is another companding algorithm, which is primarily used in 8-bit PCM digital telecommunication systems in North America and Japan. Companding algorithms reduce the dynamic range of an audio signal, resulting in an increase in the signal-to-noise ratio achieved during transmission. In the digital domain, it can reduce the quantization error.

LTE/NR signals transmitted through RRH antennas. Therefore when implementing a fronthaul network for C-RAN, extensive verification is required to ensure jitter introduced by active equipment is maintained within the tolerable range [60].

The stringent latency requirements have kept the fronthaul interface away from packet-switched schemes such as Ethernet. However, with the exponential increase in bandwidth requirements for 5G networks, packet-based transport schemes cannot be disregarded. The economy of scale and the statistical multiplexing gain of Ethernet are essential for the new fronthaul transport. In cooperation with CPRI Forum, IEEE 802.1 took the task of defining a new fronthaul transport standard under the IEEE 802.1cm[38] project. The project was entitled, Time-Sensitive Networking (TSN)[39] for fronthaul, which defines profiles for bridged Ethernet networks that will carry fronthaul payloads in response to requirements contributed by the CPRI forum. The requirements can be divided into three categories:

1. Class 1: I/Q and Control and Management (C&M) data
2. Synchronization
3. Class 2: eCPRI which has been recently added

[38] IEEE 802.1CM—time-sensitive networking for fronthaul (http://www.ieee802.org/1/pages/802.1cm.html).

[39] Time-sensitive networking is a standard developed by IEEE 802.1Q to provide deterministic messaging on standard Ethernet. Time-sensitive networking scheme is centrally managed with guaranteed delivery and minimized jitter using scheduling for those real-time applications that require deterministic behavior. Time-sensitive networking is a data link layer protocol and as such is part of the Ethernet standard. The forwarding decisions made by the time-sensitive networking bridges use the Ethernet header contents and not the Internet protocol address. The payloads of the Ethernet frames can be anything and are not limited to Internet protocol packets. This means that time-sensitive networking can be used in any environment and can carry the payload of any application. There are five main components in the time-sensitive networking solution as follows [78]:

- Time-sensitive networking flow: The time-critical communication between end devices where each flow has strict timing requirements and each time-sensitive networking flow is uniquely identified by the network devices.
- End devices: These are the source and destination of the time-sensitive networking flows. The end devices are running an application that requires deterministic communication.
- Bridges: Also referred as Ethernet switches, these are special bridges capable of transmitting the Ethernet frames of a time-sensitive networking flow on schedule and receiving Ethernet frames of a time-sensitive networking flow according to a schedule.
- Central network controller: A proxy for the network comprising the time-sensitive networking bridges and their interconnections, and the control applications that require deterministic communication. The central network controller defines the schedule based on which all time-sensitive networking frames are transmitted. Centralized user configuration: An application that communicates with the central network controller and the end devices and represents the control applications and the end devices. The centralized user configuration makes requests to the central network controller for deterministic communication with specific requirements for the flows.

I/Q and C&M data can be transported independently. The round-trip delay for I/Q is limited to 200 μs and maximum frame error rate is 10^{-7}. The C&M data has more relaxed time budgets. Synchronization signals represent an interesting aspect, with a wide range of requirements driven by wireless standards such as 3GPP LTE/NR. Four classes have been defined [75]:

1. Class A+: Strictest class with time error budget of 12.5 ns (one way) for applications such as MIMO and transmit diversity.
2. Class A: Time error budget up to 45 ns for applications including contiguous intra-cell CA.
3. Class B: Budgets up to 110 ns for non-contiguous intra-cell CA.
4. Class C: The least strict class delivers a budget up to 1.5 μs from the primary reference time clock[40] to the end application clock recovery output.

The above synchronization requirements, which continue to become more stringent with the new releases of the standard, pose new challenges for network designers. Traditional backhaul networks mostly rely on GPS receivers at cell sites. It is the simplest solution from the perspective of backhaul network design, but GPS systems have their own vulnerabilities and are not available in certain locations (e.g., deep indoor environments). Therefore, operators around the world have increasingly begun to deploy precision time protocol (PTP)/IEEE 1588v2[41] scheme as a backup mechanism and in some cases as the primary synchronization source in the absence of a viable GPS-based solution.

Standard bodies such as ITU-T have continued to refine and enhance the architectures and metrics for packet-based synchronization networks in parallel with the development of a new fronthaul. The ITU-T G.826x and G.827x[42] series provide a rich set of documents that define the architectures, profiles, and network limits for frequency and time/phase synchronization services. Phase synchronization exhibits an especially interesting challenge for synchronization experts as pointed out by the above fronthaul synchronization requirements. PTP has been defined to synchronize the time and phase of end applications to a primary reference. The PTP protocol continuously measures and attempts to eliminate any offset between the phase of the end application and the primary reference. However, in conventional Ethernet networks, packet delay variation has posed a major challenge to transferring acceptable clock qualities in wireless applications. Ethernet switch manufacturers responded

[40] The primary reference time clock provides a reference time signal traceable to a recognized time standard UTC.

[41] IEEE Std 1588-2008: IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems (https://standards.ieee.org/findstds/standard/1588-2008.html).

[42] G.826: End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections (https://www.itu.int/rec/T-REC-G.826/en) and G.827: Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths (https://www.itu.int/rec/T-REC-G.827/en).

to this challenge by delivering new classes of PTP-aware nodes such as boundary clocks and transparent clocks. PTP-aware nodes are being increasingly deployed in wireless access networks around the world. While the packet delay variation is not a major concern for these deployments, timing error analysis remains a major point of focus. Timing error defines the difference between the time of a clock at any relevant part of the network and the time of a reference clock such as one delivered by a GPS source at another part of the network. It can result from network asymmetries and node configuration/performance issues [84].

In order to relax the excessive latency and capacity constraints on the fronthaul, the operators and vendors have revisited the concept of C-RAN and considered more flexible distribution of baseband functionality between the RRH and the BBU pool. Instead of centralizing the entire BBU processing on the cloud, by dividing the physical receive and transmit chain in different blocks, it is possible to keep a subset of these blocks in the RRH. By gradually placing more and more BBU processing at the edge of the network, the fronthaul capacity requirement becomes less stringent. Nevertheless, partial centralization has two main drawbacks, both relating to the initially envisioned benefits of C-RAN: (1) RRHs become more complex, and thus more expensive; and (2) de-centralizing the BBU processing reduces the opportunities for multiplexing gains, coordinated signal processing, and advanced interference avoidance schemes. Consequently, flexible or partial centralization is a trade-off between what is gained in terms fronthaul requirements and what is lost in terms of C-RAN features.

Another key question is how the information between the RRH and the BBU is transported over the fronthaul link. A number of fronthaul transmission protocols have been studied since the inception of the C-RAN architecture. However, transport schemes such as CPRI have been predominantly considered for carrying raw I/Q samples in a traditional C-RAN architecture. Considering the potential for various functional splits between the BBU and the RRH, different types of information might need to be transported over the fronthaul link. Given the extensive adoption of Ethernet in the data centers and the core network, RoE could be a generic, cost-effective, off-the-shelf alternative for fronthaul transport. Furthermore, while a single fronthaul link per RRH to the BBU pool has usually been assumed, it is expected that the fronthaul network will evolve to more complex multi-hop topologies, requiring switching and aggregation. This is further facilitated by a standard Ethernet approach. Nevertheless, packetization over the fronthaul introduces some additional concerns related to latency and overhead. As information arriving at the RRH and/or BBU needs to be encapsulated in an Ethernet frame, header-related overhead is introduced per frame. To ensure that this overhead is small, and does not waste the potential bandwidth gains from baseband functional splitting, it would be desirable to fill an Ethernet payload before sending a frame. However, waiting to fill a payload introduces additional latency. Hence, it is important to consider the impact of packetization on the fronthaul bandwidth

and latency, in conjunction with possible functional splits between RRH and BBUs, in order to understand the feasibility and potential gains of different approaches.

In the study item for the new radio access technology, 3GPP studied different functional splits between the CU and the DU [34]. Fig. 1.26 shows the possible functional splits between the CU and the DU. After months of discussions between the opponents and proponents of open interfaces, 3GPP initially decided to specify two out of eight possible functional splits, that is, options 2 and 7, but no agreement on option 7 could be reached. Note that option 8 has already been used in LTE and previous generations, where CPRI was the main fronthaul interface transport scheme. As we move from left to right in Fig. 1.26, the split point moves from layer-3 protocols and functions to the lower layer protocols and functions, that is, layers 1 and 2, and ultimately I/Q samples transmission over the fronthaul.

Split option 7 has three variants, as shown in Fig. 1.27, depending on what aspects of physical layer processing are performed in the DU/RRUs. In the following, a detailed description of each functional split and its corresponding advantages and disadvantages are provided [34]:

- *Option 1:* This functional split option is similar to the reference architecture for dual connectivity. In this option, the RRC sublayer is located in the CU. The packet data convergence protocol (PDCP), radio link control (RLC), MAC, physical layer, and RF functional processing are located in the DU(s). This option allows separate user-plane connections (split bearers) while providing centralized RRC and management. It may, in some circumstances, provide benefits in handling edge computing or low-latency use cases where the user data must be stored/processed in the proximity of the transmission point. However, due to the separation of RRC and PDCP, securing the interface in practical deployments may affect performance of this option. Furthermore, the RRUs will be more complex and expensive due to the additional hardware for local processing of layer-1 and layer-2 functions.
- *Option 2:* This functional split is similar to option 1 except PDCP functions are also co-located with the RRC functions in the CU. This option would allow traffic aggregation from NR and LTE transmission points to be centralized. It can further facilitate management of traffic load between NR and LTE links. Note that the PDCP-RLC split was already standardized in LTE under dual-connectivity work item. In addition, this option can be implemented by separating the RRC and PDCP for the control-plane stack and the PDCP for the user-plane stack into different central entities. This option enables centralization of the PDCP sublayer, which may be predominantly affected by user-plane process and may scale with user-plane traffic load.
- *Option 3:* In this option, the lower RLC functions, MAC sublayer, physical layer, and RF functions are located in the DU, whereas PDCP and higher RLC functions are

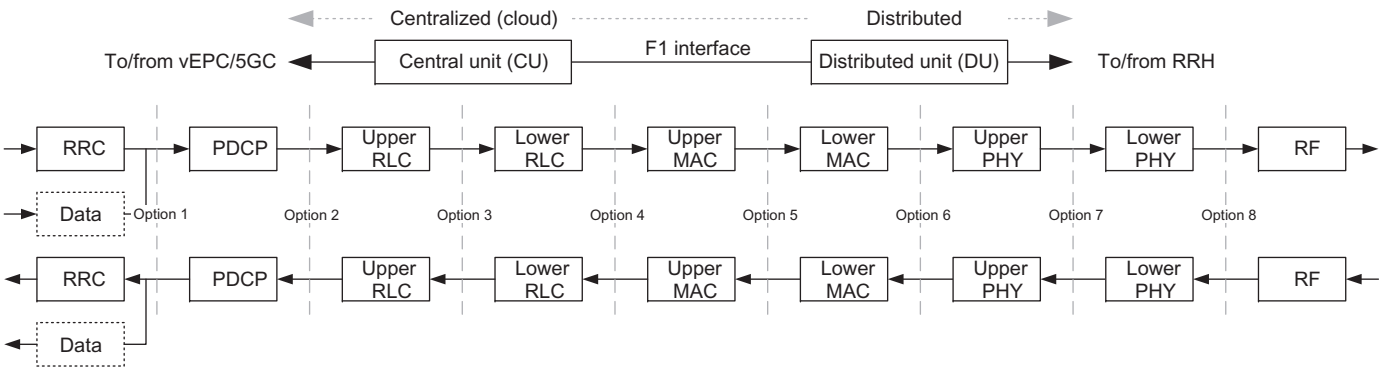


Figure 1.26
Functional split between the CU and the DU [34].

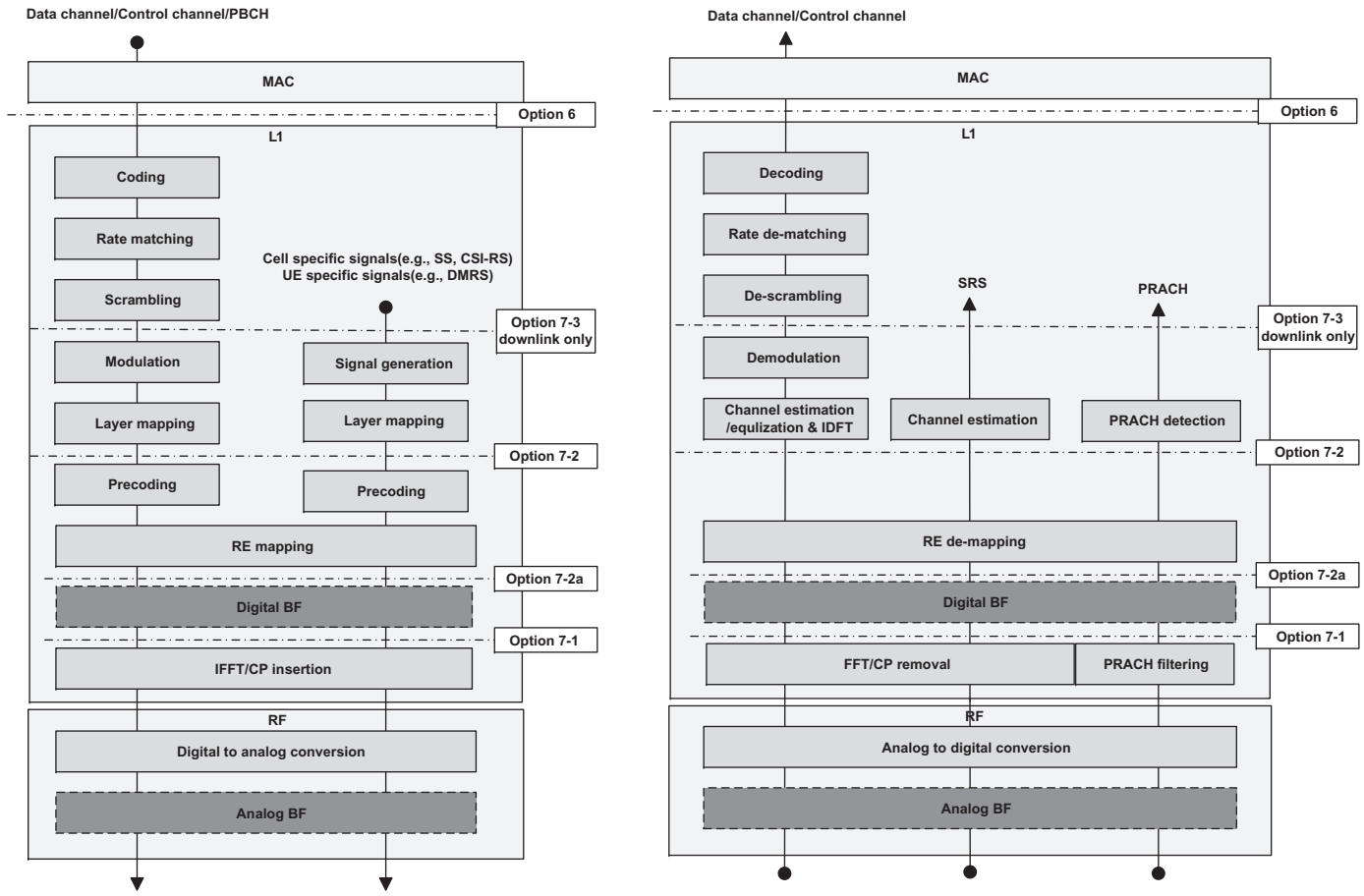


Figure 1.27
Variants of option 7 functional split [34].

implemented in the CU. Depending on real-time/non-real-time RLC processing requirements, the lower RLC may include segmentation functions and the higher RLC may include ARQ and other RLC functions. In this case, the centralized RLC functions will segment the RLC PDUs based on the status reports, while the distributed RLC functions will segment the RLC PDUs into the available MAC PDU resources. This option will allow traffic aggregation from NR and LTE transmission points to be centralized. It can further facilitate the management of traffic load between NR and LTE transmission points and it may have a better flow control across the split. The ARQ functions located in the CU may provide centralization gains. The failure over transport network may also be recovered using the end-to-end ARQ mechanism at the CU. This may provide more protection for critical data and control-plane signaling. The DUs without RLC functions may handle more connected mode UEs as there is no RLC state information stored and hence no need for UE context. Furthermore, this option may facilitate implementation of the integrated access and backhaul to support self-backhauled NR transmission points. It was argued that this option may be more robust under non-ideal transport conditions since the ARQ and packet ordering are performed at the CU. This option may reduce processing and buffering requirements in the DUs due to absence of ARQ protocol. This option may provide an efficient way for implementing intra-gNB mobility. Nonetheless, this option is more prone to latency compared to the option with ARQ in the DUs, since retransmissions are susceptible to transport network latency.

In an alternative implementation, the lower RLC functional group may consist of transmitting side of RLC protocol associated with downlink transmission and the higher RLC functional group may comprise the receiving side of RLC protocol, which are related to uplink transmission. This functional regrouping is not sensitive to the transmission network latency between the CU and the DU and uses interface format inherited from the legacy interfaces of PDCP-RLC and MAC-RLC. Since the receiving side of RLC protocol is located in the CU, there would be no additional transmission delay of PDCP/RLC reestablishment procedure when submitting the RLC SDUs[43] to PDCP. Furthermore, this alternative does not impose any transport constraint, for example,

[43] A service data unit is a specific unit of data that has been passed down from an open-system interconnection layer to a lower layer, which the lower layer has not yet encapsulated into a protocol data unit. A service data unit is a set of data that is sent by a user of the services of a given layer, and is transmitted semantically unchanged to a peer service user. The protocol data unit at a layer N is the service data unit of layer $N-1$. In fact, the service data unit is the payload of a given protocol data unit. That is, the process of changing a service data unit to a protocol data unit consists of an encapsulation process, performed by the lower layer. All data contained in the service data unit becomes encapsulated within the protocol data unit. The layer $N-1$ adds headers/subheaders and padding bits (if necessary to adjust the size) to the service data unit, transforming it into the protocol data unit of layer N. The added headers/subheaders and padding bits are part of the process used to make it possible to send data from a source node to a destination node.

transport network congestion. Nevertheless, due to performing flow control in the CU and the RLC transmit side in the DU, double buffering is needed for transmission.

- *Option 4:* In this case, MAC sublayer, physical layer, and RF functions are processed in the DUs, whereas PDCP and RLC protocols are processed in the CU. No particular advantage was shown for this option.
- *Option 5:* In this option, the RF, physical layer, and some part the MAC sublayer functions (e.g., HARQ protocol) are implemented in the DUs. The upper protocol stack is implemented in the CU. Therefore by splitting the MAC sublayer into two entities (e.g., upper and lower MAC), the services and functions provided by the MAC sublayer will be implemented in the CU and/or the DU. As an example, the centralized scheduling function located in the upper MAC will be in charge of the control of multiple lower MAC sublayers. The inter-cell interference coordination located in the upper MAC will be responsible for interference coordination. Time-critical functions in the lower MAC may include functions with stringent delay requirements (e.g., HARQ protocol) or the functions where performance is proportional to latency (e.g., radio channel and signal measurements at physical layer or random access control). Radio-specific functions in the lower MAC can perform scheduling-related processing and reporting. They can also control activities of the configured UEs and report statistics periodically or on-demand to the upper MAC. This option will allow traffic aggregation/distribution from/to NR and LTE transmission points. Moreover, it can facilitate the management of traffic load between NR and LTE transmission points. In this option, the requirement for fronthaul bandwidth and latency can be relaxed depending on the load across access and core network interface. It allows efficient interference management across multiple cells and enhanced coordinated scheduling schemes such as multipoint transmission/reception.
- *Option 6:* In this option, the physical layer and RF functions are implemented in the DU, whereas the upper protocol layers are located in the CU. The interface between the CU and the DUs carries data, configuration, and scheduling-related information, as well as measurement reports. This option will allow centralized traffic aggregation from NR and LTE transmission points, which can facilitate management of traffic load between NR and LTE access nodes. The fronthaul requirements in terms of throughput are reduced as the payload for this option are transport block bits. Joint transmission and scheduling is also possible in this case since MAC sublayer is centralized. This option may require subframe-level timing synchronization between MAC sublayer in the CU and physical layer in the DUs. Note that round-trip fronthaul delay may affect HARQ timing and scheduling.
- *Option 7:* In this option as shown in Fig. 1.27, the lower physical layer functions and RF circuits are located in the DU(s). The upper protocol layers including the upper physical layer functions reside in the CU. There are multiple realizations of this option including asymmetrical implementation of the option in the downlink and uplink (e.g., option 7-1 in the uplink and option 7-2 in the downlink). A compression technique may

be applied to reduce the required transport bandwidth between the CU and the DU. This option will allow traffic aggregation from NR and LTE transmission points to be centralized and can facilitate the management of traffic load between NR and LTE transmission points. This option can to some extent relax the fronthaul throughput requirements and allows centralized scheduling and joint processing in both transmit and receive sides. However, it may require subframe-level timing synchronization between the fragmented parts of physical layer in the CU and the DUs. The following represent different forms where this option can be implemented:

- *Option 7-1:* In this variant, the fast Fourier transform (FFT), CP removal (OFDM processing), and possibly PRACH processing is implemented in the uplink and in the DUs, and the remaining physical layer functions reside in the CU. In the downlink, inverse FFT (IFFT) and CP insertion blocks (OFDM processing) reside in the DUs and the rest of physical layer functions will be performed in the CU. This variant would allow implementation of advanced receivers.
- *Option 7-2:* In this variant, FFT, CP removal, resource de-mapping, and possibly MIMO decoding functions are implemented in the DU in the uplink and the remaining physical layer functional processing are performed in the CU. In the downlink, IFFT, CP addition, resource mapping, and MIMO precoding functions are performed in the DU, and the rest of physical layer processing is performed in the CU. This variant also allows the use of advanced receivers for enhanced performance.
- *Option 7-3:* This downlink only option implements the channel encoder in the CU, and the rest of physical layer functions are performed in the DU(s). This option can reduce the fronthaul throughput requirements as the payloads consist of the encoded bits.

- *Option 8:* In this option, RF functionality is in the DU and the entire upper layer functions are located in the CU. Option 8 allows for separation of RF and the physical layer and further facilitates centralization of processes at all protocol layer levels, resulting in very tight coordination of the RAN and efficient support of features such as CoMP, MIMO, load balancing, and mobility. This option will allow traffic aggregation from NR and LTE transmission points to be centralized. Moreover, it can facilitate the management of traffic load between NR and LTE transmission points, yielding high degree of centralization and coordination across the entire protocol stack, which enables more efficient resource management and radio performance. Separation between RF and physical layer decouples RF components from physical layer updates, which may improve their respective scalability. Separation of RF and physical layer allows reuse of the RF components to serve physical layers of different radio access technologies and allows pooling of physical layer resources, which may enable cost-efficient dimensioning of the physical layer. It further allows operators to share RF components, which may reduce system and site development/maintenance costs. However, it results in more stringent requirements on fronthaul latency, which may cause constraints on network deployments with respect to network topology and available transport options, as

well as rigorous requirements on fronthaul bandwidth, which may imply higher resource consumption and costs in transport mechanisms.

There are strict timing, frequency, and synchronization requirements for the fronthaul links. In particular, 3GPP has imposed stringent latency requirements on transporting I/Q signals over the fronthaul, which pose certain challenges for system designers [11,14]. CPRI transport for fronthaul requires a low latency link and 200 μs is a generally accepted value for the round-trip latency, which limits the length of the fronthaul links to about 20 km. CPRI implementations require tight frequency and timing synchronization and accurate time of day (ToD) clock synchronization. A frequency precision of 16 ppb and ToD accuracy within 1.5 μs are required for CPRI transport.

The advantage of any functional split mainly depends on the availability of an ideal or non-ideal transport network. In a non-ideal fronthaul transport case, the functional split needs to occur at a higher level in the protocol stack, which reduces the level of centralization that can be achieved through C-RAN. In this case, the synchronization and bandwidth requirements can be relaxed at the expense of some of these 4G/5G RAN features such as massive MIMO, CA, and multipoint joint processing. The following solutions can be used to help overcome these obstacles. White Rabbit technology[44] is a combination of physical layer and PTP timing. White Rabbit introduces the technique of measuring and compensation for asymmetry to mitigate time and phase transfer errors. White Rabbit provides sub-nanosecond timestamp accuracy and pico-second precision of synchronization for large distributed systems and allows for deterministic and reliable data delivery. To achieve sub-nanosecond synchronization, White Rabbit utilizes synchronous Ethernet (SyncE)[45] to achieve synchronization and IEEE 1588v2. White Rabbit uses the PTP to achieve sub-nanosecond accuracy. A two-way exchange of the PTP synchronization messages allows precise adjustment of clock phase and offset. The link delay is known precisely via accurate hardware timestamps and the calculation of delay asymmetry. Alternatively, partial timing support compatible with ITU-T G.8275.2 standard can be used where the position of a grandmaster clock is moved closer to the PTP slaves in the RRHs. This is an excellent alternative to full on-path support White Rabbit for those operators who are not willing or cannot upgrade their networks for White Rabbit physical layer support.

[44] White Rabbit is a multidisciplinary project for development of a new Ethernet-based technology which ensures sub-nanosecond synchronization and deterministic data transfer. The project uses an open-source paradigm for the development of its hardware and software components (https://www.ohwr.org/projects/white-rabbit/wiki/).

[45] Synchronous Ethernet is an ITU-T standard for computer networking that facilitates the transfer of clock signals over the Ethernet physical layer. This signal can then be made traceable to an external clock.

CPRI Transport The CPRI is an industry forum defining a publicly available specification for the interface between a radio equipment control (REC) and a radio equipment (RE) in wireless networks. CPRI specifies a digitized serial interface between a base station referred to as REC in CPRI terminology and an RRH or RE. The specifications cover the user-plane, the control-plane transport mechanisms, as well as the synchronization schemes. The specification supports both electrical and optical interfaces as well as point-to-point, star, ring, daisy-chain topologies. The CPRI interface provides a physical connection for I/Q samples transport as well as radio unit management, control signaling, and synchronization such as clock frequency and timing synchronization [75].

CPRI transports I/Q samples to/from a particular antenna port and RF carrier. This is called an antenna-carrier (AxC) and is the amount of digital baseband (I/Q) user-plane data necessary for either reception or transmission of only one carrier at one independent antenna element. An AxC group is an aggregation of multiple AxC streams with the same sample rate, the same sample width, and the same destination. An AxC container consists of a number of AxCs and is a part of a basic CPRI frame (see Fig. 1.28). Data is organized into basic frames of 16 words. The first word of each basic frame is the control word. Each word can be 8, 16, or 32 bits, depending on the width of the I/Q samples. The width of the word depends on the CPRI line rate. For example, in an LTE system, if I = 16 bits and Q = 16 bits, then one AxC is 32 bits. Each 256 basic frames make up a hyperframe and 150 hyperframes are needed to transport an LTE 10 ms frame. Data in a basic frame is encoded with 8B/10B encoding, that is, 8 bits of data are encoded in 10 bits. The extra bits are used to detect link failures. Some of the CPRI rates support 64B/66B encoding scheme and this

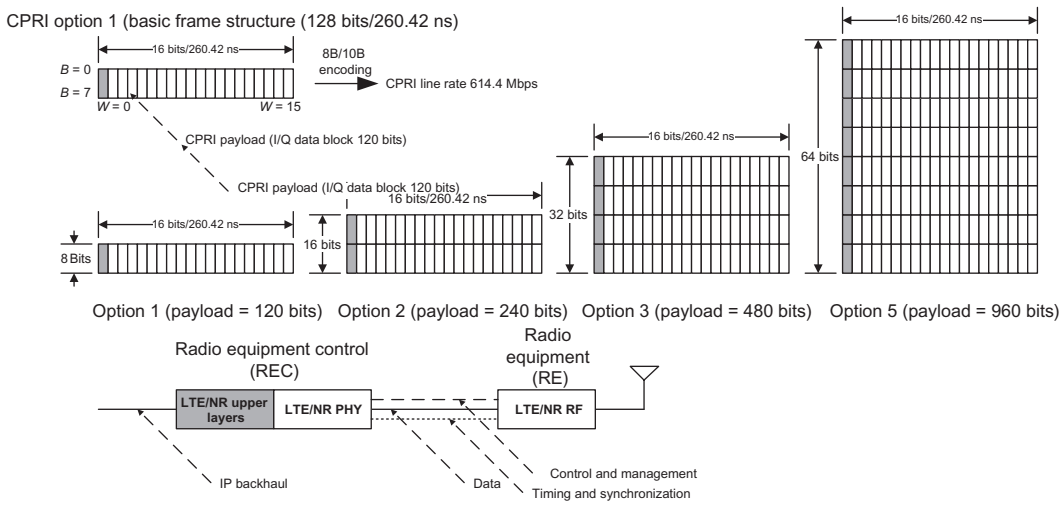


Figure 1.28
CPRI frame structure [60].

extension is used to detect sync header impairments and link failures. Note that 8B/10B and 64B/66B encodings incur 20% and 3% overhead, thus the latter would be a significant improvement in overhead reduction.

The CPRI specification specifies the maximum allowed effect of the fronthaul jitter on the frequency accuracy of the clock recovered at the RRH relative to a master reference clock at the BBU. One of the CPRI technical requirements defines the clock frequency accuracy of RRH as ± 0.002 ppm. This requirement states that the maximum impact of jitter from the CPRI fronthaul on the frequency accuracy of RRH should be less than ± 0.002 ppm. In addition to jitter, there are other factors that may affect the accuracy of clock frequency. CPRI requires very high reliability with bit error rates (BERs) of $\leq 10^{-12}$.

The CPRI framing process is illustrated in Fig. 1.29. User data is transported as baseband digital I/Q stream in a data block of a CPRI basic frame. The RRH, upon receiving the data, converts it into an analog signal, amplifies it, and then radiates the signal over the air. Control and management data and synchronization information are delivered through CPRI subchannels, more specifically through control words in the CPRI basic frames. This information is only used by the REC (on the BBU side) and the RE (on the RRH side). CPRI subchannels are created per CPRI hyper-frame, which is 66.67 μs and a hyperframe consists of 256 basic frames (260.42 ns). Each basic frame has one byte of a control word and 15 bytes of payload. A group of 256 control words in one hyperframe collectively constitute 64 subchannels. Fig. 1.29 shows a CPRI subframe and how the control and management data and synchronization information are mapped and transported [75].

eCPRI Transport The concepts of CPRI-over-Ethernet and replacing the TDM-like CPRI format with Ethernet messaging both hold the promise of reducing the bandwidth requirements of CPRI transport and making fronthaul affordable and available to all mobile operators. Ethernet is a very cost-effective transport technology that is widely deployed in the

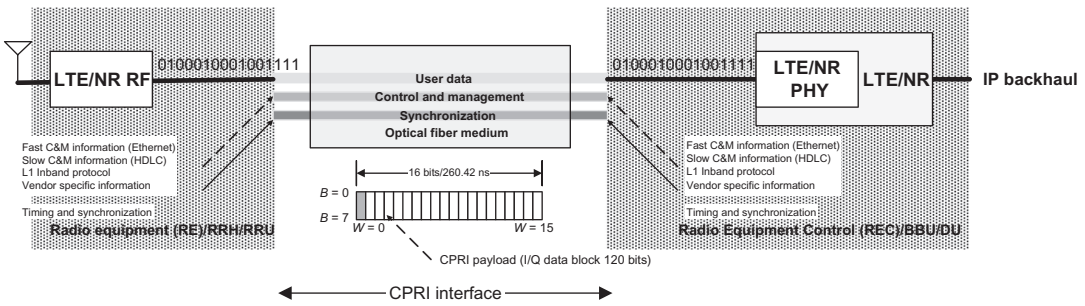


Figure 1.29
Illustration of CPRI framing [60].

backhaul transport network. However, it is also an asynchronous best effort technology that has not been originally designed to meet the low latency, low jitter, and tight synchronization requirements of baseband signal transmission. The new specification, known as eCPRI, introduces improved transport efficiency to match the speed and bandwidth requirements of 5G fronthaul networks. The eCPRI specification was released in August 2017 that supports partitioning of base station functions. The main advantages of the eCPRI protocol include support of functional split option 7, flexible bandwidth scaling according to user-plane traffic, and the use of mainstream transport technologies, which makes it possible carrying eCPRI and other traffic simultaneously in the same switched network.

The main difference between eCPRI and CPRI v7.0 can be summarized by looking at their respective characteristics [76].

- CPRI characteristics
  - It is intrinsically a point-to-point interface.
  - There is a master port and a slave port connected directly by optical/electrical cable (s) as a hop.
  - Networking functions are application layer functions and not supported by the CPRI interface itself.
  - Supported topologies depend on REC/RE functions.
  - Supported logical connections include point-to-point (one REC ↔ one RE) and point-to-multipoint (one REC ↔ several REs).
  - Redundancy, QoS, security, etc. are REC/RE functions.
- eCPRI characteristics
  - An eCPRI network consists of eCPRI nodes (eRECs and eREs), transport network, as well as other network elements including grand master for timing and EMS/NMS for management.
  - There is no longer a master port/slave port classification at physical level. SAP_S: master of PTP and synchronous Ethernet is not an eREC entity in general. SAP_{CM}: some of management-plane entities may be managed by EMS/NMS.
  - The eCPRI layer is above the transport networking layer.
  - The eCPRI layer does not depend on a specific transport network layer (TNL) topology.
  - The transport network may include local network and local switches provided by the eREC/eRE vendors.
  - Supported logical connections include point-to-point (one eREC ↔ one eRE), point-to-multipoint (one eREC ↔ several eREs), multipoint-to-multipoint (eRECs ↔ eREs, eRECs ↔ eRECs, eREs ↔ eREs).
  - Redundancy, QoS, security, etc. are mainly transport network functions; eCPRI nodes need to implement proper TNL protocols to support these capabilities.

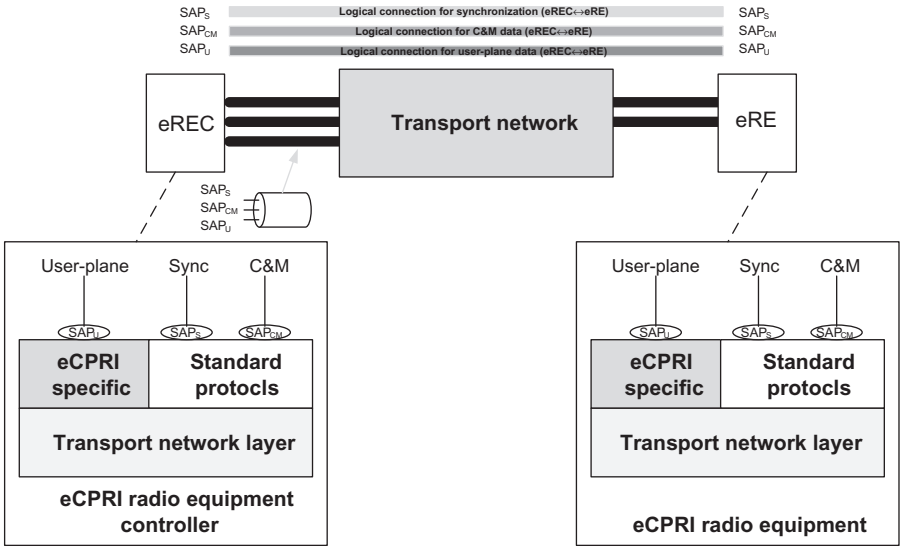


Figure 1.30
eCPRI system and interface definition [76].

As shown in Fig. 1.30, in eCPRI, the radio base station is divided into two building blocks: eCPRI radio equipment control (eREC) and eCPRI radio equipment (eRE), which are physically separated and are connected via a transport network. The eREC implements part of the physical layer functions and higher layer functions of the air interface, whereas the eRE contains the remaining part of the physical layer functions and the analog RF functions. User-plane data, control and management, and synchronization signals (i.e., synchronization data used for frame and timing alignment) are packetized, multiplexed, and transferred over the transport network which connects eREC(s) and eRE(s). The eCPRI does not rely on specific transport network and data-link-layer protocols, thus any type of network can be used for eCPRI provided that eCPRI requirements are fulfilled (see Fig. 1.31).

Fig. 1.32 shows high-level protocol stack and physical layer processing of an LTE eNB or NR gNB. The eCPRI specification defines five functional splits identified as A to E splits. An additional set of intra-PHY functional divisions identified as I_D, II_D, and I_U are also defined. It is understood that the CPRI specification supports only functional split E. The physical layer processing stages shown in Fig. 1.32 are consistent with those of the NR. The eCPRI specification focuses on three different reference splits, two splits in the downlink and one split in the uplink. Any combination of the different DL/UL splits is also possible. Other functional splits within the physical layer and/or upper layers are not precluded by eCPRI specification. The information flows for the eCPRI interface are defined as user plane including user data, real-time control data, and other eCPRI services; control and

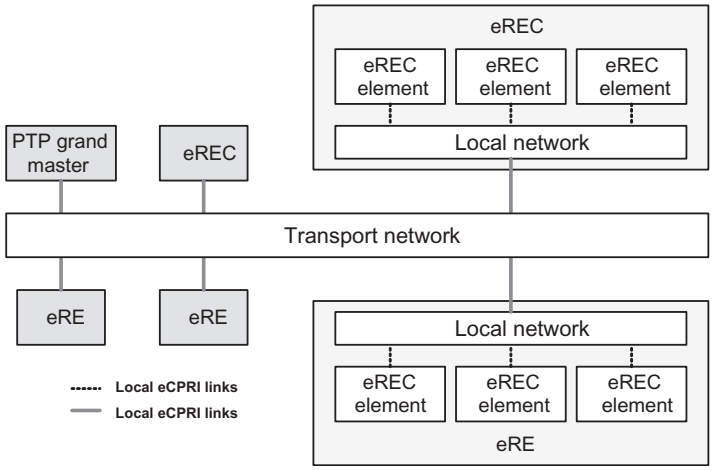


Figure 1.31
eCPRI example system architecture [76].

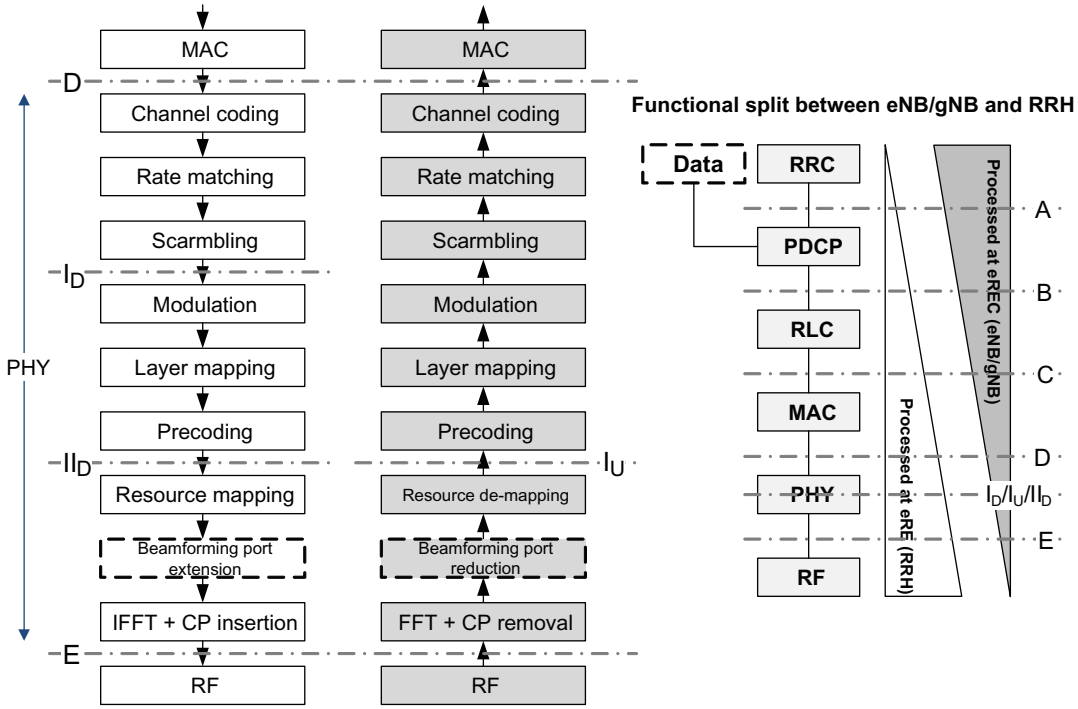


Figure 1.32
Processing stages of the physical layer shown in eCPRI specification [76].

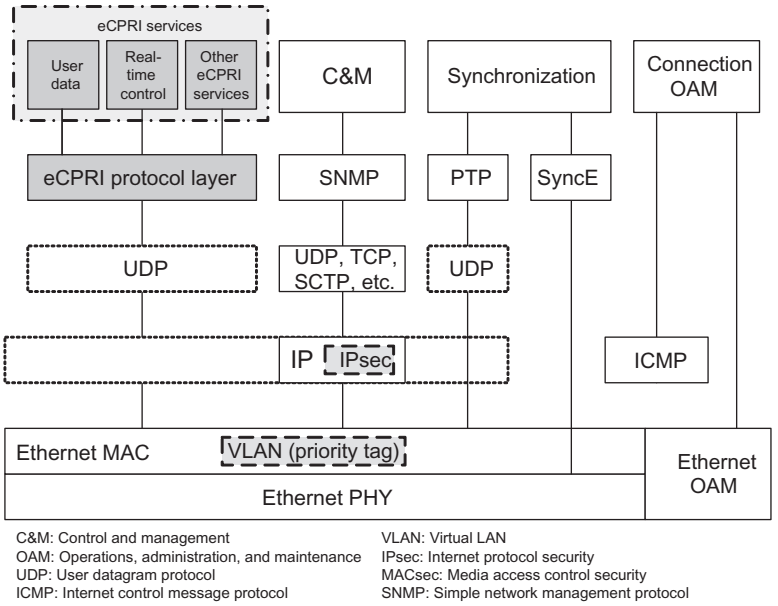


Figure 1.33
eCPRI protocol stack over IP or Ethernet [76].

management plane; and synchronization plane. The control and management information exchanged between the control and management entities are within the eREC and the eRE. This information flow is provided to the higher protocol layers and is not considered to be time critical. An eCPRI protocol layer for the user plane is defined, as shown in Fig. 1.33. The eCPRI specification identifies Ethernet and IP as two transport options for the user plane. It further defines certain messages for the user plane, which include user data, real-time control data, and other services. The *I/Q Data* and *Bit Sequence* message types are defined for the user data whose selection depends on the functional split that is used. The *Real-Time Control Data* message type is defined for real-time control information. These message formats are shown in Fig. 1.34.

The eCPRI specification does not provide the detailed description of the information fields of the above message types. In these message formats, the following fields are identified: PC_ID (an identifier of a series of *I/Q Data Transfer* messages; or an identifier of a series of *Bit Sequence Transfer* messages), RTC_ID (an identifier of a series of *Real-Time Control Data* messages), SEQ_ID (an identifier of each message in a series of *I/Q Data Transfer* messages; or an identifier of each message in a series of *Bit Sequence Transfer* messages), I/Q samples of user data (a sequence of I/Q sample pairs (I,Q) in frequency domain or time domain and associated control information, if necessary), bit sequence of user data, real-time control data, whose interpretation is left to implementation. Therefore, the details of

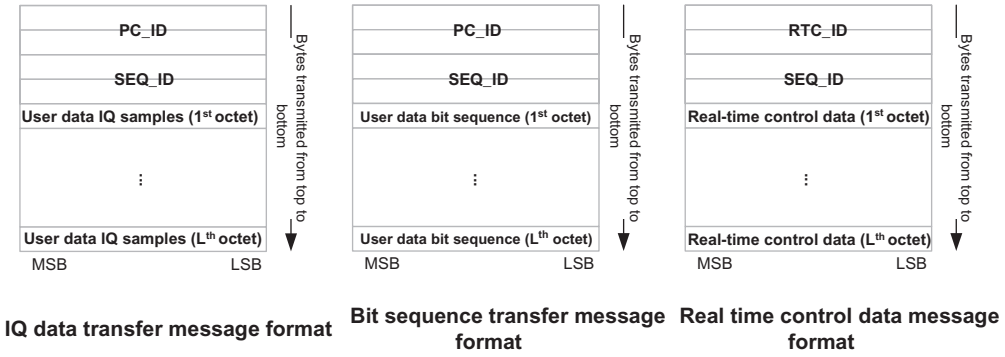


Figure 1.34
eCPRI user-plane message formats [76].

information flow are out of the scope of the eCPRI specification. This flexibility implies that there is additional work required to realize multi-vendor interoperable solutions.

IEEE 1914.3 Radio-Over-Ethernet Transport As we mentioned earlier, the TSN has been designed to ensure timely transport of delay-sensitive packetized streams such as CPRI-over-Ethernet; however, it does not deal with the encapsulation of various fronthaul transport payloads. RoE is a standard for radio transport over Ethernet including specification of encapsulations and mappings developed by IEEE 1914.3 working group.[46] It enables transport of I/Q data over Ethernet (i.e., native RoE packet mapper) as well as support of structure-aware and structure-agnostic mappers for CPRI and other data formats. The work targeted among others definition of a native RoE encapsulation and mapper transport format for both digitized radio payload (I/Q data) and management and control data. The Ethernet packet format itself is not changed and neither is the MAC protocol, as shown in Fig. 1.35.

The RoE defines a native encapsulation header format for transporting time-sensitive radio data and control information. The definition of protocol primitives allows multiplexing of independent streams, for example, antenna and carriers; time stamping or sequence numbering to enable time synchronization of RoE packets and timing alignment of the streams; control protocol for auxiliary non-data streams and for link and RoE endpoint management; and mapper(s) for existing CPRI framing standards to a native RoE encapsulation and transport. There is also focus on enabling support for non-native radio data where the transport structure is simply a container for the data (see Fig. 1.35). IEEE 1914.3 has further

[46] IEEE 1914.3: Standard for radio-over-Ethernet encapsulations and mappings (http://sites.ieee.org/sagroups-1914/p1914-3/).

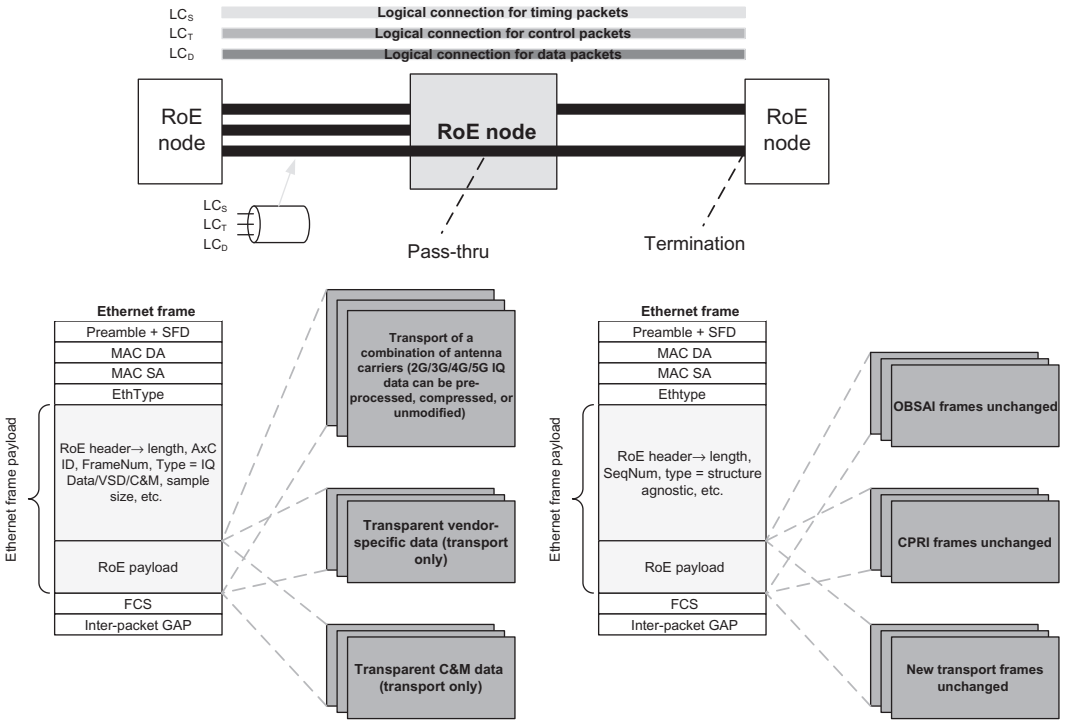


Figure 1.35
RoE encapsulation: RoE structure aware and agnostic mappers [77].

considered implementing a structure-aware mapper for CPRI with well-defined encapsulation procedure. One can therefore distinguish between a simple tunneling mapper for the former use case and the structure-aware mapper for CPRI. There is also a structure-agnostic mapper in the specs which offers a middle ground for efficiency and complexity relative to the other mappers. Several use cases of RoE can be considered including aggregation of multiple CPRI streams from a number of RRHs to a single RoE link to the BBU pool, or a native edge-to-edge RoE connection from the RRH directly to the BBU pool. The RoE will logically add a new switching/aggregation node between the baseband pool and the radio resources.

IEEE 1914.1 Next-Generation Fronthaul Interface The fronthaul packet transport enables implementation of critical 4G/5G technologies such as massive MIMO, CoMP transmission and reception, and scalable centralized/virtual RAN functions. Current network deployment models and practices based on traditional backhaul or fronthaul requirements are likely to be unsustainable and expensive for 5G deployments as the need for integrated access and backhaul in heterogeneous networks becomes more compelling. The NGFI is the new

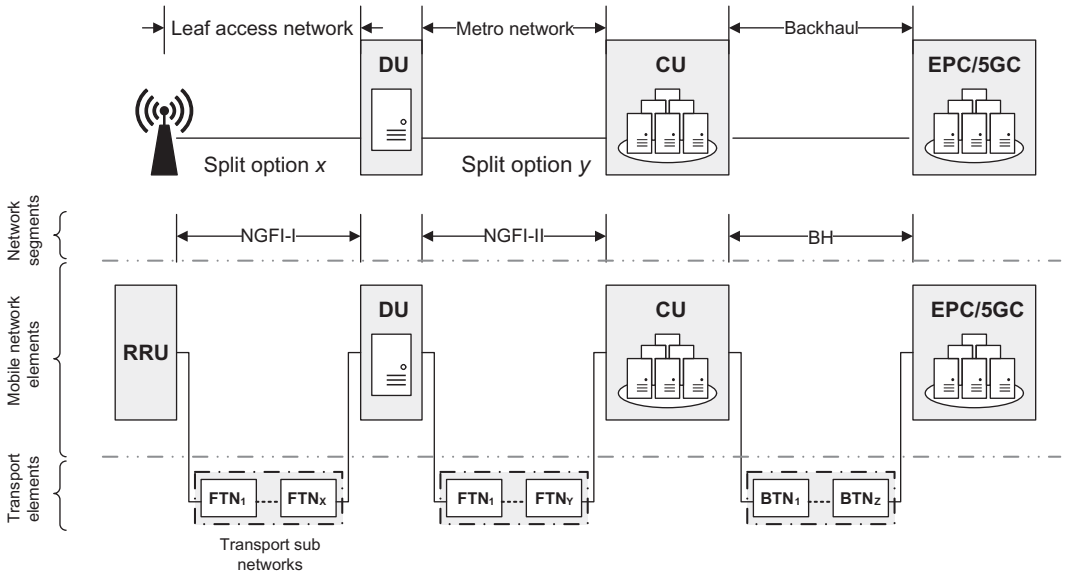


Figure 1.36
Example of RAN aggregation node with CU and DUs [78].

packet-based fronthaul interface specified by IEEE 1914.1[47] in order to provide bandwidth efficiency and to achieve scalability in transport networks as the CPRI standard cannot scale with the bandwidth requirements of 5G. IEEE 1914.1 standard simplifies network design and operation, increases network flexibility and resource utilization, and lowers cost by leveraging the existing and mature Ethernet-based solutions for critical functions such as QoS, synchronization, and data security. The fronthaul architecture provides unified management and control mechanisms, common networking protocols, and universal network elements, thus facilitating migration to cloud-based mobile networks.

As shown in Fig. 1.36, the high-level architecture for transport network for the next-generation mobile systems is typically hierarchical and rigorously follows the physical OTN topology. In the reference architecture, the core network is where the packet core gateways are located. The metro aggregation network aggregates one or more metro ANs, which again aggregates one or more cell site or leaf transport networks. Ring network topologies are common due to their resilience properties; however, other topologies are also conceivable. The leaf networks are often point-to-point topologies. There is no single location for central units and BBU pools. Each of the larger transport network domains may have their own CU/BBU pool sites. The same also applies to DUs. For instance, a DU may be located in an evolved RRH, in an aggregation node connecting to multiple RRHs, or in a central

[47] IEEE 1914.1: Standard for packet-based fronthaul transport networks (http://sites.ieee.org/sagroups-1914/p1914-1/).

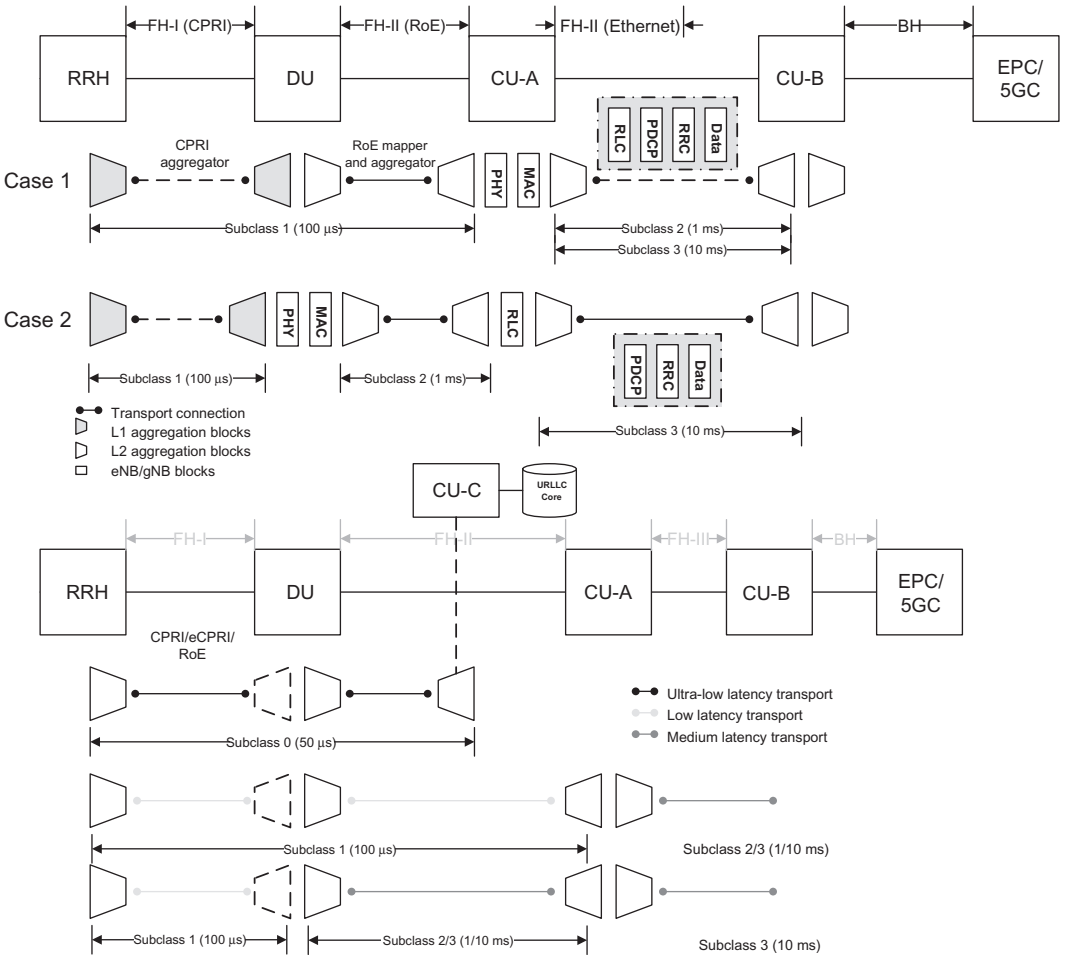


Figure 1.37
Next-generation fronthaul: CPRI-over-Ethernet for LTE and NR [78].

office. These networks must be able to transport 5G flows with heterogeneous traffic profiles. The traffic profiles may consist of traditional backhaul IP traffic, several different 3GPP functional split options traffic profiles, application traffic with varying latency needs, or non-IP CPRI TDM traffic. The transport network has to be able to serve all traffic profiles with vastly different service-level requirements in the same transport network infrastructure [78].

The transport network dedicated to 5G services is hierarchical, which means it comprises different domains and progressively aggregates signals from RRHs, at one end and up to the packet core at the other end. The support of multi-level functional split, results in a logical partitioning where more fronthaul segments and a backhaul segments may be identified. Fig. 1.37 depicts a generic model for converged fronthaul/backhaul network, where the

following segments are identified: Fronthaul-I (NGFI-I), connecting the RU to a DU; Fronthaul-II (NGFI-II), connecting the DU to a CU; and Backhaul (BH), connecting the CU to the packet core elements. The NGFI reference architecture assumes all network deployment scenarios can leverage the same transport network infrastructure. Fig. 1.37 illustrates a deployment scenario where both new and legacy radio technologies coexist in the same cell site. In essence, the same transport infrastructure has to serve legacy backhaul, legacy non-packet CPRI fronthaul, and the highly versatile 5G fronthaul incorporating multiple functional split options with varying traffic profiles. It is also possible to deploy multi-level functional splits between an RRH and a BBU pool, resulting in multiple fronthaul transport domains in the network. However, practical limitations limit the number of splits that can be supported. For instance, an RRH to the aggregating DU node connection may implement 3GPP functional split option 7, and the DU to the CU connection may subsequently implement 3GPP functional split option 2. Fig. 1.37 illustrates an example deployment with two functional splits between the RRH and the CU. Typically, the DU would be an aggregation node close to the radio access network edge, and possibly in charge of time- and latency-sensitive coordinated scheduling and MAC-level retransmission functions.

IEEE 1914.1 standard specifies a number of service classes corresponding to the characteristics of traffic being transported over the backhaul/fronthaul links in a C-RAN, which includes control information or user traffic. In particular, it defines dedicated subclasses providing requirements for maximum tolerable latency for mobile control, transport control, and synchronization signals. The data-plane (or user traffic) class is further divided into five different subclasses, each addressing a specific network application (e.g., 5G service transport or functional split options implemented between RRH, DU, and CU). More specifically, the very low-latency subclass addresses network segment supporting URLLC service; the low-latency subclass addresses network segment where 3GPP split options 6, 7, 8 are implemented, the medium-latency subclass addresses network segment where 3GPP split options 2, 3, 4, 5 are implemented, the high-latency subclass applies to functional split options 2 and 3 with longer transport distances, and the very high-latency subclass is applicable to functional split option 1 or legacy transport that connects the access and core networks with much longer transport distance.

Network slicing enables next-generation network to provide multiple type of services and applications with different service requirements under a common and shared physical network infrastructure. An NGFI-compliant transport network supports transport of the network slicing traffic and serves as a sub-network instance and resource manageable by the network slicing orchestrator. From architectural perspective, two operation modes may be defined depending on the level of transparency to the network slicing.

In slicing-agnostic transport mode, the NGFI deployment scenarios may coexist across multiple instances in the same transport network segment, potentially owing to variations in RAN node (RRU, DU, CU) locations that resulted from network slicing operation.

Therefore, it is possible that multiple classes of service be simultaneously enacted in a transport connection between two network nodes. The combined classes of service are logically presented in Fig. 1.38, which are supported by a slicing-agnostic transport network. The slicing-agnostic transport is able to provide multiple levels of transport service and to maintain different transport QoS based on the class of service requirement. It also performs transport key performance indicator (KPI) monitoring and reports the results to NGFI operation and maintenance (OAM), on the basis of classes of service. The transport network in this mode is not directly aware of the network slicing operation. Instead, it simply makes the classes of service available via its interface to the other network entities, where a slicing-to-classes of service mapping needs to be performed by aggregating the slicing traffic with similar KPI requirements. If RAN nodes that support the sliced services are not geographically co-located, this class of service may be routable to multiple destinations. Upon addition, deletion, or modification of the slicing operations, the slicing-agnostic transport is not expected to adapt to the change and to perform any reconfiguration process for optimization of the transport network.

In slicing-aware transport mode, while the user plane remains class of service based and the transport QoS is maintained at class of service level, a slicing-aware transport network interfaces with the network slicing orchestrator which is aware of the network slicing operation. Thus, the transport operation can be controlled and managed via the NGFI OAM configuration and provisioning functions for the purpose of network slicing optimization. As depicted in Fig. 1.38, the slice-to-class of service mapping is required to support class of service-based transport operation and is realized within the transport network and controlled by OAM configuration function that communicates with the network slicing orchestrator. This slice-to-class of service mapping correspondence is flexible by nature and should be dynamically or semi-dynamically reconfigured without service interruption. Furthermore, the transport OAM monitoring function reports the transport KPIs to the network slicing orchestrator, providing a means of feedback for integrated network optimization. Upon deletion, addition, or any modification of the network slicing services, the slice-aware transport adapts to the changes and performs seamless reconfiguration over the transport network for the purpose of overall network optimization. A slice-based transport that is fully optimized for network slicing should not be class of service-based where each slice traffic should be individually identified, labeled, and transported according to its own QoS requirements [78].

1.1.6.3 Backhaul Transport Options

The increasing demand for broadband wireless applications has a significant effect on the entire mobile infrastructure including the mobile backhaul network. In an operator's

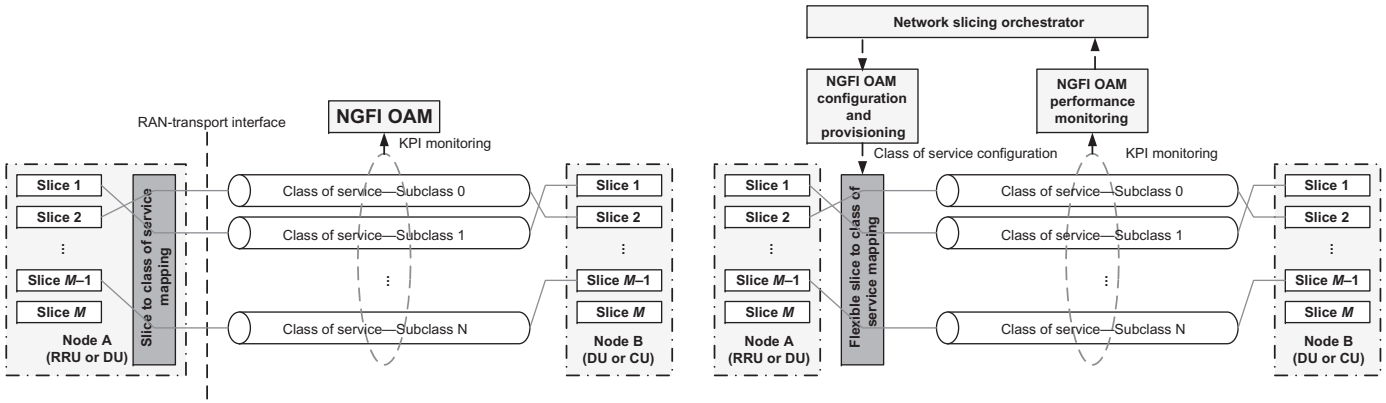


Figure 1.38
Comparison of slice-agnostic and slice-aware transports [78].

network, the mobile backhaul connects small and macro-cell sites to the core network that is further connected to external data centers serving content and applications. The RAN is an increasingly critical part of the global network infrastructure and is the primary reason that network operators are extremely focused on the mobile backhaul network as a key element of their short to long-term business strategies. Therefore the capacity, latency, reliability, and availability of mobile backhaul networks must improve as the wireless access data rates increase to enable video-centric and other broadband user applications. In addition, mobile backhaul networks support specific technologies that together ensure an acceptable quality of experience, which include network timing and synchronization as well as operations, administration, maintenance, and provisioning.

Recent technology advances and 4G/5G network deployments have created a new landscape in the access networks through integration of wireless and fiber technologies. In the past, the use and deployment of fiber links in the backhaul was slow compared to that of wireless backhaul schemes due to somewhat low data rate requirements of the backhaul supporting typically large cell sites. With the decreasing cost of fiber deployments and penetration of the fiber in the access networks as well as the demand of the latest wireless standards for smaller and higher bandwidth cells, the use of fiber connectivity has become more prevalent. Depending on the demarcation point between key network elements, one can decide whether fiber should be used only as a high data rate backhaul path or a transition to radio-over-fiber techniques can be afforded for the fronthaul links, as well. Backhaul traffic comprises a number of components in addition to the user-plane traffic. As the transport networks evolve, network operators are evaluating and, in some cases, have already started to deploy mobile fronthaul networks to support centralized RANs and ultimately C-RANs. In these networks, the BBU is moved from the cell site to a central location. This creates a new fronthaul network between the BBU and the cell site that has typically utilized CPRI protocol until just recently, which effectively carry digitized RF signals. These networks require fiber-based backhaul of Ethernet traffic from either the cell site or the BBU location, regardless of the last mile technology. The last mile could be the same Ethernet-over-fiber connection or Ethernet over some other media such as copper or microwave. As the cell topology changes from a traditional macro-cell to smaller cells, the requirements for the endpoint of the backhaul service typically become more stringent to meet certain deployment specifications such as temperature range, space, and power consumption. The performance of the underlying transport network must substantially improve in order to support the considerably tighter transport performance requirements in terms of frequency synchronization, phase synchronization, and latency. Since the performance of the backhaul networks is becoming more critical to end-to-end 5G services/applications, performance monitoring capabilities are imperative to ensure that the QoS requirements and service-level agreements are met (see Fig. 1.39).

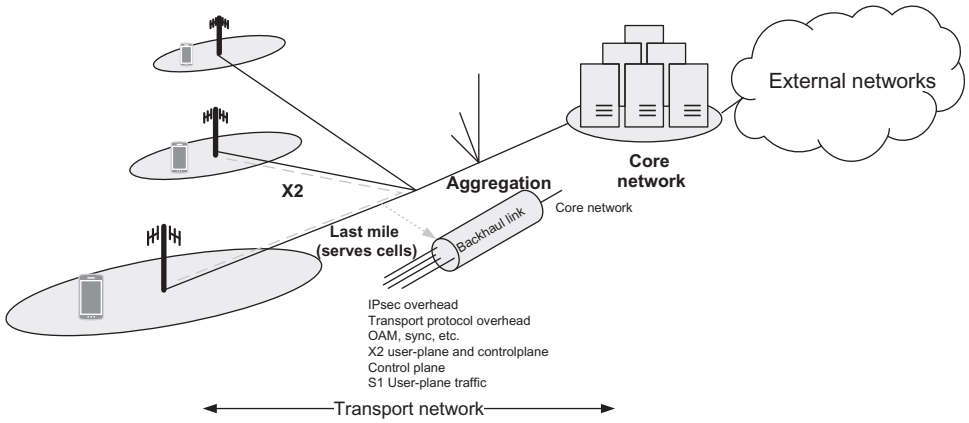


Figure 1.39
Illustration of backhaul components in a typical cellular network [66].

Mobile backhaul is an example application area where packet optical technology[48] enables the paradigm shift from traditional TDM-based backhaul to high performance, low cost, and scalable solutions that are currently required. Modern packet optical solutions enable the optimization of IP traffic between cell site gateways and core routers, avoiding unnecessary router hops. New generation of mobile backhaul supports Ethernet transport for all cell types and all locations regardless of last mile technology, whether CPRI-based fronthaul, DASs, fiber-connected small-cells or macro-cells, or fiber aggregation points supporting microwave backhaul in non-fiber environments are utilized. The use of frequency-division duplex scheme over the air-interface requires only simple frequency synchronization using SyncE or IEEE 1588v2 packet-based synchronization schemes. However, time-division duplex scheme requires phase synchronization, in which the network needs to track the phase of the synchronization signal and to receive accurate time-of-day timestamps. The more complex radio-access network features such as CoMP transmission and reception and eICIC further require phase synchronization.

Frequency synchronization is provided through a number of methods, where the most common solution is SyncE. It can also be provided in some regions using the global navigation

[48] Packet optical transport covers technologies and architectures that enable the transport of Internet protocol packets on both fixed and mobile optical networks. Converged products include the functional switching capability of wavelength division multiplexing schemes, Ethernet switching via various protocols, as well as time division multiplexing and optical transport network switching. The technologies include a combination of optical networking products that operate separately or within a single converged platform called packet optical transport system such as reconfigurable optical add-drop multiplexers, time division multiplexing, and carrier Ethernet switching products. These platforms reside in the metro edge, metro core, and the long-haul networks of major service providers.

satellite system (GNSS) methods such as global positioning system (GPS). Phase synchronization is provided using IEEE 1588v2 precision timing protocol. There are a number of ways in which good network performance can improve PTP quality within the base station. The use of network elements with low jitter has a positive impact on the quality of the received PTP by reducing errors. Furthermore, networks that support both SyncE and IEEE 1588v2 are able to operate in hybrid mode, with SyncE assisting the IEEE 1588v2 protocol for an improved overall performance. Inadequate synchronization has a negative impact on network performance, resulting in less efficient radio interface, poor performance for data traffic, and dropped calls.

Mobile backhaul is provisioned throughout the cellular network to transport voice and data traffic between the access and core networks. Wireless equipment in the radio access network includes macro-cell base stations, small-cell access points, and DASs. Wired and wireless transport mechanisms are the two types of mobile backhaul deployed across the RANs. With the emergence of heterogeneous networks, mobile backhaul has become a critical component in the 4G and 5G networks.

The cellular networks are evolving toward a heterogeneous architecture where different classes of small-cell base stations and DAS installations are coordinated, cooperating with macro-site base stations. A HetNet topology improves cellular network capacity and coverage to support the exponential growth in mobile traffic. Subsequently, HetNets can deliver ubiquitous connectivity to the mobile users with exceptional quality of experience. Backhaul is the confluence of mobile broadband users, small cells, DAS, macro-cells, and the core network. The emerging HetNet topologies have created a need for diverse wired and wireless mobile backhaul solutions. Small cells are being deployed in indoor and outdoor environments, on utility poles, and other urban structures. The sites can be located in private or public locations. Depending on the use case, each small-cell site has specific requirements for power sourcing, power budget, and backhaul transport. Meanwhile, the conventional macro-cell base stations will continue to increase network capacity, further driving demand for high-throughput backhaul.

Wireless backhaul, emerged as a cost-effective connectivity option, has many advantages relative to wired technologies, but wireless solutions also present unique design challenges among which are the need for spectrally efficient radio links, low operating power, small form factor, and environmentally resilient high-reliability equipment. RF analog integration also plays an important role. As an example, a typical microwave radio transmitter relies on RF analog integration and RF building blocks to reduce the size, lower the power, and improve the dynamic performance. A wireless backhaul equipment requires four key components: antennas, radio transceiver, modem, and interface. The antenna transmits and receives electromagnetic waves. The radio transceiver handles RF carrier frequency transformation to and from the baseband.

The modem performs channel coding/decoding and modulation/demodulation of the baseband signals, and the interface transports information between the radio and TDM/IP transport.

As shown in Fig. 1.40, wired and wireless backhaul solutions employ broadband technologies that vary in terms of physical media and access method. Wired backhaul physical media include copper wire, hybrid fiber-coaxial (HFC)[49] cable, and single-mode and multimode optical fiber. Transport access technologies are fractional-T/E carrier (T1/E1), digital subscriber line (DSL), pseudo-wire, Ethernet, WDM, and gigabit passive optical network.[50] The choice of wired backhaul is driven by the availability of physical media, cost, and capacity requirements. Wireless backhaul is needed when base stations do not have access to copper, HFC, or fiber transport. Wireless backhaul is also attractive when time to deployment is critical or when leasing costs are prohibitive. It is estimated that nearly 70% of worldwide LTE base station installations use wireless backhaul [80]. The methods of delivering wireless backhaul transport are LoS microwave, LoS millimeter wave, non-LoS (NLoS) sub-6 GHz microwave, broadband satellite links, and in-band or out-of-band relay nodes.

The HetNet architecture comprises four general classes of base station: (1) macro-cell, (2) metro-cell, (3) pico-cell, and (4) femto-cell. Table 1.2 compares the types of base station, deployment scenarios, and the set of possible wireless backhaul solutions. Wireless backhaul radios operate over a wide spectrum of licensed and unlicensed RF bands extending to 80 GHz (see Fig. 1.41). The RF spectrum for wireless backhaul ranges from sub-6 GHz NLoS to C/Ka/Ku-band microwave LoS, and Q/V/E-band mmWave LoS. Each RF band has spectrum restrictions, channel bandwidth limitations, and specific propagation characteristics. Channel bandwidth can vary from 5 to 160 MHz in NLoS systems; from 3.5 to 56 MHz in microwave LoS systems; or from 28 to 112 MHz and 250 MHz to 5 GHz in mmWave systems. All these specifications impact the type of modulation and carrier-to-noise ratio, and thereby mandating certain capacity trade-offs and maximum link distance.

Table 1.2 shows that backhaul throughput for each base station class must match the respective cell-site capacity. An optimal wireless backhaul solution further adapts the performance requirement with a particular deployment scenario. The method of wireless backhaul determines frequency band operation, radio design specifications, and the radio architecture.

[49] A hybrid fiber coaxial network is a telecommunication technology in which optical fiber cable and coaxial cable are used in different portions of a network to carry broadband content. An advantage of hybrid fiber coaxial is that some of the characteristics of fiber-optic cable (high bandwidth and low noise and interference susceptibility) can be brought close to the user without having to replace the existing coaxial cable that is installed at home or business.

[50] Gigabit passive optical network is a point-to-multipoint access network. Its main characteristic is the use of passive splitters in the fiber distribution network, enabling one single feeding fiber from the provider to serve multiple homes and small businesses. Gigabit passive optical network has a downstream capacity of 2.488 Gbps and an upstream capacity of 1.244 Gbps that is shared among users. Encryption is used to keep each user's data secured and private from other users [ITU-T G.984].

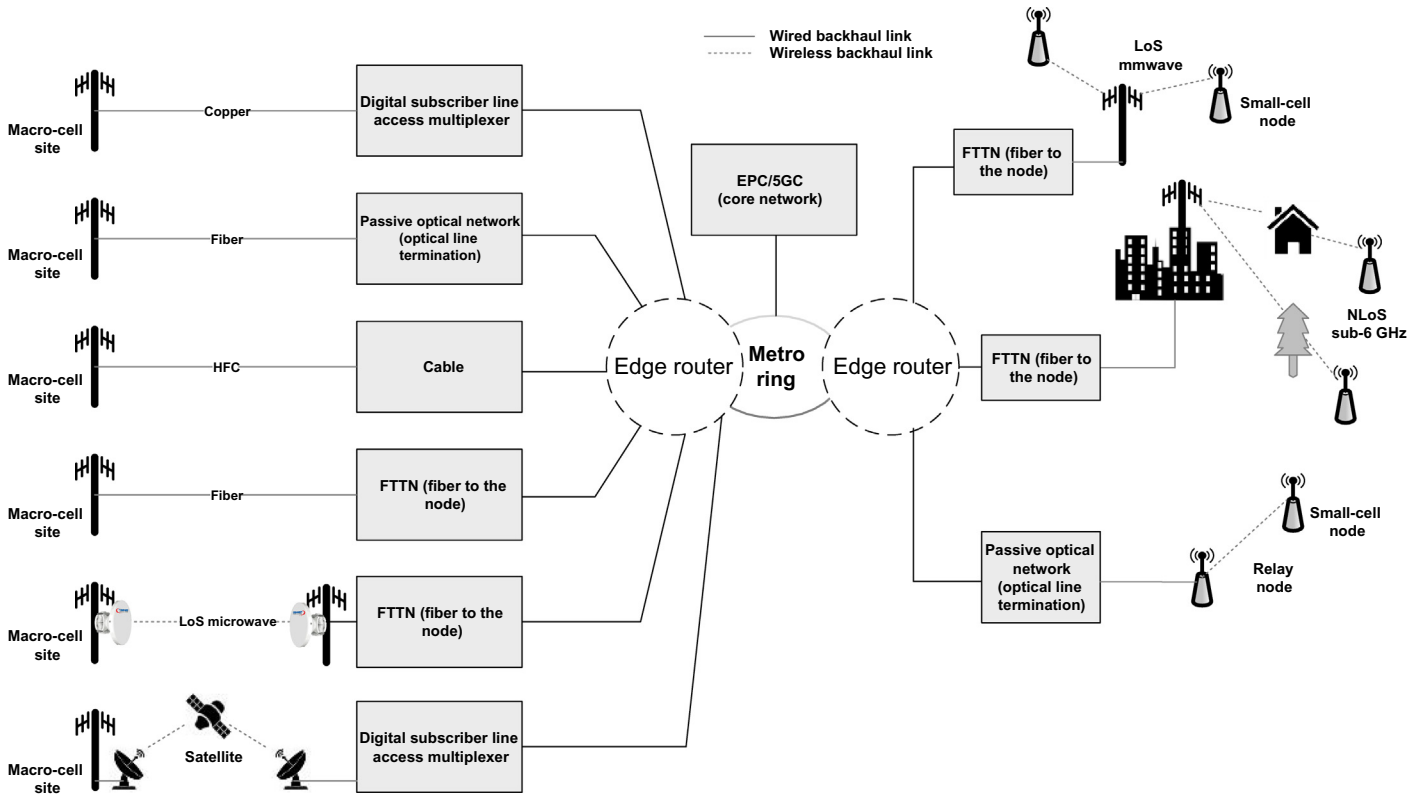


Figure 1.40

Illustration of mobile backhaul network physical media and access layer with macro-cell and small-cell base station [79].

Table 1.2: Example of LTE-advanced base stations and wireless backhaul solutions [79].

Base Station Type	Deployment Scenario	Number of Active Users	Cell Radius (km)	Power Amplifier Output Power (dBm)	Signal Bandwidth (MHz)	Number of Sectors/ Number of Antennas	Total Base Station Theoretical Capacity (Gbps)	Wireless Backhaul Scheme
Macro-cell	Outdoor	200–1000	>1	50	100	3 4×4	9	Microware, mmWave, VSAT
Metro-cell	Outdoor	200	<1	38	40	2 2×2	1.6	Microware, mmWave, VSAT
Pico-cell	Indoor/ outdoor	32–100	<0.3	24	20	1 2×2	0.8	mmWave, sub-6 GHz, relay
Femto-cell	Indoor	4–16	<0.1	20	10	1 2×2	0.4	Sub-6 GHz, relay

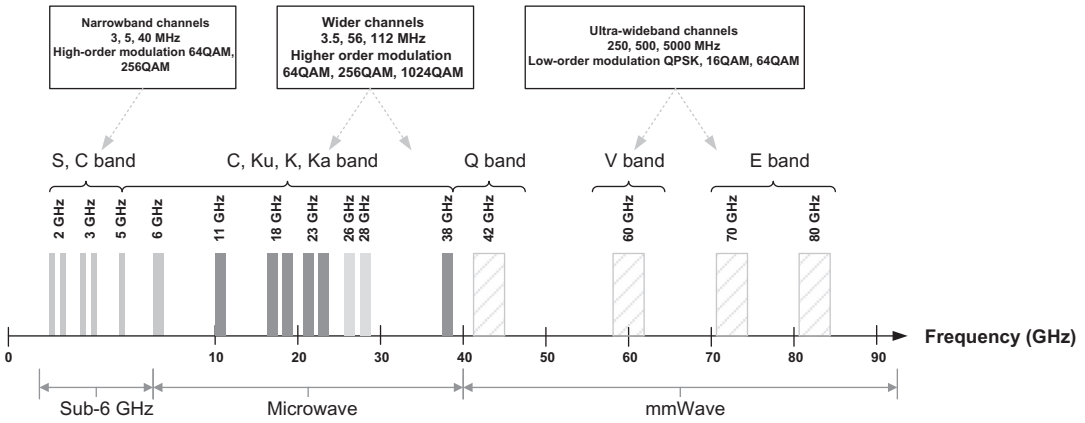


Figure 1.41
Frequency spectrum, channel bandwidth, and modulation considerations for RF bands [79].

Table 1.3 summarizes different characteristics for each wireless backhaul method and further outlines the key factors to be considered in backhaul selection.

Low-order modulation schemes such as QPSK can be used with wideband channels or for operation in poor atmospheric conditions with low SNR channel conditions. On the other hand, high-order modulation up to 2048 QAM can be used with narrowband channels or for operation in good channel quality and in clear atmospheric conditions. Depending on the link capacity requirements, deployment scenario, SNR, and atmospheric conditions, the data throughput can range from 100 Mbps to 10 Gbps. For macro-cell base station applications, the migration from indoor units to full outdoor units lowers the power, improves signal quality, and lowers OPEX. Macro-cells take advantage of full outdoor unit partition because RF loss in the waveguide or coaxial cable is minimized, or eliminated, which lowers RF power output and improves receiver input sensitivity. In small-cell base stations, the adoption of an integrated configuration means that systems can achieve a small footprint with lower equipment cost. Small cells benefit from an embedded partition because a single unit houses the wide and local area network connectivity, and wireless backhaul radio functions, resulting in reduced system size and simplified installation. Furthermore, since many small-cell deployments rely on E-band/V-band backhaul operating at 60−80 GHz, the RF losses associated with radio and antenna connections are significantly reduced.

Conventional point-to-point, LoS microwave systems operate in the licensed spectrum from C-band up to Ka-band. Common operating band frequencies are 6, 11, 18, 23, 26, and 38 GHz. These systems require unobstructed propagation. Fig. 1.42 illustrates a point-to-point microwave backhaul link connecting a macro-cell base station node to an aggregation node. For small-cell base station applications some microwave equipment vendors have demonstrated NLoS operation using conventional LoS microwave bands, leveraging high antenna gains with

Table 1.3: Wireless backhaul options and associated parameters [79].

Backhaul Type	NLoS/ LoS	PTP/ PMP	Frequency Band	Licensed/ Unlicensed	Channel Bandwidth (MHz)	Modulation	Range (km)	Latency (ms)	Single-Channel Capacity (Gbps)	Application	Notes
Microwave	LoS	PTP/ PMP	C, Ku, Ka	Licensed	3.5/7/14/ 28/56 10/20/30/ 40/50	QPSK 16−2048QAM	<10	<0.2	0.5	Macrocell small-cell aggregation	High reliability and high capacity links
mmWave	LoS	PTP/ PMP	Q	Licensed	28/56/112	QPSK 16−2048QAM	–	<0.05	0.3−10	Macrocell small-cell aggregation	Narrow beams and oxygen absorption to improve frequency reuse in V band
		PTP	E	Unlicensed	>250	QPSK	<4				
		PTP	V	Lightly licensed	250−5000	16QAM, 64QAM	≪1				
VSAT	LoS	PTP	C, Ku, Ka	Licensed	26/33/50/ 72/500	QPSK, 8PSK, 32ASK	>10	<120 (medium earth orbit) <330 (GEO)	<1	Small cell	Remote and rural areas with no infrastructure
Sub-6 GHz	NLoS/ LoS	PTP/ PMP	S, C	Licensed/ unlicensed	5/10/20/ 40/80/160	64QAM,256QAM	1 (NLoS) 10 (LoS)	<12	0.5	Metro-cell, picocell, femtocell	Fast deployment and unpredictable capacity
In-band relay	NLoS	PTP	LTE bands 1−43	Licensed	5/10/15/ 20/40	64QAM	<10	>10	–	Picocell, femtocell	Occupies cellular spectrum and adds latency

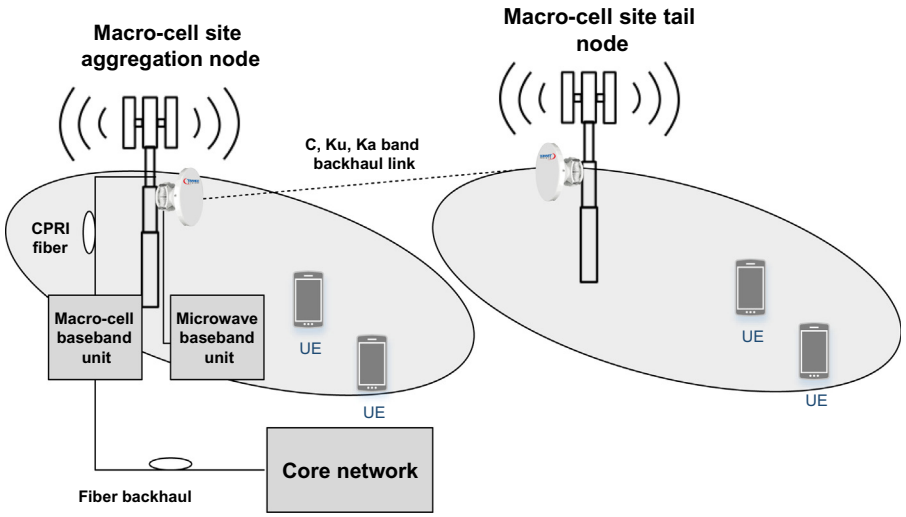


Figure 1.42
A point-to-point LoS microwave link with a relay node and aggregation node [79].

operating guidelines for the electromagnetic wave propagation effects such as diffraction, reflection, and penetration to overcome the additional path loss as a result of NLoS operation.

In clear weather conditions when radio-link SNR is high, the spectral efficiency and throughput are increased by employing higher order QAM constellations such as 256QAM, 1024QAM, or even 4096QAM. In poor weather conditions as SNR degrades, the modulation order can be lowered to 16QAM or QPSK to ensure operational link for high-priority data but at reduced throughput. However, shifting to higher order QAM constellations yields a point of diminishing returns in terms of throughput gained versus added cost, RF transmitter power utilized, required RF signal-chain linearity, and higher dynamic range. With each increase in modulation order, 3–4 dB increase in SNR or transmitter power is needed; however, with each increase in modulation order the throughput only improves by about 10%.

Co-channel dual polarization (CCDP) utilizes cross-polarization interference cancelation (XPIC)[51] to double the link capacity over the same channel. CCDP-XPIC allows simultaneous transmission of two separate data streams on the same frequency. Data is transmitted

[51] Cross-polarization interference cancelation is an algorithm to suppress mutual interference between two received streams in a polarization-division multiplexing communication system. The cross-polarization interference canceler is a signal processing technique implemented on the demodulated received signals at the baseband level. This technique is typically necessary in polarization-division multiplexing systems where the information to be transmitted is encoded and modulated at the system's symbol rate and upconverted to an RF carrier frequency, generating two (orthogonally polarized) radio streams radiated by a single dual-polarized antenna. A corresponding dual-polarized antenna is located at the remote receiver site and connected to two RF receivers, which down-convert and later combine the radio streams into the baseband signal.

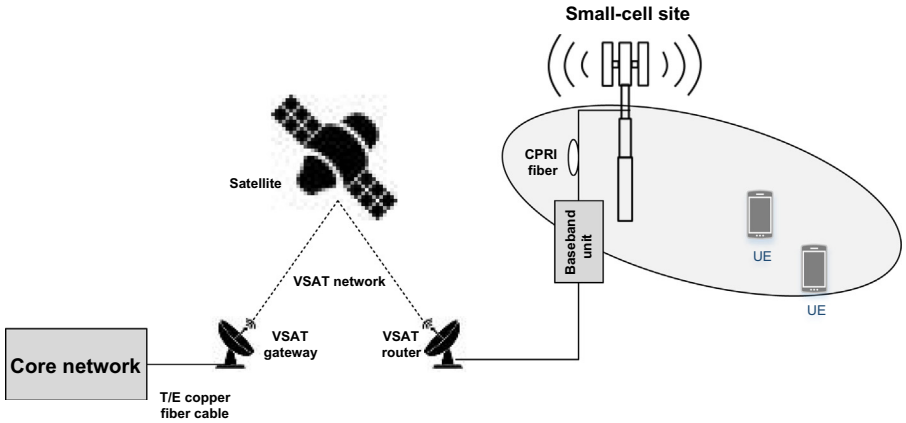


Figure 1.43
Illustration of an example satellite backhaul [79].

on orthogonal antenna polarizations (vertical and horizontal) and cross-polarization interference is canceled using digital signal processing. Spatial multiplexing significantly improves spectral efficiency and uses multi-antenna techniques to send multiple data streams over the same RF channel. A 2×2 MIMO link can ideally double the capacity. Spatial multiplexing has been used in many wireless access technologies including LTE/NR and IEEE 802.11n/ac/ax, which relies on multipath interference and exploits spatial propagation paths caused by reflections. However, an LoS microwave link does not exhibit multipath phenomenon, thus a multipath condition is simulated by deliberate separation of the antennas, thereby creating a pseudo multipath condition. While it is evident that high-density RF analog integration is important to reduce the size and lower the component count, there are still many radio functions that rely on [discrete] RF building blocks. The IF circuitry and frequency up/down conversion require several key analog functions including phase-locked loop (PLL)[52] frequency synthesizer, and the variable gain amplifier (VGA).

Commercial satellite systems use very small aperture terminals (VSAT) for cost-effective delivery of telephony, broadband access, and video content. VSAT systems are deployed in enterprise-grade private networks, consumer broadband services, and cellular base station backhaul. In cellular base station backhaul applications, VSAT systems are ideal for remotely located small-cell sites. Fig. 1.43 shows a typical VSAT system used in a base station backhaul application. Router and gateway VSAT

[52] A phase-locked loop is a control system that generates an output signal whose phase is related to the phase of an input reference signal. There are several different phase-locked loop types, but the simplest form is an electronic circuit consisting of a variable frequency oscillator and a phase detector in a feedback loop. The oscillator generates a periodic signal, and the phase detector compares the phase of that signal with the phase of the input reference signal, adjusting the oscillator frequency to maintain phase matching.

terminals are ground-based units with a two-way communication link to C/Ka/Ku-band satellites. The satellites can be geostationary or geosynchronous equatorial orbit, medium earth orbit, or low earth orbit. Orbiting satellites are powered by a finite energy source; therefore they are energy-constrained and a satellite downlink channel has limited transmitter power. The link is also susceptible to atmospheric loss because geosynchronous satellites orbit at 35,786 km from ground-level terminals. As a result, the radio link operates with a very low SNR. To achieve the desired data throughput with acceptable BER at low SNR, VSAT systems use wide-channel bandwidths with relatively low-order modulation schemes such as QPSK or 8PSK and low coding rates. Microwave and broadband satellite backhaul are two common wireless technologies deployed across the RAN. As the base station capacity and throughput increase to support growing mobile data demand, backhaul capacity must increase. Similarly, as base station size and power decrease, the backhaul solutions must become smaller and more efficient. As such, wireless backhaul systems will continue relying on RF analog integration and RF building block solutions to achieve high spectral efficiency, smaller form factor, and lower operating power.

1.1.7 Mobile Edge Computing

MEC or multi-access edge computing is an emerging 5G technology which enables provisioning of cloud-based network resources and services (e.g., processing, storage, and networking) at the edge of the network and in the proximity of the users. The edge may refer to the base stations themselves and/or data centers close to the radio network possibly located at the aggregation points. The end-to-end latency perceived by the mobile user can be significantly reduced using the MEC platform, which is a key enabling factor for many 5G services such as the tactile Internet. MEC supports different deployment scenarios, and the MEC servers can be located at different locations within the radio access network depending on technical and business requirements. Applications and analytics at the MEC server will not be impacted by congestion in other parts of the network. By performing analytics or caching content at the MEC server, the volume of data transmitted to the core network for processing is reduced, and the impact on the data traffic through the network is minimized, resulting in more efficient use of existing network bandwidth. This establishes an ultra-low-latency environment capable of providing mission-critical and real-time services. The user location information can be used by applications and services hosted by the MEC server to offer location/context-related services to the subscribers. Since these applications and services are found at the edge of the network instead of within a centralized cloud, responsiveness can be improved, resulting in an enriched quality of experience for the user.

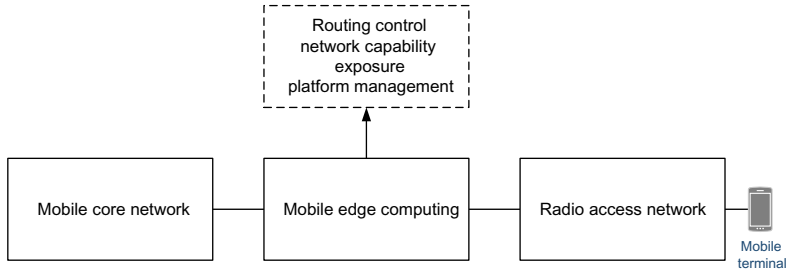


Figure 1.44
Conceptual MEC architecture [48].

Established in December 2014, the ETSI Industry Specification Group (ISG)[53] on MEC has produced normative specifications that enable the hosting of third-party applications in a multi-vendor environment. The initial scope of the ISG MEC was to focus on use cases, and to specify the requirements and the reference architecture, including the components and functional elements that were the key enablers for MEC solutions. The work has continued on platform services, APIs, and interfaces. The MEC platform API is application-agnostic and allows smooth porting of value-creating applications on every mobile-edge server with guaranteed service-level agreement.

The main functions in the MEC platform include routing, network capability exposure, and management (see Fig. 1.44). The routing entity is responsible for packet forwarding among the MEC platform, radio access network, and the mobile core network, as well as within the MEC platform. The network capability exposure entity enables the authorized exposure of the radio network information service and the RRM. The management entity supports the authentication, authorization, and accounting and management of the third-party applications in the MEC platform. This section presents the architectural description of the MEC platform as well as main applications and key functionalities enabling this technology.

1.1.7.1 Service and Deployment Scenarios

The primary objective of multi-access edge computing is to reduce network congestion and to improve application performance by processing the corresponding tasks in the proximity of the users. Furthermore, it intends to improve the type and delivery of the content and applications to those users. The use cases already being realized include augmented reality and virtual reality, which both benefit from fast response times and low-latency

[53] ETSI multi-access edge computing (http://www.etsi.org/index.php/technologies-clusters/technologies/multi-access-edge-computing).

communications; connected cars, which also thrive in high-bandwidth, low-latency, highly available settings; and industrial/residential IoT applications that rely on high performance and smart utilization of network resources. Large public and enterprise locations are also beneficiaries of MEC. In large-scale situations where localized venue services are important, content is delivered to onsite consumers from a MEC server located at the venue. The content is locally stored, processed, and delivered, not requiring information transport through a backhaul or centralized core network. Large enterprises are also increasingly motivated to process user traffic locally rather than backhaul traffic to a central network, using small-cell networks instead [48]. As shown in Fig. 1.45, edge computing use cases may be classified into two major categories, that is, third-party applications and operator applications.

The MEC ecosystem is likely to bring significant benefit to the mobile operators and other industries as well as to the consumers that will be able to experience services which need to rely on very accurate localization or high performance in terms of latency and throughput. In other words, MEC will be able to support new IoT services that would not be technically or economically feasible without 5G networks. Several use cases are addressed by MEC and also currently considered as part of next-generation mobile networks. Security and safety have been among the most important verticals for IoT. The advances in technology with an ever-increasing amount of information collected from sensors and high-resolution video cameras create the need for a scalable, flexible, and cost-effective solution to analyze the content in real time. MEC can host the analytics applications close to the source and enable increased reliability, better performance, and significant savings by locally processing large volume of data.

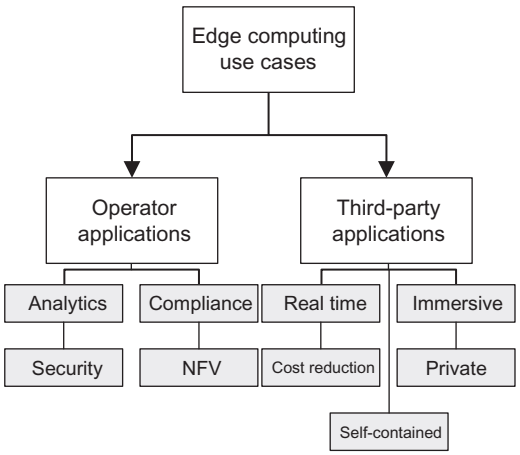


Figure 1.45
MEC use cases [45,48].

The automotive sector is another area where the new technologies are revolutionizing the industry. Self-driving cars have been already demonstrated by both traditional automotive and new Internet players, and it is anticipated to make the first autonomous cars commercially available in 2020+. While the work on future 5G systems is currently being conducted by various organizations around the globe, the digitalization in the automotive industry is clearly reflected in the use cases and the requirements coming from this sector. The IoT is a key driver for the next-generation technology and most of the use cases appear to focus on the connected cars. With the next-generation system, the latency requirements are set to less than 1 ms to empower a wide range of use cases. MEC is the ideal solution and has been identified as a key component to support these ultra-low latency scenarios as it enables hosting applications close to the users at the edge cloud and therefore provides the shortest path between the applications and the servers.

Computationally intensive applications running on mobile terminals may be offloaded to the cloud for various reasons, such as availability of more computing power or of specific hardware capabilities, reliability, joint use of the resources in collaborative applications, or saving network capacity. The computation offload is particularly suitable for IoT applications and scenarios where terminals have limited computing capabilities, to guarantee longer battery life. Such offload may happen statically (server components are deployed by the service provider proactively in advance) or dynamically (server components are deployed on demand by request from the UE). In this case, applications benefit from the low delay provided by the MEC.

1.1.7.2 Architectural Aspects

MEC provides a highly distributed computing environment that can be used to deploy applications and services as well as to store and process content in close proximity of the mobile users. Applications can also be exposed to real-time radio and network information and can offer a personalized and contextualized experience to the mobile subscriber. This translates into a mobile broadband experience that is not only more responsive but also opens up new business opportunities and creates an ecosystem where new services can be developed in and around the base station.

Fig. 1.46 shows the high-level functional entities in the MEC framework, which are further grouped into the system-level, host-level, and network-level entities. The host-level group consists of the MEC host and the corresponding MEC host-level management entity. The MEC host is further split to include the MEC platform, applications, and the virtualization infrastructure. The network-level group consists of the corresponding external entities that are 3GPP radio access networks, the local networks, and the external networks. This layer represents the connectivity to local area networks, cellular networks, and external networks such as the Internet. Above everything is the MEC system-level management that by

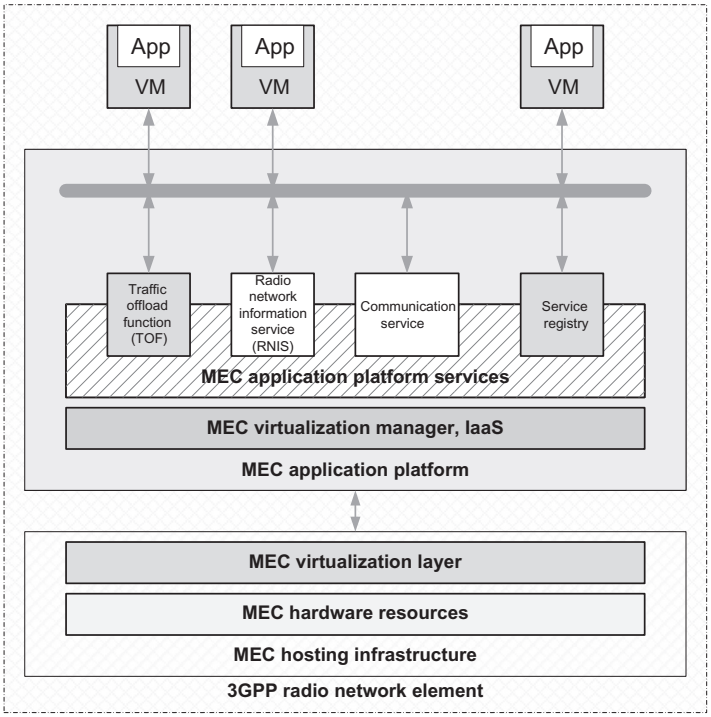


Figure 1.46
Overview of ETSI MEC [46].

definition has the overall visibility to the entire MEC system. The MEC system consists of the MEC hosts and the MEC management necessary to run MEC applications within an operator network or a subset of an operator network [53].

An in-depth understanding of the MEC systems can be attained from the reference architecture depicted in Fig. 1.47, which defines the functional entities and their relationships. The reference architecture follows the earlier described functional grouping of the general framework and includes system-level and host-level functions; however, the network-level functional group is not visible because there are no MEC-specific reference points needed to access those entities. The MEC host is an entity consisting of the MEC platform and the virtualization infrastructure that provides computing, storage, and network resources for the MEC applications. In addition, the MEC host can provide storage and ToD information for the applications. The virtualization infrastructure includes a data plane that executes the forwarding rules received by the MEC platform and routes the traffic between the applications, services, and networks. The MEC server provides computing resources, storage capacity, connectivity, and access to user traffic and radio and network information.

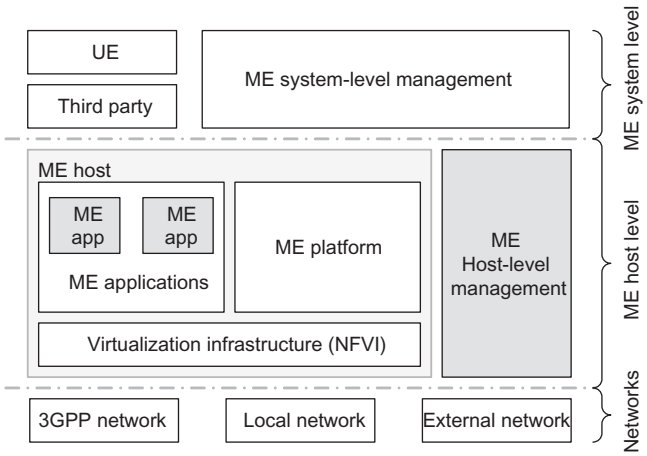


Figure 1.47
MEC general framework [46].

The MEC platform represents a collection of baseline functionalities that are required to run applications on a particular MEC host and to enable MEC applications to discover, advertise, offer, and exploit the MEC services. MEC services can be provided by the platform and by the applications, where both the platform and applications may utilize MEC services. The baseline functionalities of the MEC platform are needed to navigate the traffic between the applications, services, and networks. The MEC platform receives the traffic forwarding rules from the MEC platform manager, MEC applications, and MEC services, and based on those criteria, as well as policies, it provides the instructions to the forwarding plane.

The reference architecture shows the functional elements that comprise the mobile edge (ME) system and the reference points between them. Fig. 1.48 depicts the ME system reference architecture. There are three groups of reference points defined between the system entities as follows [46]:

1. Reference points related to ME platform functionality (Mp)
2. Management reference points (Mm)
3. Reference points interfacing with external entities (Mx)

The MEC applications run as VMs on top of virtualization infrastructure provided by the MEC host. The applications interact with the MEC platform over an Mp1 reference point to utilize the services offered by the platform. The MEC platform manager is a host-level entity that is further split into MEC platform element management, MEC application life cycle management, and MEC application rules and requirements management functions. The application life cycle management consists of application instantiation and termination procedures as well as providing indication to the MEC orchestrator on application-related

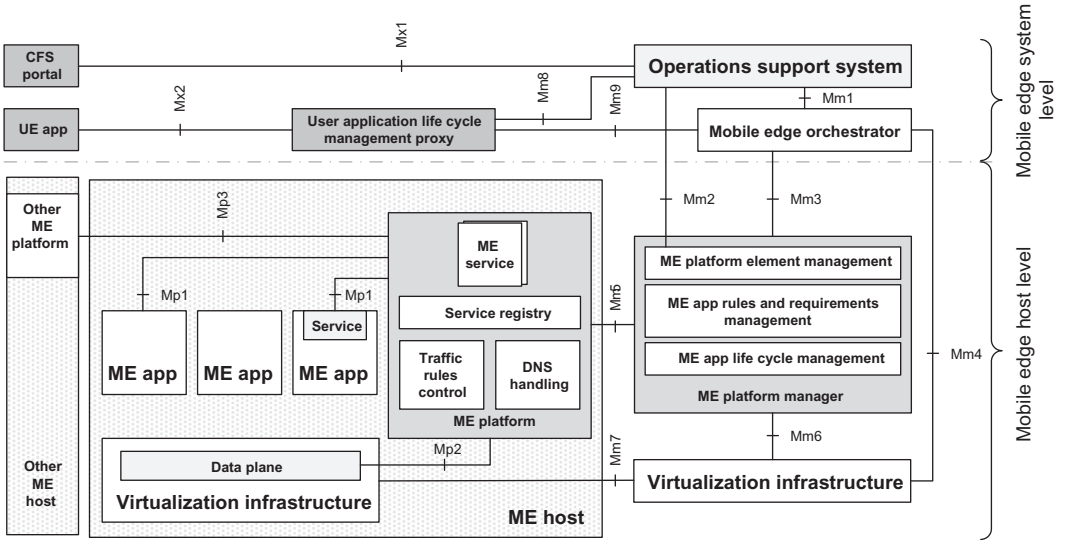


Figure 1.48
MEC reference architecture [46].

events. The MEC orchestrator is the central function in the MEC system that has visibility over the resources and capabilities of the entire MEC network. The MEC orchestrator maintains information on the entire MEC system, the services and resources available in each host, the applications that are instantiated, and the topology of the network. The orchestrator is also responsible for managing the MEC applications and the related procedures by integrating the applications, checking the integrity and authenticity of the application, validating the policies for the applications, and maintaining a catalog of the applications that are available.

The MEC applications may indicate their requirements for the resources, services, location, and performance, such as maximum allowed latency, and it is the MEC orchestrator's responsibility to ensure that their requirements are satisfied. The orchestrator uses the requirements received from the applications in the selection process for the target MEC host. The reference point toward the VIM is used to manage the virtualized resources of the MEC host and to manage the application images that are provided for instantiation. It is further used for maintaining status information on available resources. The operations support system of an operator is a function that is widely used to manage various services and subsystems in the operators' network. The reference point between the MEC orchestrator and VIM is used for management of the application images and the virtualized resources as well as for monitoring the availability of the resources.

The customer-facing service (CFS) acts as an entry point for a third-party application. This portal can be used for operations to manage the provisioning, selection, and ordering of the

MEC applications. The user application life cycle management proxy is a function that the MEC-related clients and applications use to request services related to onboarding, instantiation, and termination of the applications. This proxy can be used to request transfer of the application from the MEC system to the external cloud or to the MEC system from the external cloud. More specifically, the ME system-level management includes the ME orchestrator as its core component, which has an overall view of the complete ME system. The ME host-level management comprises the ME platform manager and the VIM, which handles the management of the ME-specific functionality of a particular ME host and the applications running on it. The ME host is an entity that contains the ME platform and a virtualization infrastructure which provides compute, storage, and network resources for the ME applications. The virtualization infrastructure includes a data plane that executes the traffic rules received by the ME platform, and routes the traffic among applications, services, DNS server/proxy,[54] 3GPP network, local networks, and external networks.

The ME platform is responsible for offering an environment where the ME applications can discover, advertise, consume, and offer ME services, including ME services available via other platforms; receiving traffic rules from the ME platform manager, applications, or services; and instructing the data plane. This includes the translation of tokens representing UEs in the traffic rules into specific IP addresses, receiving DNS records from the ME platform manager, configuring a DNS proxy/server, hosting ME services, and providing access to persistent storage and ToD information. The ME applications run as VMs on top of the virtualization infrastructure provided by the ME host, and can interact with the ME platform to utilize and provide ME services. Under certain conditions, the ME applications can also interact with the ME platform to perform certain support procedures related to the life cycle of the application, such as indicating availability, preparing relocation of user state, etc. The ME applications can have a certain number of rules and requirements associated with them such as required resources, maximum latency, required or useful services, etc. These requirements are validated by the ME system-level management and can be assigned to default values if not provided.

The ME orchestrator is the core functionality in ME system-level management. The ME orchestrator is responsible for maintaining an overall view of the ME system based on deployed ME hosts, available resources, available ME services, and topology; on-boarding

[54] Domain name system is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. It translates readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. A domain name system proxy improves domain lookup performance by caching previous lookups. A typical domain name system proxy processes domain name system queries by issuing a new domain name system resolution query to each name server that it has detected until the hostname is resolved.

of application packages, including checking the integrity and authenticity of the packages, validating application rules and requirements, and if necessary adjusting them to comply with operator policies, keeping a record of on-boarded packages, and preparing the VIM(s) to handle the applications; selecting appropriate ME host(s) for application instantiation based on constraints such as latency, available resources, and available services; triggering application instantiation and termination; and triggering application relocation as needed when supported.

The operations support system shown in Fig. 1.48 refers to the OSS of an operator. It receives requests via the CFS portal and from UE applications for instantiation or termination of applications and decides whether to grant these requests. Granted requests are forwarded to the ME orchestrator for further processing. The OSS also receives requests from UE applications for relocating applications between external clouds and the ME system. A user application is an ME application that is instantiated in the ME system in response to a request of a user via an application running in the UE. The user application life cycle management proxy allows UE applications to request on-boarding, instantiation, termination of user applications, and relocation of user applications in and out of the ME system. It also allows informing the UE applications about the state of the user applications. The user application life cycle management proxy authorizes requests from UE applications in the UE and interacts with the OSS and the ME orchestrator for further processing of these requests. The user application life cycle management proxy is only accessible from within the mobile network. It is only available when supported by the ME system.

The VIM is responsible for managing the virtualized resources for the ME applications. The management tasks consist of allocating and releasing virtualized computing, storage, and network resources provided by the virtualization infrastructure. The VIM also prepares the virtualization infrastructure to run software images, which can also be stored by the VIM for a faster application instantiation. Since it is possible for virtualized resources to run out of capacity or to fail in operation, it is important to closely monitor them. The VIM provides support for fault and performance monitoring by collecting and reporting information on virtualized resources and providing the information to server and system-level management entities. The VIM has a reference point toward the virtualization infrastructure to manage the virtualized resources.

The ME reference architecture shown in Fig. 1.48 incorporates the following reference points [46]:

- Mp1 is a reference point between the ME platform and the ME applications that provides service registration, service discovery, and communication support for services. It also enables other functionalities such as application availability, session state relocation support procedures, traffic rules and DNS rules activation, access to persistent storage and ToD information, etc.

- Mp2 is a reference point between the ME platform and the data plane of the virtualization infrastructure and is used to instruct the data plane on how to route traffic among applications, networks, services, etc.
- Mp3 is a reference point between the ME platforms and is used for controlling communication between ME platforms.

Reference points related to the ME management

- Mm1 is a reference point between the ME orchestrator and the OSS that is used for triggering the instantiation and the termination of ME applications in the ME system.
- Mm2 is a reference point between the OSS and the ME platform manager that is used for the ME platform configuration, fault detection, and performance management.
- Mm3 is a reference point between the ME orchestrator and the ME platform manager and is used for the management of the application life cycle, application rules and requirements, and keeping track of available ME services.
- Mm4 is a reference point between the ME orchestrator and the VIM which is used to manage virtualized resources of the ME host including maintaining track of available resource capacity and managing application images.
- Mm5 is a reference point between the ME platform manager and the ME platform and is used to perform platform configuration, configuration of the application rules and requirements, application life cycle support procedures, management of application relocation, etc.
- Mm6 is a reference point between the ME platform manager and the VIM which is used to manage virtualized resources and to realize the application life cycle management.
- Mm7 is a reference point between the VIM and the virtualization infrastructure that is used to manage the virtualization infrastructure.
- Mm8 is a reference point between the user application life cycle management proxy and the OSS and is used to handle UE requests for running applications in the ME system.
- Mm9 is a reference point between the user application life cycle management proxy and the ME orchestrator of the ME system and is used to manage ME applications requested by UE application.

Reference points related to external entities

- Mx1 is a reference point between the OSS and the CFS portal and is used by a third party to request the ME system to run applications in the ME system.
- Mx2 is a reference point between the user application life cycle management proxy and the UE application, which is used by a UE application to request the ME system to run an application in the ME system, or to move an application in or out of the ME system. This reference point is only accessible within the mobile network. It is only available when supported by the ME system.

The ME computing and NFV are complementary concepts that can exist independently. The ME architecture has been designed in such a way that a number of different deployment options of ME systems are possible. An ME system can be realized independent of an NFV environment in the same network, or can coexist with that environment. Since both MEC and NFV are based on the use of virtualization concept, the MEC applications and VNFs can be fully or partially instantiated over the same virtualization infrastructure. The MEC reference architecture reuses the concept of a VIM similar to that of the VIM of NFV framework. Multiple scenarios for deployments are possible, depending on operators' preferences for their networks and their network migration plans. The relationship between MEC and NFV-MANO components is an important aspect of integrated MEC/NFV deployments.

In 5G networks, there are three types of session and service continuity (SSC) modes. Different SSC modes can guarantee different levels of service continuity. As shown in Fig. 1.49, SSC mode 1 maintains the same UPF. In SSC mode 2, the network may trigger the release of the PDU session and instruct the UE to establish a new PDU session to the same data network immediately. Upon establishment of the new PDU session, a new UPF acting as PDU session anchor can be selected. In SSC mode 3, the network allows the establishment of UE connectivity via a new UPF to the same application server before connectivity between the UE and the previous UPF is terminated. Different applications have different service and session continuity requirements. Therefore, in order to achieve efficient control of MEC APPs with different SSC mode requirements in 5G network, the coordination between ME APPs on the ME host and the 5G network, for example, how to indicate the SSC mode requirement of an ME APP to the 5G network, must be carefully considered.

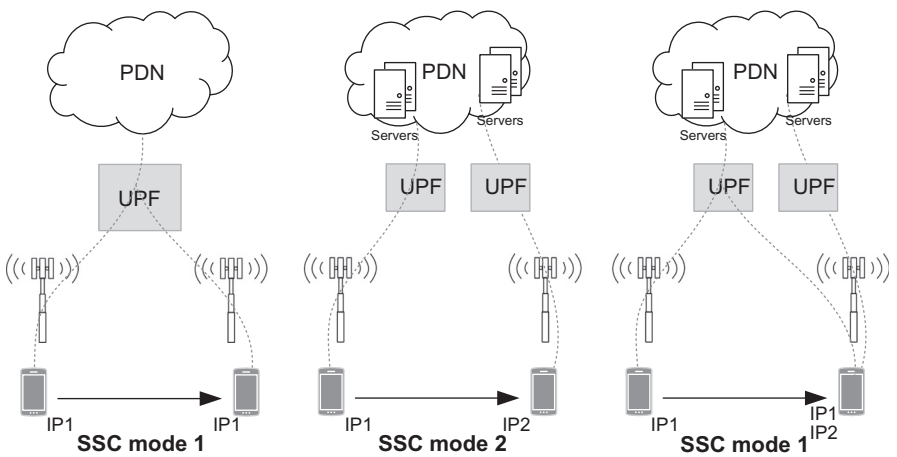


Figure 1.49
SSC modes [3,4].

A large part of the functionality providing data connectivity is for supporting flexible deployment of application functions (AFs) in the network topology as needed for edge computing, which is supported via the three different SSC modes or via the functionality of uplink classifiers and branching points. The SSC modes include the traditional SSC 1 mode, where the IP anchor remains stable to provide continuous support of applications and to maintain the path toward the UE as its location is updated. The new modes allow relocating the IP anchor. There are two options, make-before-break (SSC mode 3) and break-before-make (SSC mode 2). The architecture enables applications to influence selection of suitable data service characteristics and SSC modes. Given that 5G network deployments are expected to serve extremely large amount of mobile data traffic, an efficient user-plane path management is critical. The system architecture defines in addition to the SSC modes the functionality of uplink classifiers and branching points to allow breaking out and injecting traffic selectively to and from AFs on the user plane path before the IP anchor. Also, as permitted by policies, AFs may coordinate with the network by providing information relevant for optimizing the traffic route or may subscribe to 5G system events that may be relevant for applications [3,4].

1.1.8 Network Sharing

A network sharing architecture allows multiple participating operators to share resources of a single shared network according to agreed allocation terms. The shared network includes a RAN. The shared resources include radio resources of that network. The shared network operator allocates shared resources to the participating operators based on their plans and current needs and according to service-level agreements. A UE that has a subscription to a participating network operator can select the participating network operator while within the coverage area of the shared network and to receive subscribed services from the participating network operator. 3GPP laid out two approaches to sharing a RAN, which are illustrated in Fig. 1.50, where they primarily differ in the core network aspects. In multi-operator core network (MOCN) approach, each network operator has its own core network. Maintaining a strict separation between the core network and the radio network has a number of benefits related to service differentiation, interworking with legacy networks, fall back to circuit-switched voice services, and the support of roaming. Alternatively, in the gateway core network (GWCN) approach, the network operators also share the mobility management entity of the core network, which is responsible for bearer management and connection management between the mobile terminal and the network. The GWCN approach enables additional cost savings compared to the MOCN approach, but it is relatively less flexible, potentially reducing the level of differentiation among the participating operators. 3GPP Rel-15 supports MOCN network sharing architecture, in which only the RAN is shared in the 5G system. However, RAN and AMF support for operators that use more than one PLMN ID is required [3].

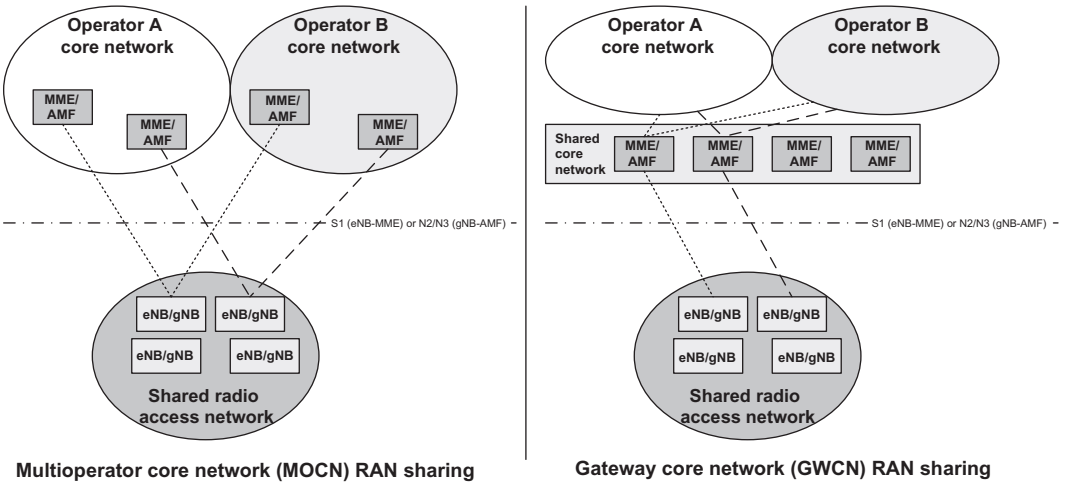


Figure 1.50
3GPP-defined network sharing architecture options [34].

In each case, the network broadcasts system information and supports signaling exchanges that allow the UE to distinguish between up to six different sharing network operators, to obtain service or to perform handover, with no consideration of the underlying network sharing arrangement. As network sharing becomes a central feature of mobile network operation, there is a need to address a wide variety of technical, commercial, and regulatory requirements. Among other things, there is an interest in pooling spectrum, sharing resources asymmetrically and dynamically based on financial considerations and load, and the ability for participating operators to manage and control the use of resources independently. If a shared NG-RAN is configured to indicate the available core network operators to the UEs for selection, each cell in the shared RAN would then include the PLMNs related to the available core network operators in the shared network in the broadcast system information. The broadcast system information provides a set of PLMN IDs and optionally one or more additional set of parameters per PLMN such as cell-ID, tracking areas (TAs), etc. All UEs compliant with the 5G system attempting to connect to NG-RAN must support reception of the basic and additional set of PLMN IDs. The available core network operators must be the same for all cells of a TA in a shared NG-RAN network. The UE decodes the broadcast system information and takes the information concerning the available PLMN IDs into account in the network and cell (re-)selection procedures.

A UE that has a subscription to a participating operator in a network sharing scenario must be able to select this participating network operator while present within the coverage area of the shared network and to receive subscribed services from the participating network operator. Each cell in the shared NG-RAN must include the PLMN-IDs corresponding to the available core network operators in the shared network in the broadcast

system information. When a UE performs an initial access to a shared network, one of the available PLMNs is selected to serve the UE. The UE uses all received broadcast PLMN-IDs in its PLMN (re)selection processes and informs the NG-RAN of the selected PLMN so that the NG-RAN can properly route its traffic. After initial access to the shared network, the UE does not switch to another available PLMN as long as the selected PLMN is available to serve the UE at its present location. The network does not move the UE to another available PLMN by handover as long as the selected PLMN is available to serve the UE.

The NG-RAN uses the selected PLMN information, which is provided by the UE at RRC establishment or provided by the AMF/source NG-RAN at N2/Xn handover, to select target cells for future handovers and allocation of radio resources. In case of handover to a shared network, the NG-RAN selects a target PLMN based on either PLMN in use, preset configuration, or the equivalent PLMN list in the handover restriction list provided by the AMF. For Xn-based handover procedure, the source NG-RAN indicates the selected PLMN ID to the target NG-RAN by using target cell ID. For N2-based handover procedure, the NG-RAN indicates the selected PLMN ID to the AMF as part of the tracking area identity (TAI) sent in the handover required message. The source AMF uses the TAI information supplied by the source NG-RAN to select the target AMF/MME and to forward the selected PLMN ID to the target AMF/MME. The selected PLMN ID is signaled to the target NG-RAN/eNB so that it can select target cells for future handovers. In a network slicing scenario, a network slice is defined within a PLMN. Network sharing is performed among different PLMNs and each PLMN sharing the NG-RAN defines and supports its PLMN-specific set of slices that are supported by the common NG-RAN [3].

1.2 Reference Architectures

5G systems have been designed to support seamless user connectivity and to render new services/applications which would require deployment of networks that exploit innovative techniques such as NFV and SDN. A distinct feature of 5G system architecture is network slicing. The previous generation supported certain aspects of this with the functionality for dedicated core networks. In the context of 3GPP 5G system architecture, a network slice refers to the set of 3GPP defined features and functionalities that together form a complete PLMN for providing services to UEs. Network slicing allows controlled composition of a PLMN from the specified NFs with their specifics and provides services that are required for a specific usage scenario. The need for these new techniques is increasing due to the versatility of data services that are supported by 5G networks. Mobile networks were traditionally designed as voice-centric and later data-centric systems; however, with 5G this design philosophy has changed as a result of proliferation of new use cases and applications.

Having such requirements in mind, 3GPP attempted to maintain the premises of flat architecture where the control-plane functions are separated from the user plane in order to make them scale independently, allowing the operators to exploit logical functional split for dimensioning in deploying and adapting their networks. Another central idea in the design of 5G network was to minimize dependencies between the access network and the core network with a converged access-agnostic core network with a common interface which integrates different 3GPP and non-3GPP access types.

5G is a service-centric architecture which strives to deliver the entire network as a service. 3GPP system architecture group took the approach to rearchitect the LTE core network based on a service-oriented framework. This involves breaking everything down to more functional granularity. The MME no longer exists and its functionality has been redistributed between mobility management and session management NFs. As such, registration, reachability, mobility management, and connection management are now considered new services offered by a new general NF labeled as AMF. Session establishment and session management, also formerly part of the MME, are now new services offered by a new NF called session management function (SMF). Furthermore, packet routing and forwarding functions, currently performed by the SGW and PGW in 4G, will now be realized as services rendered through a new NF called UPF. The main reason for this new architectural approach is to enable a flexible network as a service solution. By standardizing a modularized set of services, various deployment options such as centralized, distributed, or mixed configurations will be enabled for different users or applications. The dynamic service chaining lay the groundwork for network slicing which is an important concept in 5G to satisfy the diverse user and application demands, shifting the design emphasis on software rather than hardware. The physical boxes where these software services are instantiated could be in the cloud or on any targeted general-purpose hardware in the system.

In the following sections, we will discuss the reference architecture, network entities, and interfaces of the 3GPP 5G access and the core networks. The user-plane and control-plane protocols will be further discussed.

1.2.1 Access Network

1.2.1.1 Reference Architecture: Network Entities and Interfaces

The overall reference architecture of next-generation network comprises the entities associated with the radio access network (NG-RAN) and the core network (5GC) and their corresponding interfaces that terminate the protocols. In this section, we will describe the access network reference architecture. The NG-RAN architecture consists of a set of gNBs connected to the 5GC through the NG interface (see Fig. 1.51). The interface between the NG-RAN and 5GC is referred to as N2 and N3 depending on the termination point in 3GPP

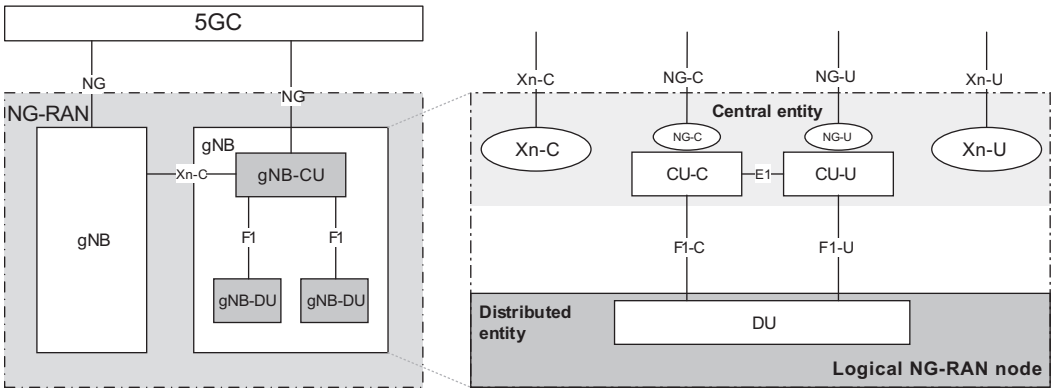


Figure 1.51
Overall NG-RAN architecture [15].

system architecture specifications. Furthermore, gNBs are interconnected through the Xn interface. In a C-RAN architecture, a gNB may be further disaggregated such that some lower layer protocol functions are implemented in the DUs and the remaining upper layer protocol functions are implemented in the edge cloud and as part of the CU(s). In that case, the gNB would consist of a gNB-CU and gNB-DUs as shown in Fig. 1.51. The gNB-CU and gNB-DU entities are connected via F1 logical interface. Note that one gNB-DU is connected to only one gNB-CU. In some deployment scenarios, one gNB-DU may be connected to multiple gNB-CUs. In NG-RAN reference architecture, NG, Xn and F1 are logical interfaces [16].

The traditional architecture of a base station where all protocol layers and functionalities were concentrated in a single logical RAN entity has evolved into a disaggregated model in 5G network architecture. In a disaggregated gNB architecture, the NG and Xn-C interfaces are terminated at the gNB-CU. In an LTE−NR dual connectivity (EN-DC) scenario, the S1-U and X2-C interfaces for a disaggregated gNB terminate at the gNB-CU. It must be noted that the gNB-CU and its associated gNB-DUs are seen as a gNB to other gNBs and the 5GC. The NG-RAN comprises a radio network layer (RNL) and a TNL. The NG-RAN architecture, that is, the NG-RAN logical nodes and the corresponding interfaces, is defined as part of the RNL, whereas the NG-RAN interfaces (NG, Xn, F1) are specified as part of TNL protocols and functionalities. The TNL provides services for user-plane and signaling transport. The protocols over Uu (i.e., the radio air-interface) and NG interfaces are divided into two classes: user-plane protocols, which are the protocols implementing the actual PDU carrying user data through the AS; and control-plane protocols, which are the protocols for controlling the PDU sessions and the connection between the UE and the network from different aspects including requesting the service, controlling different transmission resources, handover, etc. as well as a mechanism for transparent transfer of NAS messages

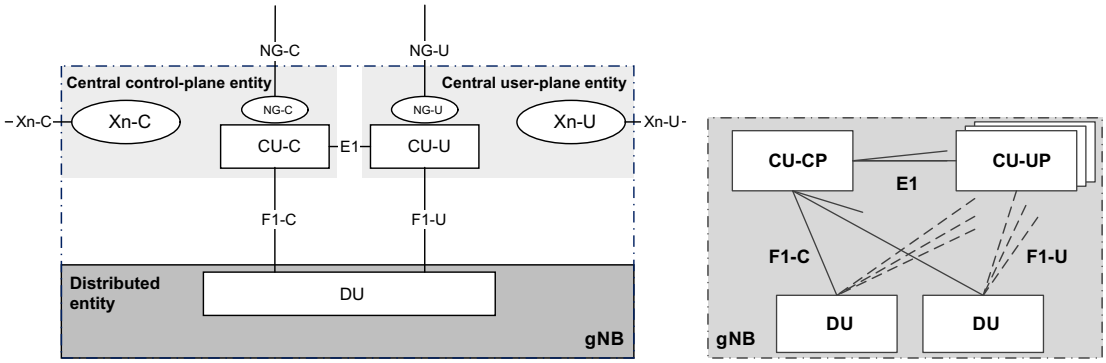


Figure 1.52
Disaggregated gNB model [15].

via encapsulation in RRC messages. The NG interface, comprising a user-plane interface (NG-U) and a control-plane interface (NG-C), connects the 5GC and the NG-RAN. In this architecture, the NG-RAN termination is an NG-RAN node which can be either an ng-eNB or a gNB and the 5GC termination is either the control-plane AMF logical node or the user-plane UPF logical node. There may be multiple NG-C logical interfaces toward 5GC from any NG-RAN nodes which are selected by the NAS node selection function. Likewise, there may be multiple NG-U logical interfaces toward 5GC from any NG-RAN node which can be selected within the 5GC and signaled to the NG-RAN node by the AMF [15,17] (see Fig. 1.52).

The NG interface supports procedures to establish, maintain, and release NG-RAN part of PDU sessions; to perform intra-RAT handover and inter-RAT handover; the separation of each UE on the protocol level for user-specific signaling management; the transfer of NAS signaling messages between UE and AMF; and mechanisms for resource reservation for packet data streams. The functions supported over the NG interface include the following [17]:

- Paging function which supports transmission of paging requests to the NG-RAN nodes that are part of the paging area to which the UE is registered.
- UE context management function which allows the AMF to establish, modify, or release the UE context in the AMF and the NG-RAN node in order to support user-specific signaling on NG interface.
- Mobility function for UEs in ECM-CONNECTED, which includes the intra-system handover function to support mobility within NG-RAN and inter-system handover function to support mobility from/to EPS system including the preparation, execution, and completion of handover via the NG interface.

- PDU session function that is responsible for establishing, modifying, and releasing the involved PDU sessions NG-RAN resources for user data transport once the UE context is available in the NG-RAN node.
- NAS signaling transport function provides means to transport or re-route a NAS message for a specific UE over the NG interface.
- NG-interface management functions which provide mechanisms to ensure a default start of NG-interface operation and handling different versions of application part implementations and protocol errors.

The interconnection of NG-RAN nodes to multiple AMFs is supported in the 5G system architecture. Therefore, a NAS node selection function is located in the NG-RAN node to determine the AMF association of the UE, based on the UE's temporary identifier, which is assigned to the UE by the AMF. If the UE's temporary identifier has not been assigned or is no longer valid, the NG-RAN node may consider the slicing information to determine the AMF. This functionality is located in the NG-RAN node and enables proper routing via the NG interface.

As shown in Fig. 1.53, each NG-RAN node is either a gNB, that is, an NR base station, providing NR user-plane and control-plane protocol terminations toward the UE or an ng-eNB, that is, a Rel-15/16 LTE base station, terminating LTE user-plane and control-plane protocols to/from the UE. The gNBs and ng-eNBs are interconnected through Xn interface. The gNBs and ng-eNBs are also connected via NG interfaces to the 5GC. More specifically, NG-C interfaces NG-RAN nodes to the AMF and NG-U interfaces the NG-RAN nodes to the UPF [16].

In 5G network architecture, the gNB entity is responsible for performing functions corresponding to RRM including radio bearer control, radio admission control, connection mobility control, dynamic allocation of resources to UEs in both uplink and downlink (scheduling). The gNB further performs IP header compression and encryption and integrity protection of data as well as selection of an AMF upon UE attachment when no routing to an AMF can be determined from the information provided by the UE. It also provides routing of user-plane data toward UPF(s) along with routing of control-plane information toward AMF; the connection setup and release; scheduling and transmission of paging messages originated from the AMF; scheduling and transmission of system information originated from the AMF or network operation and management; measurement and reporting configuration for mobility and scheduling; session management; support of network slicing; QoS flow management and mapping to data radio bearers (DRBs); support of UEs in RRC_INACTIVE state; as well as RAN sharing and DC [16].

In NG-RAN architecture, the role of AMF is similar to that of MME in the EPC which hosts core network control-plane functions such as terminating NAS signaling and security; AS security control; internetwork signaling for mobility between 3GPP access networks;

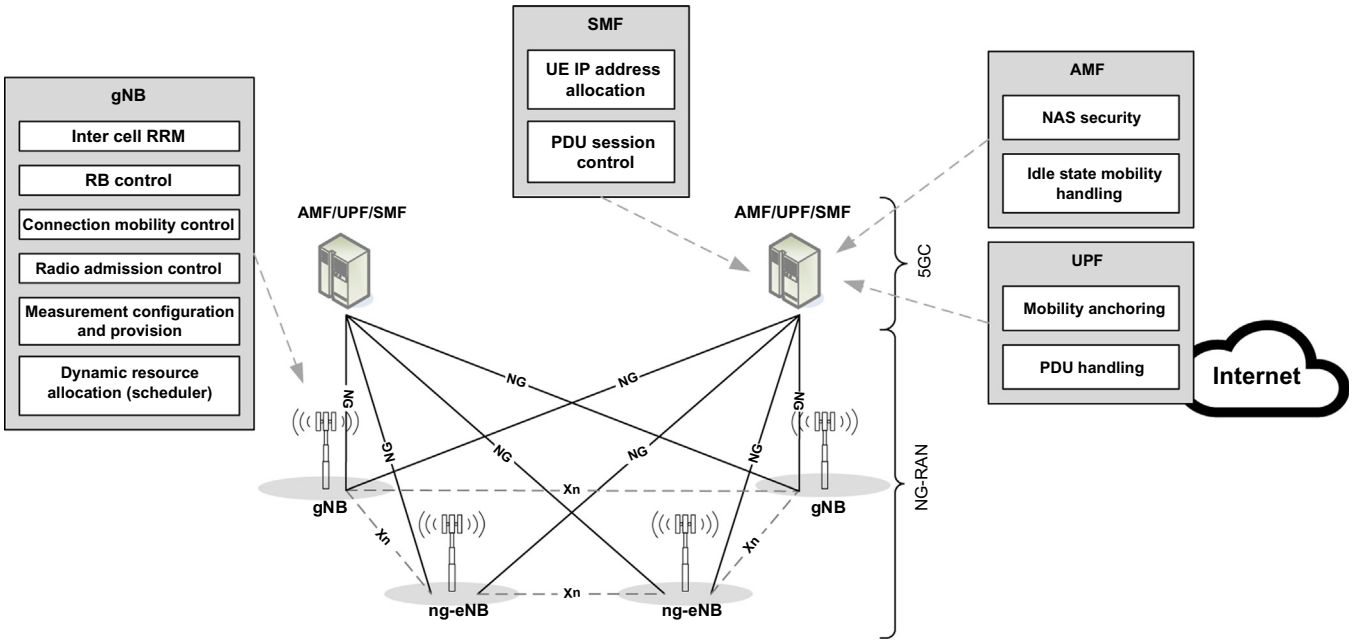


Figure 1.53
Overall access network architecture [16].

idle-mode UE reachability which includes paging control, registration area management; support of intra-system and inter-system mobility; access authentication and authorization; mobility management control; support of network slicing; and SMF selection.

The role of SMF in the new architecture is similar to that of EPC PGW entity hosting user-plane functions such as session management; allocating and managing UE IP address; selecting and controlling of UPFs; configuring traffic steering at UPF in order to route traffic toward proper destination; controlling part of policy enforcement; and the QoS.

The new architecture further features a UPF entity which is similar to the EPC SGW user-plane entity. This entity hosts the UPFs such as anchor point for intra- or inter-RAT mobility, external PDU session point of interconnect to data network, packet routing and forwarding, packet inspection and user plane part of policy rule enforcement, traffic usage reporting, uplink classifier to support routing traffic flows to a data network, QoS handling for user plane which includes packet filtering, gating, UL/DL rate enforcement, uplink traffic verification, that is, service data flow (SDF)[55] to QoS flow mapping, and downlink packet buffering and downlink data notification triggering [16].

1.2.1.1.1 Xn Control-Plane/User-Plane Functions and Procedures

Xn is a reference point connecting the NG-RAN access nodes, supporting the transfer of signaling information and forwarding of user traffic between those nodes. Xn is a logical point-to-point interface between two NG-RAN access nodes which establishes a logical connection between the two nodes even when a direct physical connection does not exist between the two nodes (which is often the case). It comprises both user-plane and control--plane protocols.

The user-plane protocol stack of Xn interface is shown in Fig. 1.54. The TNL uses GTP-U[56] over UDP/IP to transfer the user-plane PDUs. As a result, Xn-U interface can

[55] User traffic using different services or applications has different quality of service classes. A service data flow is an IP flow or an aggregation of IP flows of user traffic classified by the type of the service in use. Different service data flows have different quality of service class attributes, thereby a service data flow serves as a unit by which quality of service rules are applied in accordance with network policy and charging rules.

[56] GPRS tunneling protocol is a protocol that is used over various interfaces within the packet core in 3GPP networks to allow the user terminals to maintain a connection to a packet data network while on the move. The protocol uses tunnels to allow two GPRS support nodes to communicate over a GPRS tunneling protocol-based interface and separates traffic into different communication flows. GPRS tunneling protocol creates, modifies, and deletes tunnels for transporting IP payloads between the user equipment, the GPRS support node in the core network and the Internet. GPRS tunneling protocol comprises three types of traffic, namely control-plane (GTP-C), user-plane (GTP-U), and charging. GTP-C protocol supports exchange of control information for creation, modification, and termination of GPRS tunneling protocol tunnels. It creates data forwarding tunnels in case of handover. GTP-U protocol is used to forward user IP packets over certain network interfaces. When a GTP tunnel is established for data forwarding during LTE handover, an End Marker packet is transferred as the last packet over the GPRS tunneling protocol tunnel.

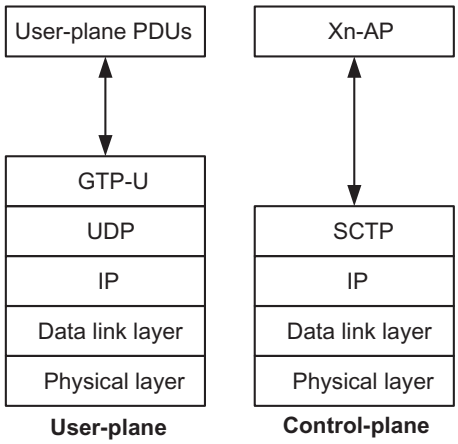


Figure 1.54
Xn-U and Xn-C protocol stacks [16].

only provide non-guaranteed delivery of user-plane PDUs, but it supports data forwarding and flow control. The Xn interface specifications facilitate interconnection of NG-RAN nodes manufactured by different vendors as well as separation of Xn interface radio network and transport network functionalities in order to allow future extensions. The Xn interface supports intra-NG-RAN mobility and DC procedures.

The control-plane protocol stack of Xn interface is also illustrated in Fig. 1.54. The TNL uses stream control transmission protocol (SCTP)[57] over IP. The application layer signaling protocol is referred to as Xn application protocol (Xn-AP). The SCTP layer provides guaranteed delivery of application layer messages. In the transport IP layer, point-to-point transmission is used to deliver the signaling PDUs. The Xn-C interface supports Xn interface management and error handling (the functionality to manage the Xn-C interface), mobility support for UE in CM-CONNECTED (the functionality to manage the UE mobility for connected mode between nodes in the NG-RAN), context transfer from the current serving NG-RAN node to the new serving NG-RAN node, and control of user-plane tunnels between the existing serving NG-RAN node and the new serving NG-RAN node. It further supports DC (the functionality to enable usage of additional resources in a secondary node in the NG-RAN) as well as support of paging (sending of paging messages via the last serving NG-RAN node toward other nodes in the RAN-based notification area to a UE in RRC_INACTIVE state).

[57] Stream control transmission protocol is a transport layer protocol for transmitting multiple streams of data at the same time between two end points that have established a connection in a network. It is message-oriented protocol like user data protocol and ensures reliable, in-sequence transport of messages with congestion control like transmission control protocol. Stream control transmission protocol supports multihoming and redundant paths to increase resilience and reliability.

1.2.1.1.2 F1 Control-Plane/User-Plane Functions and Procedures

As we described earlier, the NG-RAN gNB functions may be implemented in one gNB-CU and one or more gNB-DUs. The gNB-CU and gNB-DU are connected via an F1 logical interface, which is a standardized interface that supports interchange of signaling information and data transmission between the termination points. From a logical point of view, F1 is a point-to-point interface between the termination points, which may be established irrespective of the existence of a physical connectivity between the two points. F1 interface supports control-plane and user-plane separation and separates radio network and TNLs. This interface enables exchange of UE and non-UE associated information. Other nodes in the network view the gNB-CU and a set of gNB-DUs as a gNB. The gNB terminates X2, Xn, NG, and S1-U interfaces [28].

The RRM functions ensure the efficient use of the available network resources. In a gNB-CU/gNB-DU disaggregated model, different RRM functions may be located at different locations. As an example, radio bearer control function (for establishment, maintenance, and release of radio bearers) can be located either at gNB-CU or gNB-DUs, whereas inter-RAT RRM function (for management of radio resources in conjunction with inter-RAT mobility) and dynamic resource allocation and packet scheduling functions (for allocation and de-allocation of resources to user and control-plane packets) are exclusively located at gNB-CU and gNB-DU(s), respectively. Fig. 1.55 shows F1 control-plane and user-plane protocol structures. In the control plane, the TNL is based on IP transport using SCTP over IP for transfer of control messages. The application layer signaling protocol is referred to as F1 application protocol (F1AP). In the user plane, the IP-based TNL uses GTP-U over UDP/IP for transfer of data packets.

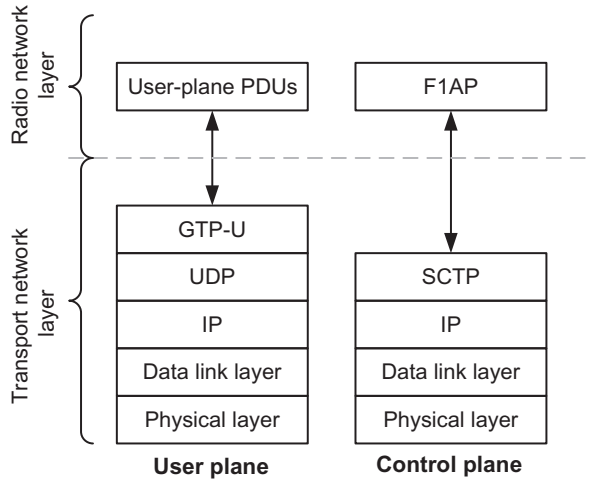


Figure 1.55
User-plane and control-plane protocol structure of F1 interface [28].

F1AP provides a signaling conduit between gNB-DU and the gNB-CU whose services are divided into non-UE-associated (related to the entire F1 interface instance between the gNB-DU and gNB-CU utilizing a non-UE-associated signaling connection); and UE-associated (F1AP functions that provide these services are associated with a UE-associated signaling connection that is maintained for a specific UE) services [31]. F1AP consists of elementary procedures (EPs), where an EP is defined as the unit of interaction between gNB-CU and gNB-DU over F1. These EPs are defined separately and are used to create complete sequences in a flexible manner. Unless otherwise stated by the restrictions, these EPs may be invoked independent of each other as stand-alone procedures, which can be active in parallel. An EP consists of an initiating message and possibly its response message. Two types of EPs, referred to as class 1 and class 2, are used, where the former consists of elementary procedures with response (success and/or failure) and the latter comprises EPs without response.

A gNB-CU UE F1AP ID is allocated to uniquely identify the UE over the F1 interface within a gNB-CU. The gNB-DU stores the received gNB-CU UE F1AP ID for the duration of time that the UE-associated logical F1-connection is valid. A gNB-DU UE F1AP ID is assigned to uniquely identify the UE over the F1 interface within a gNB-DU. When a gNB-CU receives a gNB-DU UE F1AP ID, it stores it for the period of time that the UE-associated logical F1-connection for the UE remains valid. The UE-associated signaling is used when F1AP messages corresponding to a UE utilize the UE-associated logical F1-connection for association of the message to the UE in gNB-DU and gNB-CU. A UE-associated logical F1-connection uses unique identities that are used to identify UE F1AP messages by the gNB-CU and gNB-DU. A UE-associated logical F1-connection may exist before the F1 UE context[58] is setup in the gNB-DU.

The F1 interface management procedures include reset, error indication, F1 setup, gNB-DU configuration update, and gNB-CU configuration update on the control plane. The F1-C context management procedures include UE context setup, UE context release request (gNB-DU/gNB-CU initiated), UE context modification (gNB-CU/gNB-DU initiated), and UE mobility command. The F1-C RRC message transfer procedures include initial uplink RRC message transfer as well as UL/DL RRC message transfer. The F1 control plane further includes system information procedure and paging procedures [28]. The error indication function is used by the gNB-DU or gNB-CU to indicate occurrence of an error. The reset

[58] A gNB UE context is a block of information in the gNB associated with an active user equipment. The block of information contains the necessary information in order to provide NG-RAN services to the active user equipment. The gNB user equipment context is established when the transition to active state for a user equipment is completed or in target gNB after completion of handover resource allocation during handover preparation, where in each case the user equipment state information, security information, user equipment capability information, and the identities of the user equipment-associated logical NG connection are stored in the gNB user equipment context.

function is used to initialize the peer entity after node setup and after a failure event. This procedure can be used by both the gNB-DU and gNB-CU. The F1 setup function, initiated by gNB-DU, allows exchange of application-level data between gNB-DU and gNB-CU while ensuring proper interoperability over the F1 interface. The gNB-CU and gNB-DU configuration update functions facilitate updating application-level configuration data between gNB-CU and gNB-DU to properly interoperate over the F1 interface, and activate or deactivate the cells. Scheduling of broadcast system information is performed in the gNB-DU. The gNB-DU is responsible for encoding of NR-MIB (master information block portion of NR system information). In case broadcast of RMSI (remaining system information) or other SI messages is needed, the gNB-DU will be responsible for encoding of RMSI and the gNB-CU is responsible for encoding of other SI messages. The gNB-DU and gNB-CU measurement reporting functions are used to report the measurements of gNB-DU and gNB-CU, respectively.

The gNB-DU is further responsible for transmitting paging information according to the scheduling parameters. The gNB-CU provides paging information to enable gNB-DU to calculate the exact paging occasion and paging frame. The gNB-CU is responsible for calculating paging area. The gNB-DU combines the paging records for a particular paging occasion, frame, and area and further encodes the RRC message and broadcasts the paging message. The F1 UE context management function supports the establishment and modification of the necessary overall initial UE context. The mapping between QoS flows and radio bearers is performed by gNB-CU where the granularity of bearer related management over F1 is at radio-bearer level. To support PDCP duplication for intra-DU carrier aggregation, one DRB should be configured with two GTP-U tunnels between gNB-CU and gNB-DU.

1.2.1.1.3 E1 Control-Plane Functions and Procedures

As we discussed earlier, the disaggregated gNB model was introduced to enable separation of control-plane and user-plane functions in addition to the functional split of the protocol stack in gNB which facilitates design and development of new-generation gNBs based on the SDN/NFV concepts. As such, a new interface between the gNB-CU-CP and gNB-CU-UP components has been defined by 3GPP to support exchange of signaling information between these entities (see Fig. 1.52). E1 is an open interface which would allow multi-vendor implementation of the control-plane and data-plane components of the CU. E1 establishes a logical point-to-point interface between a gNB-CU-CP and a gNB-CU-UP even in the absence of a direct physical connection between the endpoints. The E1 interface separates radio network and TNLs and enables exchange of UE associated/non-UE associated information. The E1 interface is a control interface and is not used for user data forwarding. As shown in Fig. 1.52, a gNB may consist of one gNB-CU-CP, multiple gNB-CU-UPs, and multiple gNB-DUs. One gNB-DU can be connected to multiple gNB-CU-UPs under the

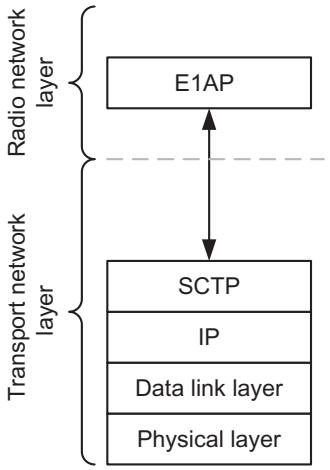


Figure 1.56
Protocol stack for E1 interface [36].

control of the same gNB-CU-CP and one gNB-CU-UP can be connected to multiple DUs under the control of the same gNB-CU-CP. The connectivity between a gNB-CU-UP and a gNB-DU is established by the gNB-CU-CP using bearer or UE context management functions. The gNB-CU-CP further selects the appropriate gNB-CU-UP(s) for the requested UE services. The E1 interface would support independent virtualization of the control and UPFs. It would also enable more flexible allocation of the functions of the central unit. It allows for energy and cost-efficient central processing and resource pooling for the user plane. Several functions such as security, packet inspection, header compression, and data mining could benefit from centralization. Furthermore, it would provide optimum routing of packets in case of multi-connectivity and interworking with other systems. The protocol structure for E1 is shown in Fig. 1.56. The TNL uses IP transport with SCTP over IP. The application layer signaling protocol is referred to as E1 application protocol (E1AP).

1.2.1.1.4 NG Control-Plane/User-Plane Functions and Procedures

The NG control-plane interface (NG-C) is defined between the gNB/ng-eNB and the AMF. The control-plane protocol stack of NG interface is shown in Fig. 1.57. The TNL relies on IP transport; however, for more reliable transmission of signaling messages, the SCTP protocol is used over IP. The application layer signaling protocol is referred to as NG application protocol (NGAP). The SCTP layer provides guaranteed delivery of application layer messages. IP layer point-to-point transmission is used to deliver the signaling PDUs. The NG-C interface further enables interface management (the functionality to manage the NG-C interface), UE context management (the functionality to manage the UE context between NG-RAN and 5GC), UE mobility

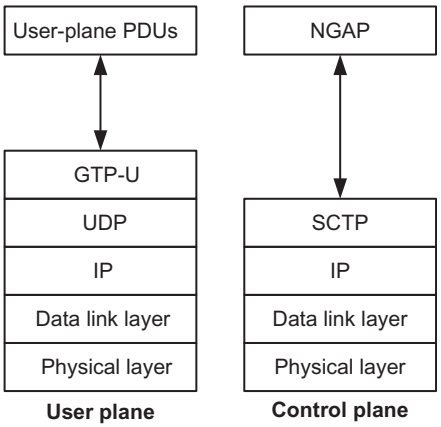


Figure 1.57
NG-U and NG-C protocol stack [16].

management (the functionality to manage the UE mobility in connected mode between NG-RAN and 5GC), transport of NAS messages (procedures to transfer NAS messages between 5GC and UE), and paging (the functionality to enable 5GC to generate paging messages sent to NG-RAN to allow NG-RAN to page the UE in RRC_IDLE state). It further enables PDU session management (the functionality to establish, manage, and remove PDU sessions and respective NG-RAN resources that are made of data flows carrying user-plane traffic) as well as configuration transfer (the functionality to transfer the NG-RAN configuration information, e.g., transport layer addresses for establishment of Xn interface, between two NG-RAN nodes via 5GC). The NGAP protocol consists of elementary procedures where an elementary procedure is a unit of interaction between the NG-RAN node and the AMF. These elementary procedures are defined separately and are used to create complete sequences in a flexible manner. Unless otherwise stated by the restrictions, the EPs may be invoked independent of each other as stand-alone procedures, which can be active in parallel. An EP consists of an initiating message and possibly the corresponding response message. Two types of EPs referred to as class 1 and class 2 are defined, where class 1 EP consists of elementary procedures with response (success and/or failure) and class 2 EP comprises elementary procedures without response.

The NG user-plane (NG-U) interface is defined between a NG-RAN node and a UPF. The NG-U interface provides non-guaranteed delivery of user-plane PDUs between the two nodes. The user-plane protocol stack of the NG interface is also shown in Fig. 1.57. The TNL relies on IP transport and use of GTP-U over UDP/IP to carry the user-plane PDUs between the NG-RAN node and the UPF.

1.2.1.2 Bearers and Identifiers

1.2.1.2.1 Radio Bearers and Packet Data Unit Sessions

In LTE, IP connection between a UE and a PDN is established via a PDN connection or EPS session. An EPS session delivers the IP packets that are labeled with UE IP address through logical paths between the UE and the PDN (UE-PGW-PDN). An EPS bearer is a logical pipe through which IP packets are delivered over the LTE network, that is, between a UE and a PGW (UE-eNB-SGW-PGW). A UE can have multiple EPS bearers concurrently. Thus different EPS bearers are identified by their EPS bearer IDs, which are allocated by the MME. An EPS bearer in reality is the concatenation of three underlying bearers: (1) A DRB between the UE and the eNB, which is set up upon user-plane establishment between the UE and the access node; (2) an S1 bearer between the eNB and SGW, which is set up upon establishment of EPS connection between the UE and the EPC; and (3) an S5/S8 bearer between the SGW and PGW, which is set up upon establishment of PDN connection between the UE and the PGW. An E-URAN random access bearer (E-RAB) is a bearer with two endpoints at the UE and at the SGW, which consists of a DRB and an S1 bearer. As such, E-RAB is a concatenation of a DRB and an S1 bearer, which logically connects the UE to the SGW. LTE QoS architecture describes how a network operator could create and configure different bearer types in order to map various IP traffic categories (user services) to the appropriate bearers according to the service QoS requirements. In that context, a bearer is an encapsulation mechanism or a tunnel that is created per user for transporting various traffic flows with specific QoS requirements within the LTE access and core networks.

In LTE and NR, there are two types of radio bearers, namely signaling radio bearers (SRB) and DRB. The SRBs are radio bearers that are only used for the transmission of RRC and NAS messages, whereas the DRBs are radio bearers that are used to transport user-plane traffic. The RRC messages are used as signaling between UE and the access node (i.e., eNB or gNB). The NAS messages are used for signaling between the UE and the core network. The RRC messages are used to encapsulate the NAS messages for transfer between the UE and the core network through the access node (transparent to the access node). The SRBs are further classified into three types: SRB0, SRB1, and SRB2, where SRB0 is used to transfer RRC messages which use common control channel, SRB1 is used to transfer RRC messages which use dedicated control channel, and SRB2 is used to transfer RRC messages which use dedicated control channel and encapsulate NAS messages. The SRB1 can be used to encapsulate NAS message, if SRB2 has not been configured. The SRB2 has lower priority than SRB1 and it is always configured after security activation. The SRB0 uses RLC transparent mode, while SRB1 and SRB2 use RLC acknowledged mode.

In LTE, upon connection establishment and at the beginning of an EPS session, a default EPS bearer, with no guaranteed bit rate and best effort QoS characteristics, is established.

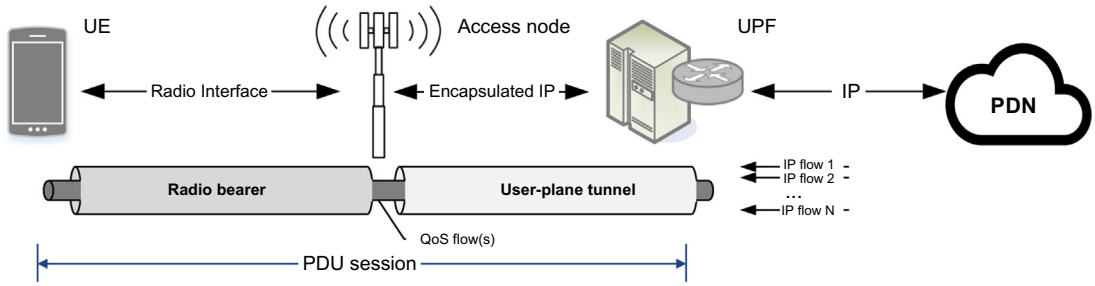


Figure 1.58
High-level illustration of 3GPP bearer architecture [16].

Dedicated EPS bearers with guaranteed bit rate and specific QoS attributes for various services can be established through negotiation and connection reconfiguration for active users. In LTE, the QoS control is performed per EPS bearer such that EPS bearers and radio bearers have a one-to-one relationship. There are two types of end-to-end bearers. The default bearer is established during the attach procedure and after an IP address is allocated to the UE and has best effort QoS characteristics. The dedicated bearer is typically established during the call setup after transition from the idle mode but can also be established during the attach procedure and supports various QoS characteristics with guaranteed bit rate. Bearer establishment negotiations are performed between the UE and the access point name (APN)[59] in the core network which maps the bearers to an external network such as the Internet or an IP multimedia subsystem (IMS).[60] However, it is important to note that the availability and provisioning of bearers is strictly controlled by operator configuration, as well as the association between the UE and the PDN that provides PDU connectivity service. The PDU sessions can be based on IPv4, IPv6, Ethernet or unstructured.

In NR and as shown in Fig. 1.58, the UE receives services through a PDU session, which is a logical connection between the UE and the data network. Various PDU session types are supported, for example, IPv4, IPv6, and Ethernet. Unlike the EPS, where at least one default bearer is always created when the UE attaches to the network, 5GS can establish a session

[59] Access point name is a gateway or anchor node between a mobile network and another IP network such as the Internet. A mobile device attempting a data connection must be configured with an access point name to present to the carrier. The carrier will then examine this identifier in order to determine what type of network connection should be created, which IP addresses should be assigned to the wireless device, and which security methods should be used. Therefore, the access point name identifies the packet data network with which a mobile data user communicates.

[60] The IP multimedia subsystem is an architectural framework developed by 3GPP for delivering IP multimedia services. Mobile networks originally provided voice services through circuit-switched networks and later migrated to all-IP network architectures. IP multimedia subsystem provides real-time multimedia sessions (voice over IP, video, teleconferencing, etc.) and nonreal-time multimedia sessions (push to talk, presence, and instant messaging) over an all-IP network. IP multimedia subsystem enables convergence of services provided by different types of networks which include fixed, mobile, and Internet.

when service is needed and independent of the attachment procedure of UE, that is, attachment without any PDU session is possible. 5GS also supports the UE to establish multiple PDU sessions to the same data network or to different data networks over a single or multiple access networks including 3GPP and non-3GPP. The number of UPFs for a PDU session is not specified. The deployment with at least one UPF is essential to serve a given PDU session. For a UE with multiple PDU sessions, there is no need for a convergence point such as SGW in the EPC. In other words, the user-plane paths of different PDU sessions are completely disjoint. This implies that there is a distinct buffering node per PDU session for the UE in the RRC_IDLE state.

5G QoS framework has been designed to allow detection and differentiation of sub-service flows in order to provide improved quality of experience relative to the previous generations of 3GPP radio interface standards. Since LTE bearer framework was insufficient to address certain 5G service requirements, a refined QoS model based on the concept of QoS flow was introduced in 5G. The QoS flow is the finest granularity for QoS enforcement in 3GPP 5G systems. All traffic mapped to the same 5G QoS flow receives the same forwarding treatment. Providing different QoS forwarding treatment requires the use of different 5G QoS flows. Fig. 1.59 illustrates the comparison between 4G and 5G QoS models. It is shown that the 5G concept allows flexible mapping of the 5G QoS flows to radio bearers, for example, the first 5G QoS flow is transported over the first 5G radio bearer while the second and third 5G QoS flows are transported together in the second 5G radio bearer. In order to support 5G QoS flows, either the existing protocols (e.g., PDCP) had to be enhanced or a new (layer-2) sublayer known as service data adaptation protocol (SDAP) had to be introduced. The main services and functions of SDAP include mapping between a

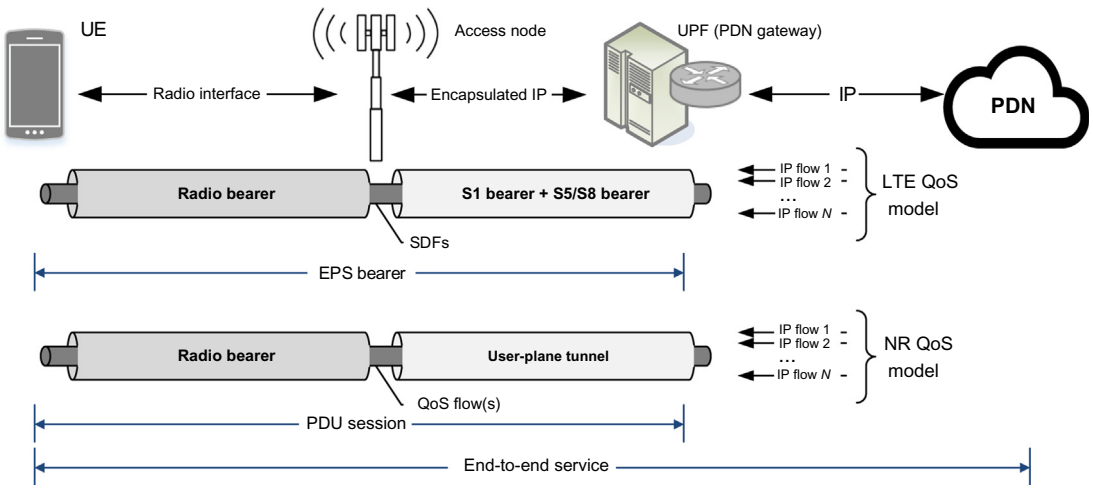


Figure 1.59
Comparison of QoS models in 4G LTE and 5G NR.

QoS flow and a data radio bearer, marking QoS flow identifier (QFI) in the downlink and uplink packets. For each DRB, the UE monitors the QoS flow ID(s) of the downlink packets and applies the same mapping in the uplink, that is, for a DRB, the UE maps the uplink packets belonging to the QoS flows(s) corresponding to the QoS flow ID(s) and PDU session in the downlink packets for that DRB.

In order to establish a PDU session, a PDU session establishment message is sent by 5GC to the gNB serving the UE, which includes the NAS message to be transferred to the UE containing the QoS-related information. The gNB sends a DRB setup request message to the UE and includes the DRB parameters and the NAS message that it received earlier. The UE establishes at least a default DRB associated with the new PDU session. It further creates the QFI to DRB mapping and sends an RRC DRB setup complete message to the gNB. The gNB sends PDU session establishment acknowledgment message to 5GC, indicating successful establishment of the PDU session. Data is sent over the N3 tunnel to the gNB and then over the DRB to the UE. The data packets may optionally include a QoS marking (same as or corresponding to QFI) in their SDAP header. The UE sends uplink packets over the DRB to the gNB. The uplink data packets include a QoS marking (same as or corresponding to QFI) in the SDAP header [16].

Dual-connectivity was introduced as part of LTE Rel-12. In LTE DC, the radio protocol architecture that a particular bearer uses depends on how the bearer is setup. Three bearer types have been defined: master cell group (MCG), secondary cell group (SCG), and split bearer. The three bearer types are illustrated in Figs. 1.60–1.62. The RRC layer is always located in the master node and signaling bearers are mapped to MCG bearer; therefore, they only use the radio resources provided by the master node. The MCG bearer can be seen as the legacy bearer that transports both data and signaling. Split bearer and SCG bearer are data only bearers. The main difference between the two is that for split bearer,

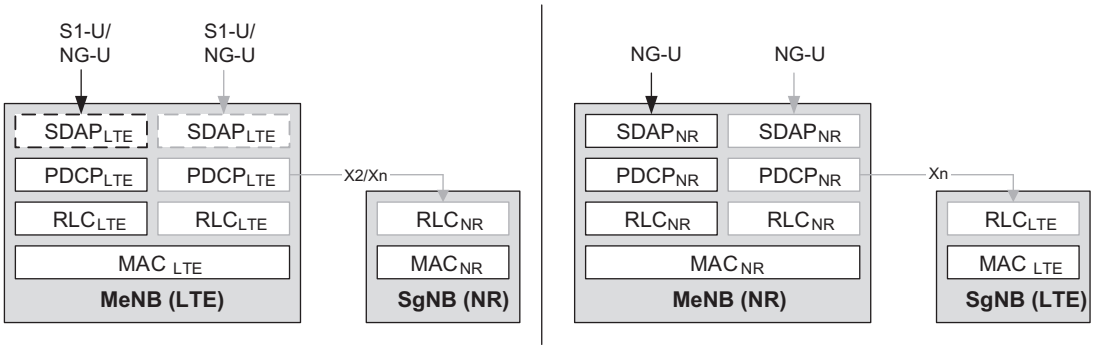


Figure 1.60
Illustration of split bearer via MCG [13,16].

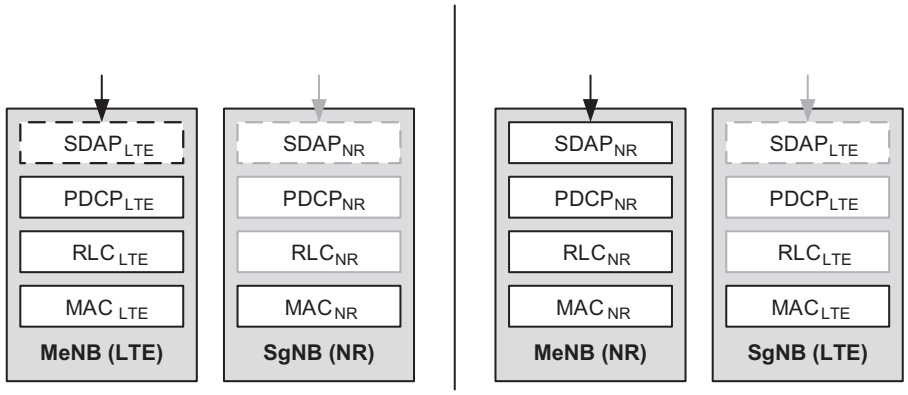


Figure 1.61
Illustration of SCG bearer [13].

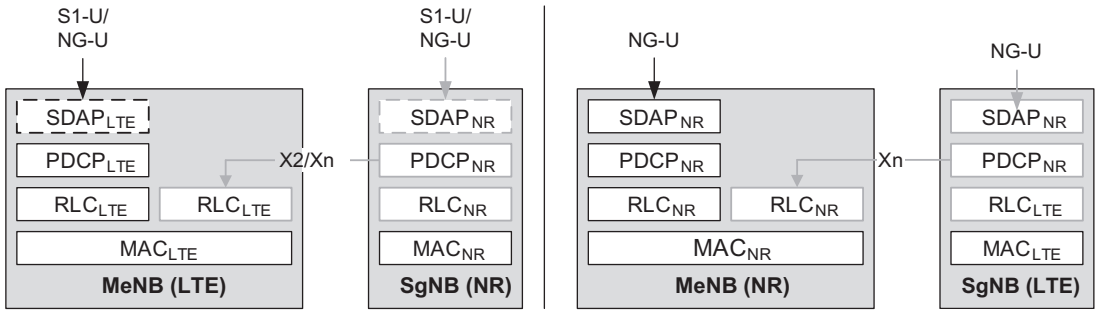


Figure 1.62
Illustration of split bearer via SCG [13].

the S1-U/NG-U interface terminates in the master node, whereas for SCG bearer, the S1-U/NG-U interface terminates at the secondary node [13].

3GPP NR supports DC in which a UE in RRC_CONNECTED is configured to utilize radio resources provided by two distinct schedulers located in two gNBs connected via a non-ideal backhaul. The gNBs involved in DC operation for a certain UE may assume two different roles, that is, a gNB may either act as an MgNB or as SgNB. In DC operation, a UE is connected to one MgNB and one SgNB. There are four bearer types in NR DC, namely MCG bearer, MCG split bearer, SCG bearer, and SCG split bearer. The dual-connectivity between LTE and NR supports similar bearer types. Split bearer via MCG, SCG bearer (a bearer whose radio protocols are split at the SgNB and belongs to both SCG and MCG), and MCG split bearer (a bearer whose radio protocols are split at the MgNB and belongs to both MCG and SCG). The MCG bearer and one SCG bearer are used for two different QoS flows [16].

In the downlink, the incoming data packets are classified by the UPF based on SDF[61] templates according to their precedence (without initiating additional N4 signaling). The UPF conveys the classification of user-plane traffic associated with a QoS flow through an N3 (and N9) user-plane marking using a QFI. The AN binds QoS flows to AN resources (i.e., data radio bearers). There is no one-to-one relationship between QoS flows and AN resources and it is the responsibility of the AN to establish the necessary resources for mapping to the QoS flows [13].

In 3GPP NR, the DRB defines the packet treatment on the radio interface. A DRB serves packets with the same packet forwarding treatment. Separate DRBs may be established for QoS flows requiring different packet handling. In the downlink, the RAN maps QoS flows to DRBs based on QoS flow ID and the associated QoS profiles. In the uplink, the UE marks uplink packets over the radio air-interface with the QoS flow ID for the purpose of marking forwarded packets to the core network. Downlink traffic is marked to enable prioritization in the IP network and in the access node. Similar traffic marking may be used for uplink traffic, according to the operator's configuration. Standardized packet marking informs the QoS enforcement functions of what QoS to provide without any QoS signaling, although the option with QoS signaling offers more flexibility and QoS granularity.

1.2.1.2.2 Radio Network Identifiers

Each entity and bearer in NG-RAN and 5GC are identified with a unique identifier. The identifiers are either permanently provisioned, such as the International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) that are assigned by an operator to the UE, or they are assigned during the lifetime of UE operation in an operator's network. Fig. 1.56 illustrates the identities that are either provisioned or dynamically/semi-statically assigned to the bearers and the entities in 5GS. This section describes the bearers and identifiers that have been introduced in 3GPP 5G specifications. The direction of the arrows in the figure indicates the entity which assigns the identifier and the entity to which the identifier is assigned. The bearers and various bearer identifiers depending on the network interface and the flow direction are also shown in the figure. Note that the protocols over NR-Uu and NG interfaces are divided into two categories: user-plane protocols, which

[61] Service data flow is a fundamental concept in the 3GPP definition of QoS and policy management. Service data flows represent the IP packets related to a user service (web browsing, e-mail, etc.). Service data flows are bound to specific bearers based on policies defined by the network operator. The traffic detection filters, for example, IP packet filter, required in the user-plane function can be configured either in the SMF and provided to the UPF, as service data flow filter(s), or be configured in the UPF, as the application detection filter identified by an application identifier. In the latter case, the application identifier has to be configured in the SMF and the UPF. In this context, service data flow filter is a set of packet flow header parameter values/ranges used to identify one or more of the packet (IP or Ethernet) flows constituting a service data flow. service data flow template is the set of service data flow filters in a policy rule or an application identifier in a policy rule referring to an application detection filter, required for defining a service data flow.

are the protocols implementing the actual PDU session carrying user data through the AS; and the control-plane protocols that are the protocols for controlling the PDU session and the connection between the UE and the network from different aspects including requesting the service, controlling different transmission resources, handover, etc.

In LTE, several radio network temporary identifiers (RNTIs) were used to identify a connected-mode UE within a cell, a specific physical channel, a group of UEs in case of paging, a group of UEs for which power control command is issued by the eNB, system information transmitted for all UEs by the eNB, etc. In general, the RNTIs are used to scramble the CRC part of the radio channel messages. This implies that if the UE does not know the exact RNTI values for each of the cases, it cannot decode the radio channel messages even though the message reaches to the UE. The radio network and UE identifiers in NR, while similar to those of LTE, have been adapted to support new features and functionalities of NR and the 5GC such as multi-connectivity and network slicing. When an NR-compliant UE is connected to 5GC, the following identities are used at cell level to uniquely identify the UE (Fig. 1.63):

- Cell Radio Network Temporary Identifier (C-RNTI) is a unique identification, which is used as an identifier of the RRC connection and for scheduling purposes. In DC scenarios, two C-RNTIs are independently allocated to the UE, one for MCG and one for SCG.
- Temporary C-RNTI, which is used during the random-access procedure, is a random value for contention resolution which during some transient states, the UE is temporarily identified with a random value used for contention resolution purposes.
- Inactive RNTI (I-RNTI) is used to identify the UE context for RRC_INACTIVE.

The following identities are used in NG-RAN for identifying a specific network entity:

- AMF Name is used to identify an AMF. The AMF Name fully-qualified domain name (FQDN) uniquely identifies an AMF, where FQDN consists of one or more labels. Each label is coded as a one octet-length field followed by that number of octets coded as 8 bit ASCII characters. An AMF Set within an operator's network is identified by its AMF Set ID, AMF Region ID, mobile country code (MCC), and mobile network code (MNC).
- NR cell global identifier (NCGI) is used to globally identify the NR cells. The NCGI is constructed from the PLMN identity to which the cell belongs and the NR cell identity (NCI) of the cell. It can be assumed that it is equivalent to CGI in LTE system.
- gNB Identifier (gNB ID) is used to identify gNBs within a PLMN. The gNB ID is contained within the NCI of its cells.
- Global gNB ID is used to globally identify the gNBs, which is constructed from the PLMN identity to which the gNB belongs and the gNB ID. The MCC and MNC are the same as included in the NCGI.
- TAI is used to identify TAs. The TAI is constructed from the PLMN identity to which the TA belongs and the tracking area code (TAC) of the TA.
- S-NSSAI is used to identify a network slice.

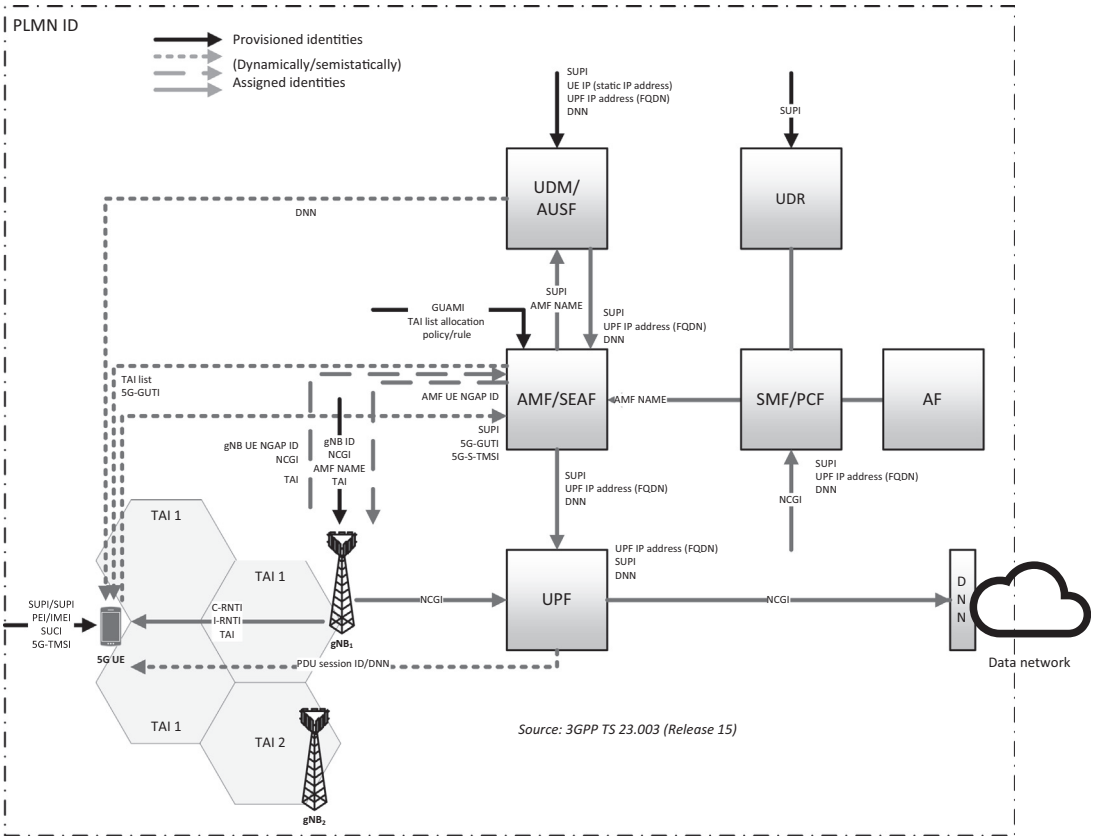


Figure 1.63
NG-RAN/5GC entities and bearers and identifiers.

An application protocol identity (AP ID) is assigned when a new UE-associated logical connection is created in either a gNB or an AMF. An AP ID uniquely identifies a logical connection with a UE over the NG interface or Xn interface within a node (gNB or AMF). Upon receipt of a message that has a new AP ID from the originating node, the receiving node stores the corresponding AP ID for the duration of the logical connection. The definition of AP IDs used over the NG, Xn, or F1 interface are as follows [15]:

- gNB UE NG application protocol (NGAP) ID is used to uniquely identify a UE over the NG interface within a gNB. This identifier is stored by the AMF for the duration of the UE association through the logical NG connection. This identifier is included in all UE associated NGAP signaling.
- AMF UE NGAP ID is allocated to uniquely identify the UE over the NG interface within an AMF. This identifier is stored for the duration of the UE-associated logical NG connection by the gNB. This identifier is included in all UE-associated NGAP signaling once known to the gNB.

- Old gNB UE XnAP ID is used to uniquely identify a UE over the Xn interface within a source gNB and it is stored by the target gNB for the duration of the UE association over the logical Xn connection. This identifier is included in all UE-associated XnAP signaling.
- New gNB UE XnAP ID is used to uniquely identify a UE over the Xn interface within a target gNB. When a source gNB receives a new gNB UE XnAP ID, it stores it for the duration of the UE association over logical Xn connection. This identifier is included in all UE-associated XnAP signaling.
- MgNB UE XnAP ID is allocated to uniquely identify the UE over Xn interface within an MgNB for dual-connectivity. The SgNB stores this identity for the duration of the UE association via logical Xn connection. This identifier is included in all UE-associated XnAP signaling.
- SgNB UE XnAP ID is used to uniquely identify the UE over Xn interface within a SgNB for dual-connectivity. The MgNB stores this identity for the duration of the UE-associated logical Xn connection. This identifier is included in all UE-associated XnAP signaling.
- gNB-CU UE F1AP ID uniquely identifies the UE association over the F1 interface within the gNB-CU.
- gNB-DU UE F1AP ID uniquely identifies the UE association over the F1 interface within the gNB-DU.
- gNB-DU ID is configured at the gNB-DU and is used to uniquely identify the gNB-DU within a gNB-CU. The gNB-DU informs the gNB-CU of its gNB-DU ID during F1 setup procedure. The gNB-DU ID is used over F1AP procedures.

1.2.1.3 User-Plane and Control-Plane Protocol Stacks

This section describes an overview of the NG-RAN protocol structure, protocol layer terminations at various access and core network nodes, as well as the functional split between the NG-RAN and the 5GC. The NG-RAN radio protocols can be divided into control-plane and user-plane categories, where the user-plane protocols are typically responsible for carrying user data and the control-plane protocols are used to transfer signaling and control information.

In general, a communication protocol is a set of rules for message exchange and/or sending blocks of data known as PDUs between network nodes. A protocol may define the packet structure of the data transmitted and/or the control commands that manage the session. A protocol suite consists of several levels of functionality. This modularity facilitates the design and evaluation of protocols. Since each protocol layer usually (logically or physically) communicates with its peer entity across a communication link, they are commonly seen as layers in a stack of protocols, where the lowest protocol layer always deals with physical interaction of the hardware across the communication link. Each higher layer

protocol adds more features or functionalities. User applications usually deal with the top-most layers.

In the context of protocol structure, we will frequently use the terms service and protocol. It must be noted that services and protocols are distinct concepts. A service is a set of primitives or operations that a layer provides to the layer(s) to which it is logically/physically connected. The service defines what operations a layer performs without specifying how the operations are implemented. It is further related to the interface between two adjacent layers. A protocol, in contrast, is a set of rules presiding over the format and interpretation of the information/messages that are exchanged by peer entities within a layer. The entities use protocols to implement their service definitions. Thus a protocol is related to the implementation of a service. The protocols and functional elements defined by 3GPP standards correspond to all layers of the open system interconnection (OSI), that is, the seven-layer network reference model.[62] As shown in Fig. 1.64, what 3GPP considers as layer-2 and layer-3 protocols is mapped to the OSI data link layer. The higher layer protocols in the 3GPP stack are the application and transport layers. The presentation and session layers are often abstracted in practice.

The NG-RAN protocol structure is depicted in Fig. 1.65 for UEs and gNBs in the user plane and control plane. In the control plane, the NAS functional block is used for network attachment, authentication, setting up bearers, and mobility management. All NAS messages are ciphered and integrity protected by the AMF and the UE. There is also a mechanism for transparent transfer of NAS messages. As shown in Fig. 1.66, the layer-2 of NR is divided into MAC, RLC, PDCP, and SDAP sublayers. The SAP or the interface between two adjacent protocol layers is marked with a circle at the interface between the sublayers in the figure. The SAP between the physical layer and the MAC sublayer provides the transport channels. The SAP between the MAC sublayer and the RLC sublayer provides the logical channels. The physical layer provides transport channels to the MAC sublayer. From the physical layer perspective, the MAC sublayer provides and receives services in the form of transport channels. The data in a transport channel is organized into transport blocks. By

[62] Open systems interconnection is a standard description or a reference model for the computer networks which describes how messages should be transmitted between any two nodes in the network. Its original purpose was to guide product implementations to ensure consistency and interoperability between products from different vendors. This reference model defines seven layers of functions that take place at each end of a communication link. Although open systems interconnection is not always strictly adhered to in terms of grouping, the related functions together in a well-defined layer, many if not most products involved in telecommunication make an attempt to describe themselves in relation to the open systems interconnection model. Open systems interconnection was officially adopted as an international standard by the International Organization of Standards and it is presently known as Recommendation X.200 from ITU-T. The layers of open systems interconnection model are classified into two groups. The upper four layers are used whenever a message passes from or to a user. The lower three layers (up to the network layer) are used when any message passes through the host computer.

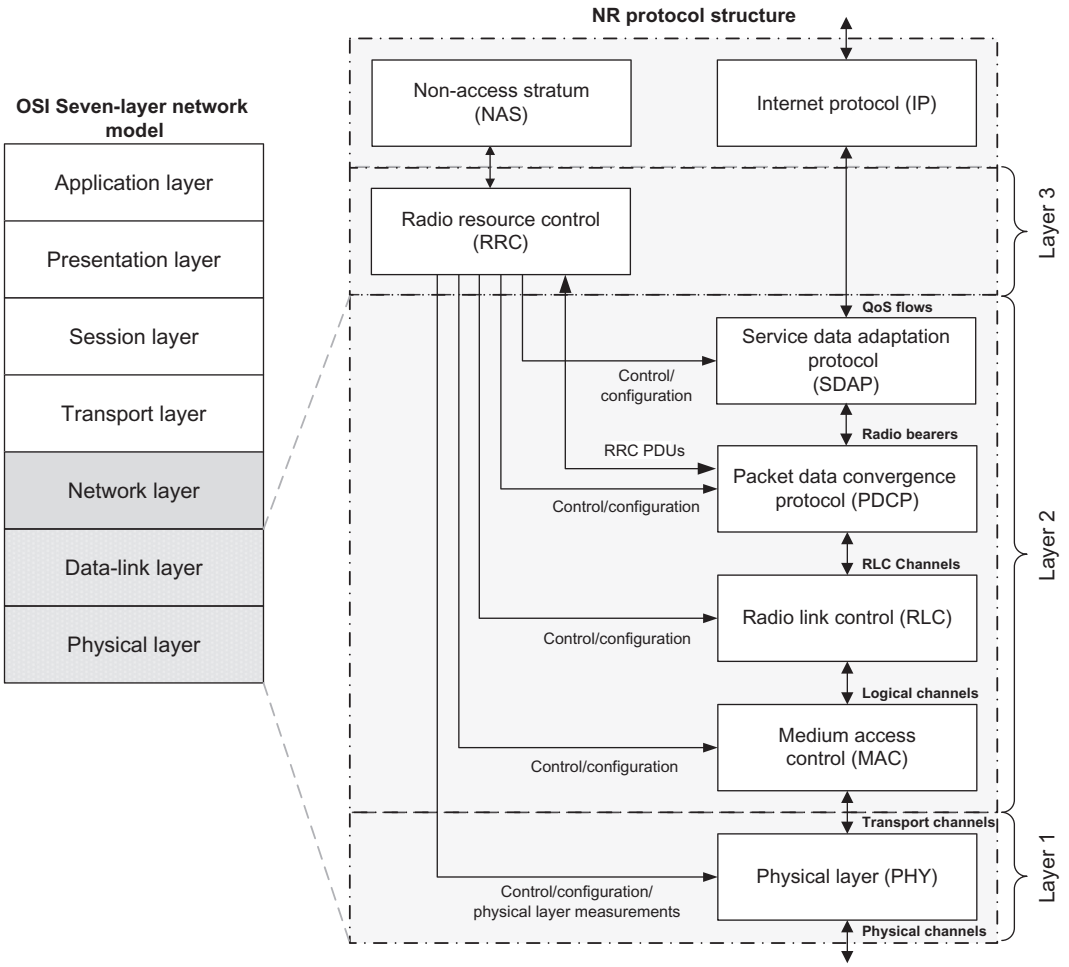


Figure 1.64
Mapping of lower NR protocol layers to OSI network reference model.

varying the transmission format of the transport blocks, the MAC sublayer can realize different data rates and reliability levels. The MAC sublayer receives the RLC SDUs mapped to various logical channels in the downlink, and generates the MAC PDUs that further become the transport blocks in the physical layer. The RLC sublayer provides RLC channels to the PDCP sublayer and the latter provides radio bearers to the SDAP sublayer. As we mentioned earlier, radio bearers are classified into data radio bearers for user-plane data and SRBs for control-plane information. The SDAP sublayer is configured by RRC and maps QoS flows to DRBs where one or more QoS flows may be mapped into one DRB in the downlink; however, one QoS flow is mapped into only one DRB at a time in the uplink

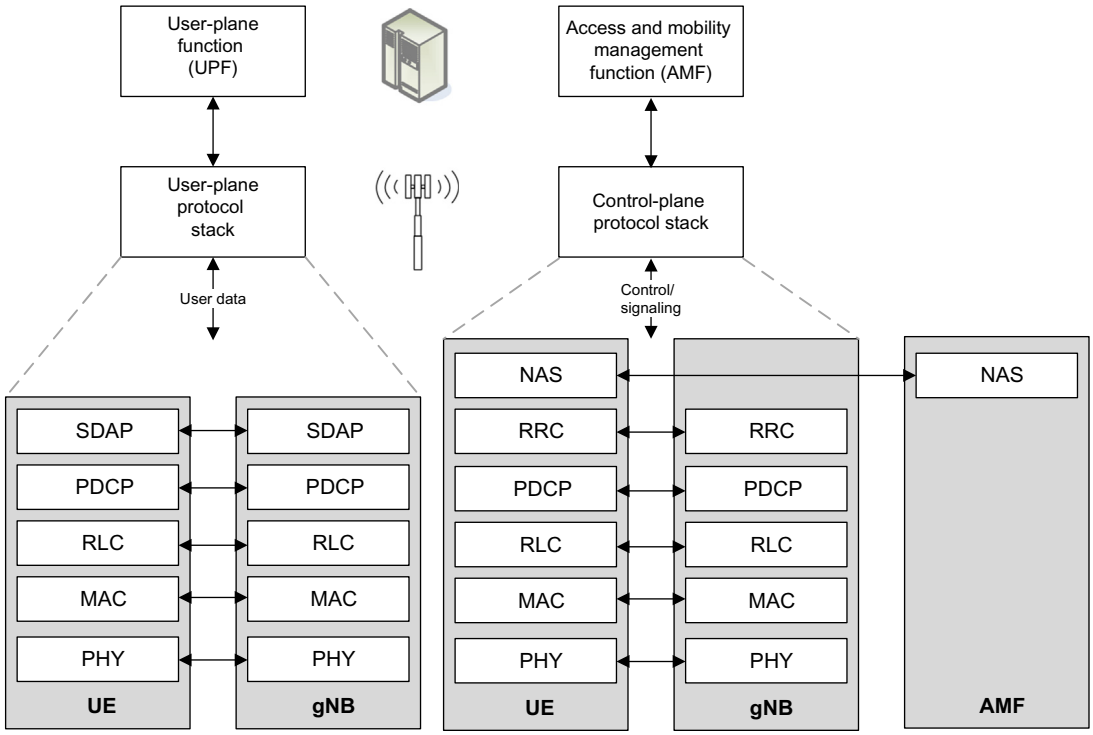


Figure 1.65
NG-RAN protocol stack [16].

[16]. The introduction of a new sublayer in NR layer-2 was meant to support the improved flow-based QoS model in NR as opposed to bearer-based QoS model in LTE.

MAC sublayer is responsible for mapping between logical channels and transport channels and multiplexing/de-multiplexing of MAC SDUs belonging to one or different logical channels to transport blocks which are delivered to or received from the physical layer through the transport channels. The MAC sublayer further handles scheduling and UE measurements/reporting procedures as well as error correction through HARQ (one HARQ entity per carrier in case of CA). It further manages user prioritization via dynamic scheduling, priority handling among logical channels of one UE through logical channel prioritization. A single MAC instantiation can support one or more OFDM numerologies, transmission timings as well as mapping restrictions on logical channels. In case of CA, the multi-carrier properties of the physical layer are only exposed to the MAC sublayer. In that case, one HARQ entity is required per serving cell. In both uplink and downlink, there is one independent HARQ entity per serving cell and one transport block is generated per transmission time interval per serving cell in the absence of spatial multiplexing. Each transport block and the associated HARQ retransmissions are mapped to a single serving cell [16].

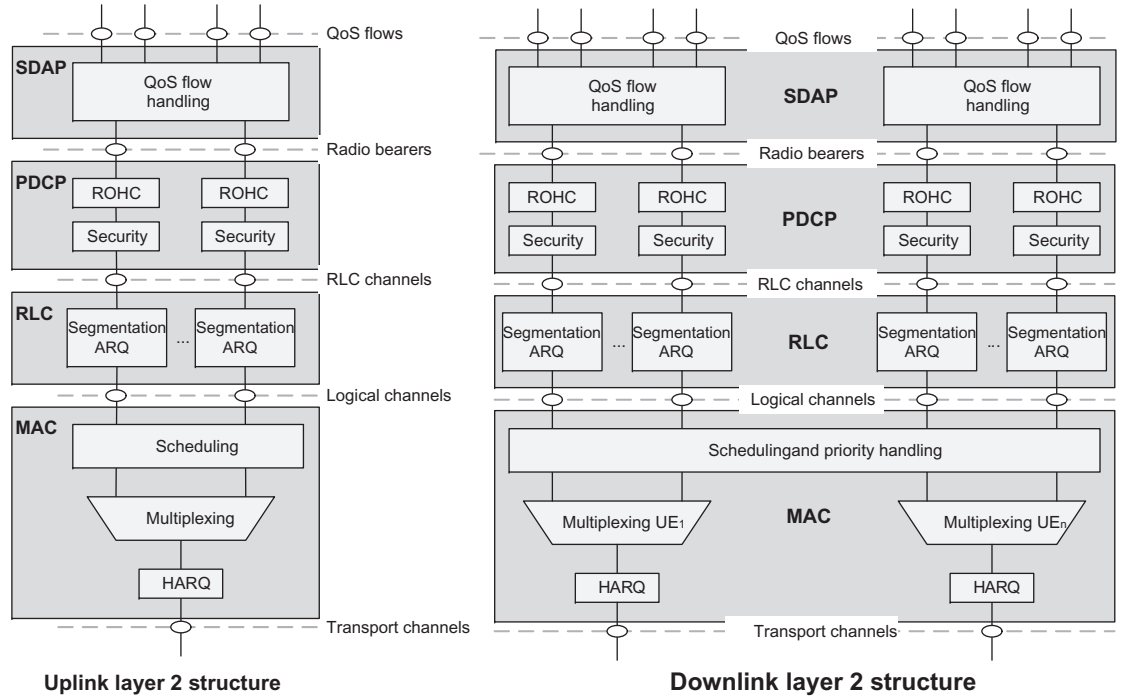


Figure 1.66
3GPP NR DL/UL layer-2 protocol structure [16].

MAC sublayer provides different type of data transfer services through mapping of logical channels to transport channels. Each logical channel type is defined by the type of information being transferred. Logical channels are classified into two groups of control and traffic channels. In NR, the control channels are used for transport of control-plane information and are of the following types (see Fig. 1.67):

- Broadcast control channel (BCCH) is a downlink channel for broadcasting system control information.
- Paging control channel (PCCH) is a downlink channel that transports paging and system information change notifications.
- Common control channel (CCCH) is a logical channel for transmitting control information between UEs and the network when the UEs have no RRC connection with the network.
- Dedicated control channel (DCCH) is a point-to-point bidirectional channel that transmits UE-specific control information between a UE and the network and is used by the UEs that have established RRC connection with the network.

Traffic channels are used for the transfer of user-plane information and are of the following type:

- Dedicated traffic channel (DTCH) is a UE-specific point-to-point channel for transport of user information which can exist in both uplink and downlink.

The physical layer provides information transfer services to the MAC and higher layers. The physical layer transport services are described by how and with what characteristics data is transferred over the radio interface. This should be clearly distinguished from the classification of what is transported which relates to the concept of logical channels in the

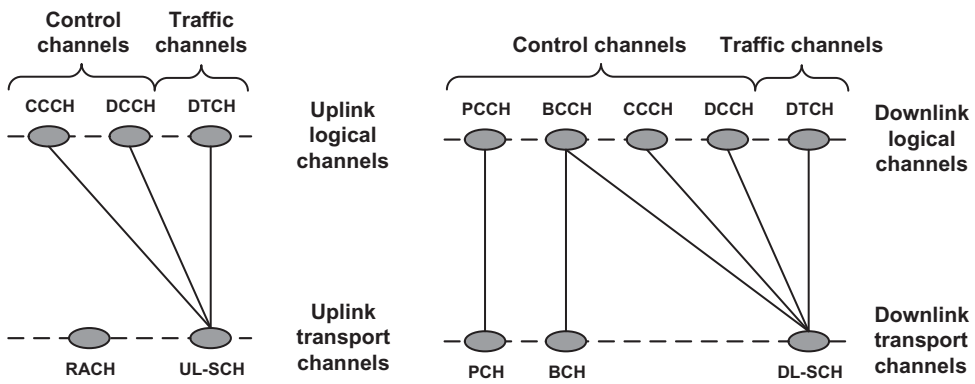


Figure 1.67
Mapping of logical and transport channels [16].

MAC sublayer. In the downlink, the logical channels and transport channels are mapped as follows (see Fig. 1.67):

- BCCH can be mapped to broadcast channel (BCH), which is characterized by fixed, predefined transport format, and is required to be broadcast in the entire coverage area of the cell. A DL-SCH may support receptions using different numerologies and/or TTI duration within the MAC entity. An UL-SCH may also support transmissions using different numerologies and/or TTI duration within the MAC entity.
- BCCH can be mapped to downlink shared channel(s) (DL-SCH), which is characterized by support for HARQ protocol, dynamic link adaptation by varying modulation, coding, and transmit power, possibility for broadcast in the entire cell, possibility to use beamforming, dynamic and semistatic resource allocation, and UE discontinuous reception (DRX) to enable power saving.
- PCCH can be mapped to paging channel (PCH), which is characterized by support for UE DRX in order to enable power saving, requirement for broadcast in the entire coverage area of the cell, and is mapped to physical resources which can also be used dynamically for traffic or other control channels. This channel is used for paging when the network does not know the location of the UE.
- Common control channel (CCCH) can be mapped to DL-SCH and represents a logical channel for transmitting control information between UEs and gNBs. This channel is used for UEs that have no RRC connection with the network.
- Dedicated control channel (DCCH) can be mapped to DL-SCH and is a point-to-point bidirectional channel that transmits dedicated control information between a UE and the network. It is used by UEs that have already established RRC connection.
- Dedicated traffic channel (DTCH) can be mapped to DL-SCH and represents a point-to-point bidirectional channel dedicated to a single UE for the transfer of user information.

In the uplink, the logical channels and the transport channels are mapped as follows:

- CCCH can be mapped to uplink shared channel(s) (UL-SCH), which is characterized by possibility to use beamforming, support for dynamic link adaptation by varying the transmit power and modulation and coding schemes, support for HARQ, support for both dynamic and semistatic resource allocation.
- DCCH can be mapped to UL-SCH.
- DTCH can be mapped to UL-SCH.
- Random access channel(s) (RACH), which is characterized by limited control information and collision risk.

The RLC sublayer is used to format and transport traffic between the UE and the gNB. The RLC sublayer provides three different reliability modes for data transport: acknowledged mode (AM), unacknowledged mode (UM), and transparent mode (TM). The UM is suitable for transport of real-time services since such services are delay-sensitive and cannot

tolerate delay due to ARQ retransmissions. The acknowledged mode is appropriate for non-real-time services such as file transfers. The transparent mode is used when the size of SDUs are known in advance such as for broadcasting system information. The RLC sublayer also provides sequential delivery of SDUs to the upper layers and eliminates duplicate packets from being delivered to the upper layers. It may also segment the SDUs. The RLC configuration is defined per logical channel with no dependency on numerologies and/or TTI durations, and ARQ can operate with any of the numerologies and/or TTI durations for which the logical channel is configured. For SRB0, paging and broadcast system information, RLC TM mode is used. For other SRBs, RLC AM mode is used. For DRBs, either RLC UM or AM mode is used.

The services and functions provided by the PDCP sublayer in the user plane include header compression/decompression of IP packets; transfer of user data between NAS and RLC sublayer; sequential delivery of upper layer PDUs and duplicate detection of lower layer SDUs following a handover in RLC acknowledged mode; retransmission of PDCP SDUs following a handover in RLC acknowledged mode; and ciphering/deciphering and integrity protection. The services and functions provided by the PDCP for the control plane include ciphering and integrity protection and transfer of control-plane data where PDCP receives PDCP SDUs from RRC and forwards them to the RLC sublayer and vice versa.

The main services and functions provided by SDAP sublayer include mapping between a QoS flow and a DRB and marking QoS flow IDs in downlink and uplink packets. A single instantiation of SDAP protocol is configured for each individual PDU session, with the exception of dual-connectivity mode, where two entities can be configured.

The RRC sublayer in the gNB makes handover decisions based on neighbor cell measurements reported by the UE; performs paging of the users over the air-interface; broadcasts system information; controls UE measurement and reporting functions such as the periodicity of channel quality indicator reports; and further allocates cell-level temporary identifiers to the active users. It also executes transfer of UE context from the serving gNB to the target-gNB during handover and performs integrity protection of RRC messages. The RRC sublayer is responsible for setting up and maintenance of radio bearers. Note that the RRC sublayer in 3GPP protocol hierarchy is considered as layer-3 protocol [16].

Fig. 1.68 shows an example of layer-2 data flow and packet processing, where a transport block is generated by MAC sublayer by concatenating two RLC PDUs from the radio bearer RB_x and one RLC PDU from the radio bearer RB_y. In this figure, H denotes the layer-specific headers or subheaders of each sublayer. The two RLC PDUs from RB_x each corresponds to one of the IP packets n and $n + 1$, while the RLC PDU from RB_y is a segment of the IP packet m.

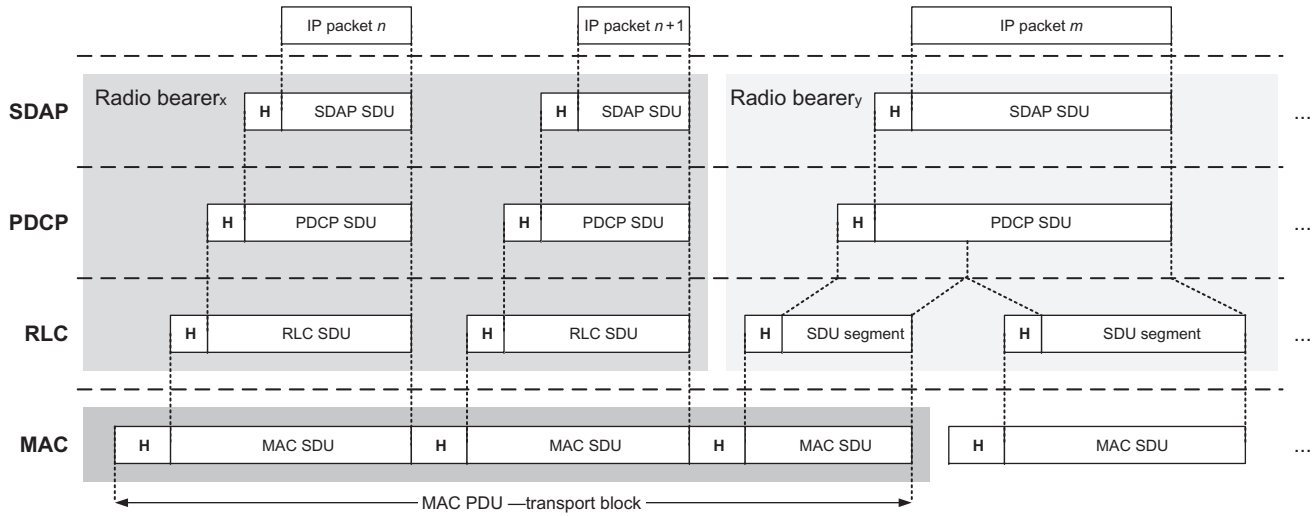


Figure 1.68
Example of layer-2 packet processing in NR [16].

1.2.2 Core Network

The design of 5G core network architecture in 3GPP was based on the following design principles in order to allow efficient support of new service networks such as information-centric networking (ICN)[63] [81]:

- Control- and user-plane separation (CUPS): This was a departure from LTE's vertically integrated control/user-plane network design to the one adopting NFV framework with modular NFs decoupled from the hardware for service centricity, flexibility, and programmability. In doing so, NFs are going to be implemented both physically and virtually, while allowing each to be customized and scaled based on their individual requirements, also allowing the realization of multi-slice coexistence. This further allows the introduction of UPF with new control functions, or reusing/extending the existing ones, to manage the new user-plane realizations.
- Decoupling of RAT and core network: Unlike LTE's unified control plane for access and the core networks, 5GC offers control-plane separation of RAN from the core network. This allows introduction of new radio access technologies and mapping of multiple heterogeneous RAN sessions to arbitrary core network slices based on service requirements.
- Non-IP PDU session support: A PDU session is defined as the logical connection between the UE and the data network. The PDU session establishment in 5GC supports both IP and non-IP PDUs (known as unstructured payloads), and this feature can potentially allow the support for ICN PDUs by extending or reusing the existing control functions.
- Service-centric design: 5GC service orchestration and control functions, such as naming, addressing, registration/authentication, and mobility, will utilize cloud-based service APIs. This enables open interfaces for authorized service function interaction and creating service-level extensions to support new network architectures. These APIs include widely used approaches, while not precluding the use of procedural approach between functional units.

Compared to LTE core network, where PDU session states in RAN and core were synchronized from session management perspective, 5GC decouples those states by allowing PDU

[63] Information-centric networking is an approach to evolve the Internet infrastructure away from a host-centric paradigm based on perpetual connectivity and the end-to-end principle, to a network architecture in which the focus is on content or data. In other words, information-centric networking is an approach to evolve the Internet infrastructure to directly support information distribution by introducing uniquely named data as a core Internet principle. Data becomes independent from location, application, storage, and means of transportation, enabling or enhancing a number of desirable features, such as security, user mobility, multicast, and in-network caching. Mechanisms for realizing these benefits is the subject of ongoing research in Internet Engineering Task Force and elsewhere. Current research challenges in information-centric networking includes naming, security, routing, system scalability, mobility management, wireless networking, transport services, in-network caching, and network management.

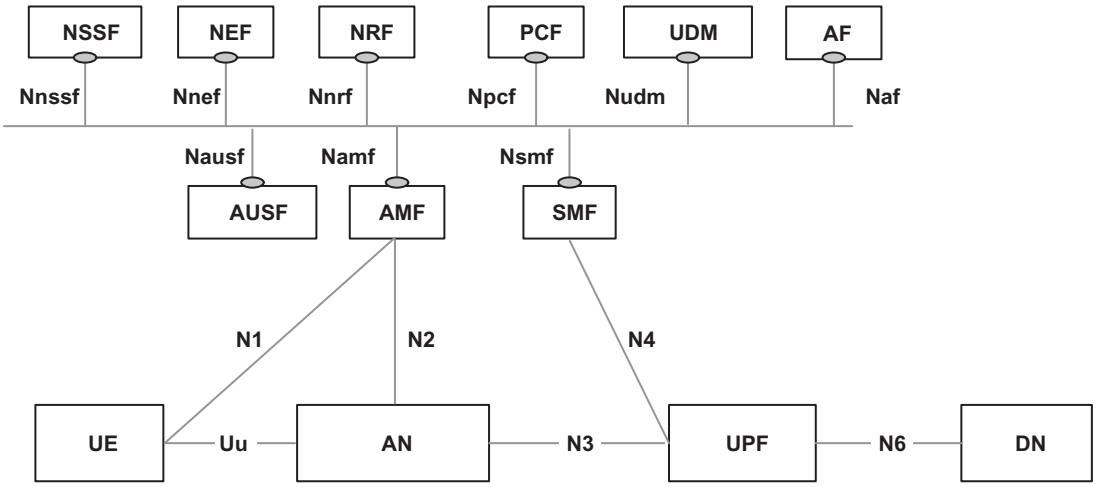


Figure 1.69
5G system service-based reference architecture [3].

sessions to be defined prior to a PDU session request by a UE. This de-coupling allows dynamic and policy-based interconnection of UE flows with slices provisioned in the core network. The SMF is used to handle IP anchor point selection and addressing functionality, management of the user-plane state in the UPFs such as in uplink classifier and branching point functions during PDU session establishment, modification and termination, and interaction with RAN to allow PDU session forwarding in UL/DL to the respective data networks. In the user plane, UE's PDUs are tunneled to the RAN using the 5G RAN protocols. From the RAN perspective, the PDU's five-tuple header information (IP source/destination, port, protocol, etc.) is used to map the flow to an appropriate tunnel from RAN to UPF.

1.2.2.1 Reference Architecture: Network Entities and Interfaces

The 5G core network architecture comprises a number of NFs,[64] some of which have newly been introduced. In this section, we provide a brief functional description of these NFs. Fig. 1.69 illustrates the 5GC service-based reference architecture. Service-based interfaces are used within the control plane. The main 5GC network entities include the following [3]:

Fig. 1.70 depicts the 5G system architecture in the non-roaming case, using the reference-point representation showing how various NFs interact with each other. Note that the

[64] NF is a 3GPP-adopted processing function in next generation network that has both functional behavior and interface. An NF can be implemented either as a network element on a dedicated hardware, as a software instance running on a dedicated hardware, or as a virtualized function instantiated on an appropriate platform such as cloud infrastructure.

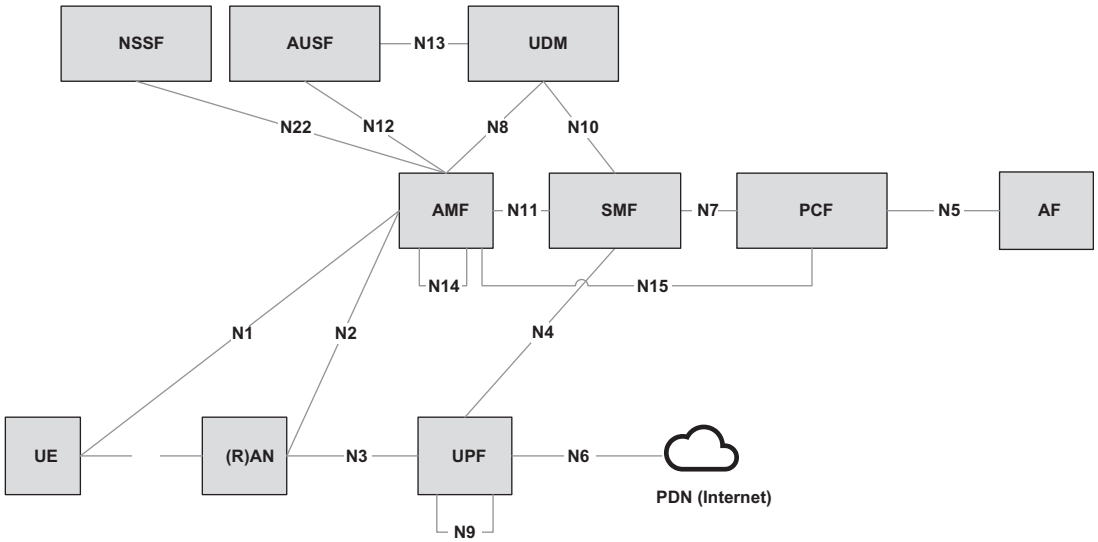


Figure 1.70
Non-roaming reference-point representation of 5G system architectures [3].

service-based and reference-point representations are two different representations of the 5GC which make it distinguished from LTE EPC. Service-based interfaces and reference points are two different ways to model interactions between architectural entities. A reference point is a conceptual point at the conjunction of two non-overlapping functional groups. A reference point can be replaced by one or more service-based interfaces that provide equivalent functionality. A unique reference point exists between two NFs, which means even if the functionality of two reference points is the same with different NFs, different reference point names must be assigned. However, when service-based interface representation is used, the same service-based interface is assigned if the functionality is equal on each interface.The functional description of the network functions is as follows [3]:

- Authentication server function (AUSF) is responsible for performing authentication process with the user terminals.
- AMF is responsible for termination of RAN control-plane interface (N2) and NAS (N1); ciphering and integrity protection of NAS messages; registration management; connection management; mobility management; lawful interception; transport of session management messages between UE and SMF; transparent proxy for routing session management messages; access authentication and authorization; and security anchor function (SEAF) and security context management (SCM). In addition to the functionalities described earlier, the AMF may support functions associated with non-3GPP ANs.
- Data network (DN) comprises operator's services, Internet access, or other services.

- Unstructured data storage network function (UDSF) is an optional function that supports storage and retrieval of information as unstructured data by any NF and the deployments can choose to collocate UDSF with other NFs such as UDR.
- Network exposure function (NEF) to securely expose the services and capabilities provided by 3GPP NFs, internal exposure/reexposure, AFs, and the edge computing. In addition, it provides a means for the AFs to securely provide information to 3GPP network, for example, mobility pattern. In that case, the NEF may authenticate, authorize, and regulate the AFs. It translates information exchanged with the AF and information exchanged with the internal NF. For example, it translates between an AF-service-identifier and internal 5G core information. The NEF receives information from other NFs based on exposed capabilities of other NFs. It may implement a frontend entity to store the received information as structured data using a standardized interface to a unified data repository (UDR).
- NF repository function (NRF) supports service discovery function; receives NF discovery request from NF instance; and provides the information of the discovered NF instances to the NF instance. It further maintains the NF profile of available NF instances and their supported services.
- NSSF selects the set of NSIs to serve a UE and to determine the allowed NSSAI and to determine the AMF set to serve the UE or depending on the configuration, a list of candidate AMF(s).
- Policy control function (PCF) supports interactions with the access and mobility policy enforcement in the AMF through service-based interfaces and further provides access and mobility management-related policies to the AMF.
- SMF handles session management (session establishment, modification, and release); UE IP address allocation and management; selection and control of UPF; traffic steering configuration at UPF to route traffic to the proper destination; termination of interfaces toward PCFs; control part of policy enforcement and QoS; and lawful interception among other functions.
- Unified data management (UDM) supports generation of 3GPP authentication and key agreement (AKA)[65] authentication credentials; user identification handling; access authorization based on subscription data; UE's serving NF registration management; service/session continuity; lawful interception functionality; subscription management; and SMS management. To provide these functions, the UDM uses subscription data (including authentication data) that may be stored in the UDR, in that case the UDM implements the application logic and does not require an internal user data storage, thus

[65] Authentication and key agreement is a mechanism which performs authentication and session key distribution in UMTS networks. Authentication and key agreement is a challenge-response-based mechanism that uses symmetric cryptography. Authentication and key agreement is typically run on a UMTS IP multimedia services identity module, which resides on a smart card device that also provides tamper-resistant storage of shared secrets. Authentication and key agreement is defined in IETF RFC 3310.

different UDMs may serve the same user in different transactions. The UDM is located in the home PLMN of the subscribers which it serves and accesses the information of the UDR located in the same PLMN.

- UDR supports storage and retrieval of subscription data by the UDM; storage and retrieval of policy data by the PCF; storage and retrieval of structured data for exposure; and application data by the NEF, including packet flow descriptions for application detection, and application request information for multiple UEs. During the deployments, the operators can opt to co-locate UDR with UDSF.
- Non-3GPP interworking function (N3IWF) supports untrusted non-3GPP access to 5GC. It further supports IPsec tunnel establishment with the UE; terminates the IKEv2[66] or IPsec[67] protocols with the UE over NWu and relays over N2 the information needed to authenticate the UE and authorize its access to the 5G core network as well as termination of N2 and N3 interfaces to 5G core network for control plane and user plane, respectively; relaying uplink and downlink control-plane NAS (N1) signaling between the UE and AMF; handling of N2 signaling from SMF related to PDU sessions and QoS; and establishment of IPsec security association (IPsec SA) to support PDU session traffic.
- UPF acts as the anchor point for intra-RAT or inter-RAT mobility; external PDU session point of interconnect to the data network; packet routing and forwarding; packet inspection and user-plane part of policy rule enforcement; lawful interception; traffic usage reporting; uplink classifier to support routing traffic flows to a data network; branching point to support multi-homed PDU session; QoS handling for user plane (packet filtering, gating, and UL/DL rate enforcement); uplink traffic verification (SDF to QoS flow mapping); transport-level packet marking in the uplink and downlink; and downlink packet buffering and downlink data notification triggering.
- AF is responsible for interacting with the 3GPP core network in order to support application influence on traffic routing; accessing network exposure function; and interacting with the policy framework for policy control. Based on operator deployment, the AF is considered to be trusted by the operator and can be allowed to interact directly with relevant NFs.

[66] IKE or IKEv2 is the protocol used to set up a security association in the IPsec protocol suite. The IKE protocol is based on a key-agreement protocol and the Internet security association and key management protocol which is a protocol defined by IETF RFC 2408 for establishing security associations and cryptographic keys in an Internet environment. The IKE uses X.509 certificates for authentication which are either pre-shared or distributed to set up a shared session secret from which cryptographic keys are derived. In addition, a security policy for every peer which will connect must be manually maintained.

[67] IPsec is a set of protocols for securing IP-based communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

- Security edge protection proxy is a non-transparent proxy which supports message filtering and policing inter-PLMN control-plane interfaces and topology hiding.
- User equipment
- Access network

Reference-point representation of the architecture can be used to develop detailed call flows in the normative standardization. N1 is defined to carry signaling between UE and AMF. The reference points for connecting AN and AMF and AN and UPF are defined as N2 and N3, respectively. There is no reference point between AN and SMF, but there is a reference point, N11, between AMF and SMF. Therefore, the SMF is controlled by AMF. N4 is used by SMF and UPF so that the UPF can be configured using the control information generated by the SMF, and the UPF can report its state to the SMF. N9 is the reference point for the connection between different UPFs, and N14 is the reference point connecting different AMFs. N15 and N7 are defined for the PCF to apply policies to AMF and SMF, respectively. N12 is required for the AMF to perform authentication of the UE. N8 and N10 are defined to provide the UE subscription data to AMF and SMF.

The 5G core network supports UE connectivity via untrusted non-3GPP access networks such as Wi-Fi. Non-3GPP access networks can connect to the 5G core network via a non-3GPP interworking function (N3IWF). The N3IWF interfaces the 5G core network control plane and UPFs via N2 and N3 interfaces, respectively, with the external network. The N2 and N3 reference points are used to connect stand-alone non-3GPP access networks to 5G core network control plane function and UPF, correspondingly. A UE that attempts to access the 5G core network over a stand-alone non-3GPP access, after UE attachment, must support NAS signaling with 5G core network control-plane functions using N1 reference point. When the UE is connected via a NG-RAN and via a stand-alone non-3GPP access, multiple N1 instances could exist for the UE, that is, there is one N1 instance over NG-RAN and one N1 instance over non-3GPP access [3].

1.2.2.2 PDN Sessions and 5GC Identifiers

In an LTE network, once a UE connects to a PDN using the IP address assigned to it upon successful initial attach to the network, the IP connection remains in place after a default EPS bearer is established over the LTE network and until the UE detaches from the LTE network (i.e., the PDN connection is terminated). Even when there is no user traffic to send, the default EPS bearer always stays activated and ready for possible incoming user traffic. Additional EPS bearers can be established, if the best effort QoS attributes of the default EPS bearer do not satisfy the service requirements. The additional EPS bearer is called a dedicated EPS bearer, where multiple dedicated bearers can be created, if required by the user or the network. When there is no user traffic, the dedicated EPS bearers can be removed. Dedicated EPS bearers are linked to a default EPS bearer. Therefore, IP traffic from or to a UE is delivered through an EPS bearer depending on the required QoS class

over the LTE network. Uplink IP traffic is mapped from a UE to the EPS bearer while downlink IP traffic is mapped from a PGW to the EPS bearer. Each E-RAB is associated with a QCI and an allocation and retention priority (ARP), where each QCI is characterized by priority, packet delay budget (PDB), and acceptable packet loss rate.

The 5G core network supports PDU connectivity service, that is, a service that provides exchange of PDUs between a UE and a data network. The PDU connectivity service is supported via PDU sessions that are established upon request from the UE. The PDU sessions are established (upon UE request), modified (upon UE and 5GC request), and released (upon UE and 5GC request) using NAS session management signaling over N1 between the UE and the SMF. Upon request from an application server, 5GC is able to trigger a specific application in the UE. The UE conveys the message to the application upon receiving the trigger message. Note that unlike LTE, 3GPP NR Rel-15 does not support dual-stack PDU session. The 5GC supports dual-stack UEs using separate PDU sessions for IPv4 and IPv6. In 3GPP NR, the QoS granularity is refined further to the flow level. In a typical case, multiple applications will be running on a UE; however, in LTE eNB, each E-RAB does not have an associated QCI or an ARP, whereas in NR, the SDAP sublayer can be configured by RRC sublayer to map QoS flows to DRBs. One or more QoS flows may be mapped to one DRB. Thus, QFI is used to identify a QoS flow within the 5G system. User-plane traffic with the same QFI within a PDU session receives the same traffic forwarding treatment (e.g., scheduling, admission threshold, etc.). The QFI is carried in an encapsulation header on N3 and is unique within a PDU session.

The 5GC is access-agnostic and allows running the N1 reference point on non-3GPP radio access schemes such as Wi-Fi. The UE can also send NAS messages for session and mobility management to the 5GC via a non-3GPP access, which was not possible in the previous 3GPP radio access standards. Non-access stratum is the signaling protocol of the UE for mobility and session-related control messages, which requires a new security procedure in order to authenticate the UE over the non-3GPP access with the AMF in the 3GPP network. Non-3GPP access networks must be connected to the 5G core network via N3IWF entity. The N3IWF interfaces the 5G core network control-plane function and UPF via N2 and N3 interfaces, respectively. When a UE is connected via an NG-RAN and via a stand-alone non-3GPP access, multiple N1 instances, that is, one N1 instance over NG-RAN and one N1 instance over non-3GPP access, will be created. The UE is simultaneously connected to the same 5G core network of a PLMN over a 3GPP access and a non-3GPP access and is served by a single AMF provided that the selected N3IWF is located in the same PLMN as the 3GPP access. However, if the UE is connected to the 3GPP access network of a PLMN and if it selects an N3IWF which is located in a different PLMN, then the UE will be served separately by two PLMNs. The UE is registered with two separate AMFs. The PDU sessions over 3GPP access are served by the visiting SMFs which are different from the ones serving the PDU sessions over the non-3GPP access. The UE establishes an IPsec tunnel

with N3IWF in order to attach to the 5G core network over the untrusted non-3GPP access and is authenticated by and attached to the 5G core network during the IPsec tunnel establishment procedure [3].

The network identifiers in 5G system are divided into subscriber identifiers and UE identifiers. Each subscriber in the 5G system is assigned a 5G subscription permanent identifier (SUPI) to use within the 3GPP system. The 5G system treats subscription identification independent of the UE identification. In that sense, each UE accessing the 5G system is assigned a permanent equipment identifier (PEI). The 5G system assigns a temporary identifier (5G-GUTI) to the UE in order to protect user confidentiality. The 5G network identifiers can be summarized as follows [3]:

- 5G Subscription Permanent Identifier is a global unique identifier that is assigned to each subscriber in the 5G system, which is provisioned in the UDM/UDR. The SUPI is used only within 3GPP system. The previous generations' IMSI[68] and network access identifier (NAI)[69] can still be used in 3GPP Rel-15 as SUPI. The use of generic NAI makes the use of non-IMSI-based SUPIs possible. The SUPI must contain the address of the home network in order to enable roaming scenarios. For interworking with the EPC, the SUPI allocated to the 3GPP UE is based on the IMSI. Furthermore, 5GS defines a subscription concealed identifier (SUCI) which is a privacy preserving identifier containing the concealed SUPI.
- Permanent Equipment Identifier is defined for a 3GPP UE accessing the 5G system. The PEI can assume different formats for different UE types and use cases. The UE presents the PEI to the network along with an indication of the PEI format being used. If the UE supports at least one 3GPP access technology, the UE must be allocated a PEI in the IMEI format. In 3GPP Rel-15, the only format supported for the PEI parameter is an IMEI.
- 5G Globally Unique Temporary Identifier is allocated by an AMF to the UE that is common in both 3GPP and non-3GPP access. A UE can use the same 5G-GUTI for

[68] International Mobile Subscriber Identity (IMSI) is used as a unique identification of mobile subscriber in the 3GPP networks. The IMSI consists of three parts: (1) mobile country code consisting of three digits. The mobile country code uniquely identifies the country of residence of the mobile subscriber; (2) mobile network code consisting of two or three digits for 3GPP applications. The mobile network code identifies the home public land mobile network of the mobile subscriber. The length of the mobile network code (two or three digits) depends on the value of the mobile country code; and (3) mobile subscriber identification number identifying the mobile subscriber within a public land mobile network.

[69] Network access identifier defined by IETF RFC 7542 is a common format for user identifiers submitted by a client during authentication. The purpose of the network access identifier is to allow a user to be associated with an account name, as well as to assist in the routing of the authentication request across multiple domains. Note that the network access identifier may not necessarily be the same as the user's email address or the user identifier submitted in an application-layer authentication.

accessing 3GPP access and non-3GPP access security context within the AMF. The AMF may assign a new 5G-GUTI to the UE at any time. The AMF may delay updating the UE with its new 5G-GUTI until the next NAS signaling exchange. The 5G-GUTI comprises a GUAMI and a 5G-TMSI, where GUAMI identifies the assigned AMF and 5G-TMSI identifies the UE uniquely within the AMF. The 5G-S-TMSI is the shortened form of the GUTI to enable more efficient radio signaling procedures.

- AMF Name is used to identify an AMF. It can be configured with one or more GUAMIs. At any given time, the GUAMI value is exclusively associated to one AMF name.
- Data Network Name (DNN) is equivalent to an APN which may be used to select an SMF and UPF(s) for a PDU session, to select N6 interface(s) for a PDU session, or to determine policies that are applied to a PDU session.
- Internal-Group Identifier is used to identify a group as the subscription data for a UE in UDM may associate the subscriber with different groups. A UE can belong to a limited number of groups. The group identifiers corresponding to a UE are provided by the UDM to the SMF and when PCC applies to a PDU session by the SMF to the PCF. The SMF may use this information to apply local policies and to store this information in charging data record.
- Generic Public Subscription Identifier (GPSI) is used for addressing a 3GPP subscription in different data networks outside of the 3GPP system. The 3GPP system stores within the subscription data the association between the GPSI and the corresponding SUPI. GPSIs are public identifiers used both inside and outside of the 3GPP system. The GPSI is either a mobile subscriber ISDN number (MSISDN) or an external identifier. If MSISDN is included in the subscription data, it will be possible that the same MSISDN value is supported in both 5GS and EPS. There is no one-to-one relationship between GPSI and SUPI.

1.2.2.3 User-Plane and Control-Plane Protocol Stacks

1.2.2.3.1 Control-Plane Protocol Stacks

The 5GC supports PDU connectivity service which provides exchange of PDUs between a UE and a data network. The PDU connectivity service is supported through PDU sessions that are established upon request from the UE. In order to establish a PDU session and access to the PDN, the UE must establish user plane and control plane over the NG-RAN and the 5GC network interfaces to the PDN. Connection management comprises establishing and releasing a signaling connection between a UE and the AMF over N1. This signaling connection is used to enable NAS signaling exchange between the UE and the core network, which includes both access network signaling connection between the UE and the access node (RRC connection over 3GPP access or UE-N3IWF connection over non-3GPP access) and the N2 connection for this UE between the access node and the AMF. A NAS connection over N1 is used to connect a UE to the AMF. This NAS connection is used for

registration management and connection management functions as well as for transport of session management messages and procedures for the UE. The NAS protocol over N1 comprises NAS mobility and session management (NAS-MM and NAS-SM) components. There are several protocol information that need to be transported over N1 using NAS-MM protocol between a UE and a core NF besides the AMF (e.g., session management signaling). Note that in 5G systems, registration/connection management NAS messages and other types of NAS messages as well as the corresponding procedures are decoupled. The NAS-MM supports NAS procedures that terminate at the AMF such as handling registration and connection management state machines and procedures of the UE, including NAS transport. There is a single NAS protocol that applies to both 3GPP and non-3GPP access. When a UE is served by a single AMF while it is connected through multiple (3GPP and/or non-3GPP) access schemes, there would be one N1 NAS connection per access link. The security for the NAS messages is provided based on the security context established between the UE and the AMF. It is possible to transmit the other types of NAS messages (e.g., NAS SM) along with RM/CM NAS messages by supporting NAS transport of different types of payload or messages that do not terminate at the AMF. This includes information about the payload type, information for forwarding purposes, and the SM message in case of SM signaling.

The NAS-SM messages control the session management functions between the UE and the SMF. The session management message is created and processed in the NAS-SM layer of UE and the SMF (see Fig. 1.71). The content of the NAS-SM message is transparent to the AMF. The NAS-MM layer creates a NAS-MM message, including security header, indicating NAS transport of SM signaling, as well as additional information for the receiving NAS mobility management (NAS-MM) entity to determine how and where to forward the SM signaling message. The receiving NAS-MM layer performs integrity check and interpretation of NAS message content. Fig. 1.71 further depicts the NAS-MM layer, which is a NAS protocol for mobility management; support of registration management; connection

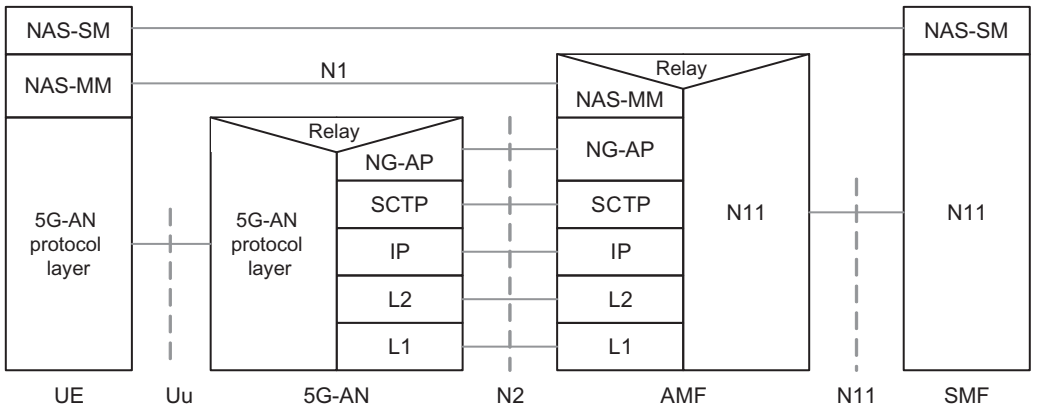


Figure 1.71
Control-plane protocol stack between the UE and the AMF/SMF [3].

management and user-plane connection activation and deactivation functions. It is also responsible for ciphering and integrity protection of NAS signaling.

The UE and AMF support NAS signaling connection setup function, which is used to establish a NAS signaling connection for a UE in CM-IDLE state. It will be explained in the next chapter that two connection management states are used to reflect the NAS signaling connectivity between the UE and the AMF, that is, CM-IDLE and CM-CONNECTED. The CM state for 3GPP access and non-3GPP access are independent of each other, that is, one can be in CM-IDLE state while the other is in CM-CONNECTED state [3].

A UE must register with the network to be authorized to use network services, to assist mobility tracking, and to be reachable. The registration procedure is used when the UE needs to perform initial registration with the 5GS; location update upon entering a new tracking area outside of the UE's registration area in CM-CONNECTED and CM-IDLE modes; when the UE performs a periodic registration update (due to a predefined inactivity time interval); and additionally when the UE needs to update its capabilities or protocol parameters that were negotiated during registration procedure. The AMF provides a list of recommended cells/TAs/NG-RAN node identifiers for paging.

The N2 interface supports management procedures which are not UE-specific, rather for configuration or reset of the N2 interface. These procedures are applicable to any access scheme and access-specific messages that carry some information for a particular access scheme such as information on the default paging DRX cycle that is used only for 3GPP access. The N2 interface further supports UE-specific and NAS-transport procedures. These procedures are in general access-agnostic, but they may also correspond to uplink NAS transport messages that carry some access-dependent information such as user location information. The N2 interface also supports procedures related to UE context management and resources for PDU sessions. These messages carry information on N3 addressing and QoS requirements that should be transparently forwarded by the AMF between the 5G access node and the SMF. The N2 interface further enables procedures related to handover management for 3GPP access.

The control-plane interface between a 5G access node and the 5G core supports connection of different types of 5G access nodes to the 5GC via a unique control-plane protocol. A single NGAP protocol is used for 3GPP and non-3GPP access schemes. There is a unique N2 termination point at the AMF for a given UE (for each access node used by the UE) regardless of the number of PDU sessions of the UE. The N2 control plane supports separation of AMF and other functions such as SMF that may need to control the services supported by 5G access nodes, where in this case, AMF transparently forwards NGAP messages between the 5G access node and the SMF. The N2 session management information (i.e., a subset of NGAP information that AMF transparently relays between an access node and SMF) is exchanged between the SMF and the 5G access node which is transparent to the AMF. The NG application protocol enables message exchange between a 5G access node and the

AMF over N2 interface using SCTP protocol, which guarantees delivery of signaling messages between AMF and 5G access node.

1.2.2.3.2 User-Plane Protocol Stacks

The protocol stack for the user-plane transport related to a PDU session is illustrated in Fig. 1.72. The PDU layer corresponds to the PDU that is transported between the UE and the PDN during a PDU session. The PDU session type can be IPv6 or Ethernet for transporting IP packets or Ethernet frames. The GPRS tunneling protocol for the user plane (GTP-U) supports multiplexing of the traffic from different PDU sessions by tunneling user data over N3 interface (i.e., between the 5G access node and the UPF) in the core network. GTP encapsulates all end-user PDUs and provides encapsulation per-PDU-session. This layer also transports the marking associated with a QoS flow [3].

The 5G encapsulation layer supports multiplexing the traffic from different PDU sessions over N9 interface (i.e., an interface between different UPFs). It provides encapsulation per PDU session and carries the marking associated with the QoS flows. The 5G access node protocol stack is a set of protocols/layers which are related to the access network as described in the previous sections. The number of UPF entities in the data path is not constrained by the 3GPP specifications; therefore, there could be none or more than one UPF entities in the data path of a PDU session that may not support PDU session anchor functionality for that PDU session. In certain cases, there is an uplink classifier or a branching point in the data path of a PDU session, which does not act as the non-PDU session anchor UPF. In that case, there are multiple N9 interfaces branching out of the uplink classifier/branching point, each leading to different PDU session anchors.

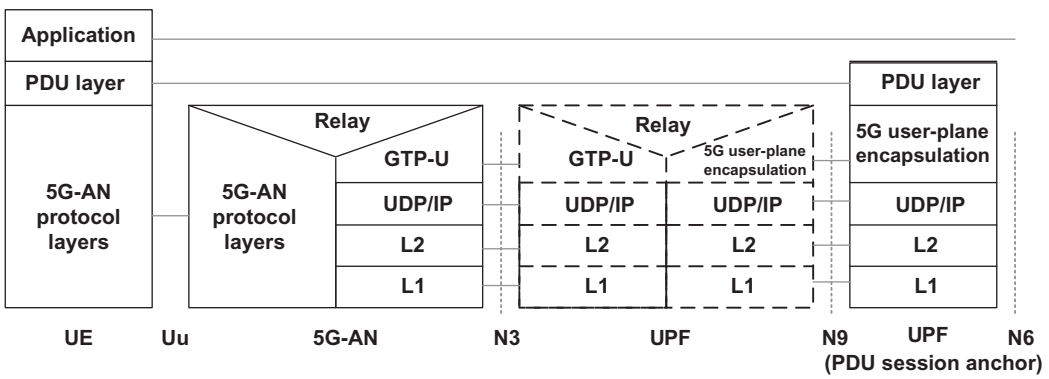


Figure 1.72
User-plane protocol stack between UE and UPF [3].

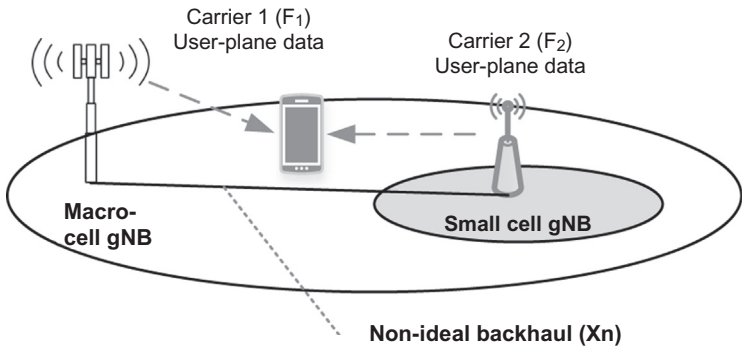


Figure 1.73
Illustration of inter-node radio resource aggregation (dual connectivity concept).

1.3 Dual Connectivity and Multi-connectivity Schemes

Dual connectivity (or multi-connectivity) is a term that is used to refer to an operation where a given UE is allocated radio resources provided by at least two different network nodes connected with non-ideal backhaul (see Fig. 1.73). Each access node involved in dual connectivity for a UE may assume different roles. Those roles do not necessarily depend on the access node's power class and can vary for different UEs. To support tight interworking between LTE and NR, where both LTE eNB and NR gNB can act as a master node. It is assumed that the dual connectivity between LTE and NR supports the deployment scenario where LTE eNB is not required to be synchronized with NR gNB.

3GPP NR supports dual connectivity operation in which a UE in the connected mode is configured to utilize radio resources provided by two distinct schedulers, located in two gNBs connected via a non-ideal backhaul as shown in Fig. 1.73. The gNBs involved in the dual connectivity for a certain UE may assume two different roles, that is, a gNB may either act as a master gNB (MgNB) or as a secondary gNB (SgNB). Under this condition, a UE is connected to one MgNB and one SgNB. Under dual connectivity framework, the radio protocol stack that a radio bearer uses depends on how the radio bearer is setup. There are four bearer types in dual connectivity framework, namely MCG[70] bearer, MCG split bearer, SCG[71] bearer, and SCG split bearer as depicted in Fig. 1.74.

Under dual connectivity framework, the UE is configured with two MAC entities, one for the MCG and one for the SCG. For a split bearer,[72] the UE is configured over one of the

[70] Master cell group in a multi-RAT dual connectivity scheme refers to a group of serving cells associated with the master node, comprising the primary cell and optionally one or more secondary cells.
[71] Secondary cell group in a multi-RAT dual connectivity scheme refers to a group of serving cells associated with the secondary node, comprising primary cell and optionally one or more secondary cells.
[72] Split bearer in multi-RAT dual connectivity is a bearer whose radio protocols are split either at the master node or at the secondary node and belongs to both secondary cell group and master cell group.

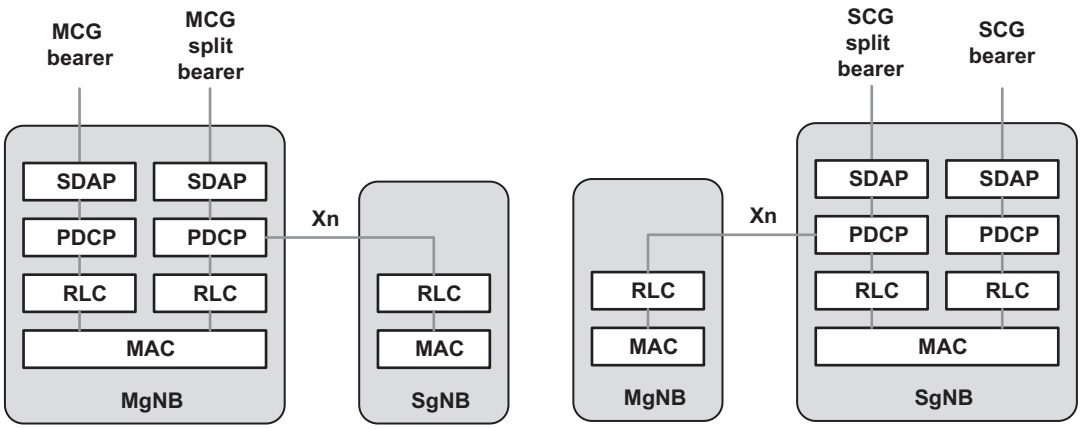


Figure 1.74
MgNB and SgNB bearers for dual connectivity [16].

links (or both) that it transmits uplink PDCP PDUs. The RLC sublayer only transmits corresponding feedback for the downlink data over the link which is not used for transmitting PDCP PDUs.

Multi-RAT DC (MR-DC) is a generalization of the intra-LTE dual connectivity, where a UE with multiple RF transceivers may be configured to utilize radio resources provided by two distinct schedulers located in two different nodes and connected via non-ideal backhaul, one providing LTE access and the other one providing NR connectivity. One scheduler is located in the master node (MN)[73] and the other in the secondary node (SN).[74] The MN and SN entities are connected via a network interface and the MN is typically connected to the core network. LTE supports MR-DC via E-UTRA-NR dual connectivity (EN-DC), in which a UE is connected to one eNB that acts as the MN and one gNB that acts as the SN. The eNB is connected to the EPC and the gNB is connected to the eNB via the X2 interface (i.e., the logical interface between LTE eNBs).

In MR-DC scenarios, the UE has a single RRC state, based on the MN RRC state and a single control-plane connection toward the core network. Fig. 1.75 shows the control-plane architecture for MR-DC. Each radio node has its own RRC entity, which can generate RRC PDUs to be sent to the UE. The RRC PDUs generated by the SN can be transported via the MN to the UE. The MN always sends the initial SN RRC configuration via MCG SRB, for example, SRB1, but subsequent reconfigurations may be sent via the MN or the SN entities. When transporting RRC PDU from the SN, the MN does not modify the UE configuration

[73] Master node in a multi-RAT dual connectivity architecture is either a master eNB or a master gNB.
[74] Secondary node in multi-RAT dual connectivity architecture is either a secondary eNB or a secondary gNB.

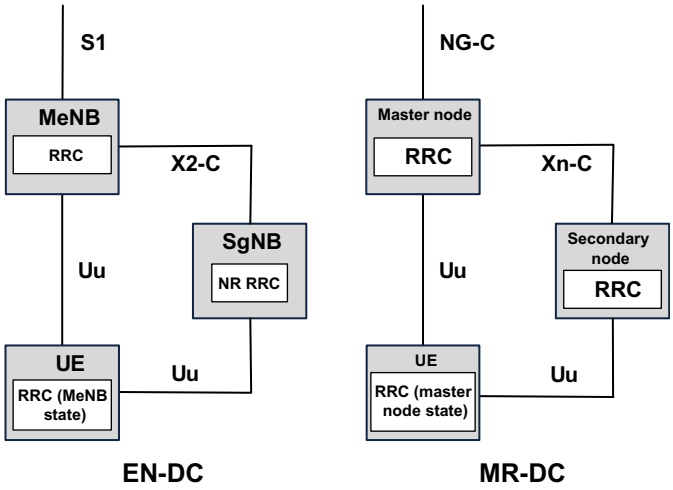


Figure 1.75
Control-plane architecture for EN-DC and MR-DC with 5GC [13].

provided by the SN. In EN-DC and NG-RAN E-UTRA-NR dual connectivity (NGEN-DC[75]) scenarios, during initial connection establishment SRB1 uses LTE PDCP; however, after initial connection establishment MCG SRB (SRB1 and SRB2) can be configured by the network to use either LTE PDCP or NR PDCP. The PDCP version change (release of old PDCP and establishment of new PDCP) of SRBs can be supported via a handover procedure (reconfiguration with mobility) or through a reconfiguration without mobility, when the network is aware that there is no uplink data in the UE buffer. For EN-DC capable UEs, NR PDCP can be configured for DRBs and SRBs before EN-DC is configured. If the SN is a gNB (i.e., for EN-DC and NGEN-DC), the UE can be configured to establish an SRB with the SN (e.g., SRB3[76]) to enable RRC PDUs for the SN to be sent directly between the UE and the SN. The RRC PDUs for the SN can only be sent directly to the UE for SN RRC reconfiguration without any coordination with the MN. Measurement reporting for mobility within the SN can be conducted directly from the UE to the SN, if SRB3 is configured. The MCG split SRB is supported for all MR-DC cases, allowing duplication of RRC PDUs generated by the MN, via the direct path and through the SN. The MCG split SRB uses NR PDCP. The SCG split SRB is not currently supported in 3GPP specifications [13].

[75] NG-RAN supports NGEN-DC, in which a UE is connected to one ng-eNB that acts as a master node and one gNB that acts as a secondary node. The ng-eNB is connected to the 5GC and the gNB is connected to the ng-eNB via the Xn interface.

[76] SRB3 in EN-DC and NGEN-DC represents a direct signaling radio bearer between the secondary node and the user equipment.

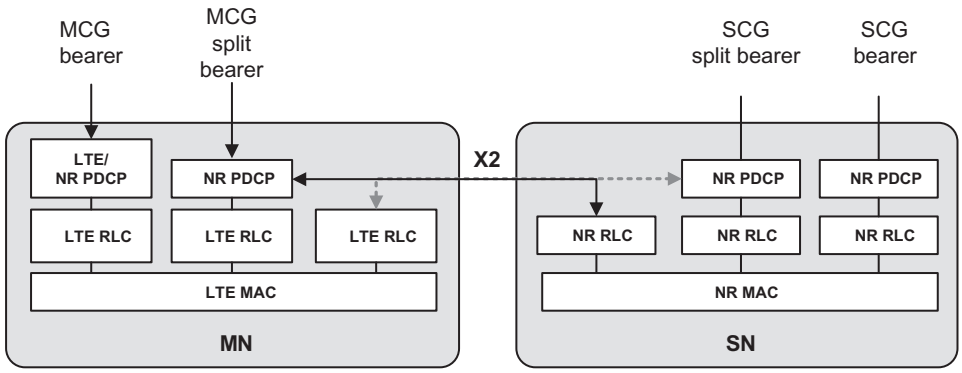


Figure 1.76
Radio protocol stack for MCG, MCG split, SCG, and SCG split bearers in MR-DC with EPC (EN-DC) [13].

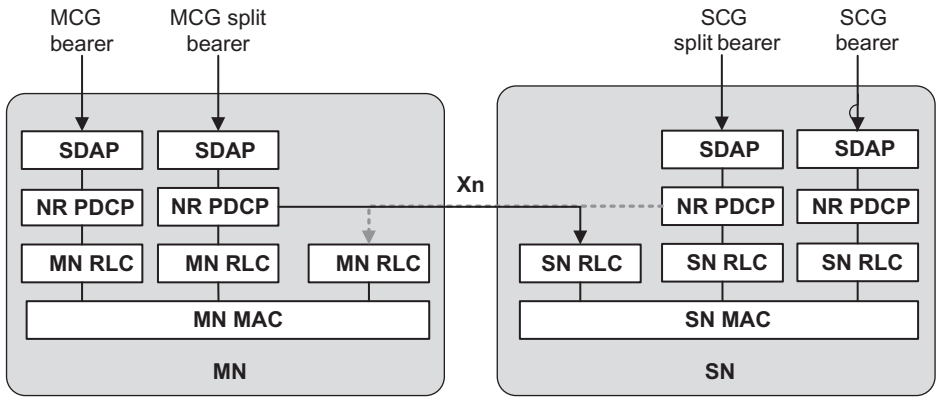


Figure 1.77
Radio protocol stack for MGC, MCG Split, SCG, and SCG split bearers in MR-DC with 5GC (NGEN-DC, NE-DC) [13].

As we mentioned earlier, there are four bearer types identified as MCG bearer, MCG split bearer, SCG bearer, and SCG split bearer in MR-DC scenarios. These four bearer types are depicted in Fig. 1.76 for MR-DC with EPC (EN-DC) and in Fig. 1.77 for MR-DC with 5GC (NGEN-DC, NE-DC). For EN-DC, the network can configure either LTE PDCP or NR PDCP for MCG bearers while NR PDCP is always used for SCG bearers. For split bearers, NR PDCP is always used and from the UE perspective there is no difference between MCG and SCG split bearers. In MR-DC with 5GC, NR PDCP is always used for all bearer types.

From system architecture point of view, in MR-DC, there is an interface between the MN and the SN entities to facilitate control-plane signaling and coordination. For each MR-DC

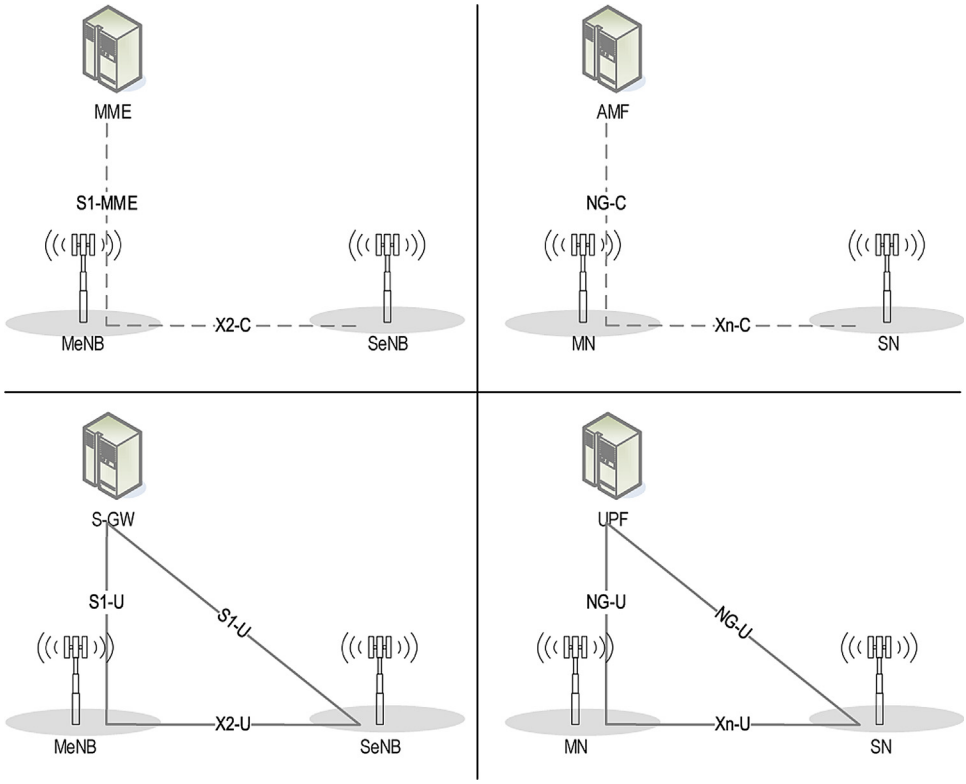


Figure 1.78
Control-plane and user-plane architecture for EN-DC and MR-DC with 5GC [13].

capable UE, there is also one control-plane connection between the MN and a corresponding core network entity. The MN and the SN entities involved in MR-DC operation for a UE control their own radio resources and are primarily responsible for allocating radio resources of their cells. Fig. 1.78 shows control-plane connectivity of an MN and SN involved in MR-DC with a UE. In MR-DC with EPC (EN-DC) scenario, the involved core network entity is the MME. S1-MME is terminated in MeNB and the MeNB and the SgNB are interconnected via X2-C. In MR-DC with 5GC (NGEN-DC, NE-DC) scenario, the terminating core network entity is the AMF. The NG-C interface is terminated at the MN and the MN and the SN are interconnected via Xn-C interface [13].

There are different user-plane connectivity options for the MN and SN involved in MR-DC operation with a certain UE, as shown in Fig. 1.78. The user-plane connectivity depends on the configured bearer type. For MCG bearers, the user-plane connection to the core network entity is terminated at the MN. The SN is not involved in the transport of user-plane data for this type of bearer over the Uu interface (i.e., the radio interface). For MCG split bearers, the user-plane connection to the core network entity is terminated in the MN.

PDCP data is transferred between the MN and the SN via MN-SN user-plane interface. The SN and MN participate in transmitting data of this bearer type over Uu interface. For SCG bearers, the SN is directly connected to the core network entity via a user-plane interface. The MN is not involved in the transport of user-plane data for this type of bearer over Uu interface. For SCG split bearers, the user-plane connection to the core network entity is terminated at the SN. The PDCP packets are transferred between the SN and the MN via MN/SN user-plane interface. The SN and MN transmit data of this bearer type over the Uu interface. For MR-DC with EPC (EN-DC), X2-U interface is the user-plane interface between MeNB and SgNB, and S1-U is the user-plane interface between MeNB and SGW. For MR-DC with 5GC (NGEN-DC, NE-DC), Xn-U interface is the user-plane interface between MN and SN, and NG-U is the user-plane interface between MN and UPF [13].

1.4 LTE-NR Interworking and Deployment Scenarios

1.4.1 RAN-Level and CN-Level Interworking

To provide full 5G services to the users, 5G cells will have to be deployed with full coverage and all UEs will have to be able to connect to 5G network everywhere. However, in the early phases of 5G deployments, the 5G cells will be partially deployed and there will be 5G coverage gaps. Large-scale 5G commercial services and deployments are expected in 2020 + and the initial investments for 5G service are expected to be limited due to lack of 5G user equipment. As a result, the 5G networks need to be able to interwork with the existing LTE networks. The interworking solution can provide seamless service to the users. In this section, we discuss the solutions for LTE−NR interworking and we will compare the solutions in terms of performance, features and ease of migration to a full 5G network. If 5G cells are not deployed with full coverage, a seamless service can be provided to the users by interworking with the existing LTE networks, which are already deployed with full coverage. For LTE−NR interworking, two types of solutions namely access-network-level interworking and core-network-level interworking, have been studied in 3GPP.

In RAN-level interworking solutions, the interworking service between LTE and 5G is made possible by using a direct interface between LTE eNB and NR gNB. The RRC messages are transmitted over the LTE radio interface, thus the connection and the mobility of UE are controlled by the LTE eNB. The user traffic is simultaneously transmitted through LTE eNB and NR gNB either by PDCP aggregation or using NR gNB split bearer. Although the RRC messages can be processed by the LTE eNBs that provide larger coverage than NR gNBs, LTE radio interface always remains connected, even though user traffic is transmitted over the NR. RAN-level interworking is necessary in non-stand-alone architecture, where the NR cannot be used without overlaid LTE network. Note that when the LTE EPC is used, only EPC-based services can be provided, even though 5G radio

technology is used. Two different core networks can be used for RAN-level interworking, as shown in Fig. 1.79. LTE and NR interworking can be achieved by upgrading some LTE eNBs connected to NR gNBs and by increasing the gateway capacity in EPC. The new 5G core network, 5GC, has been designed to support RAN-level interworking. In this solution, the new 5GC network slicing feature can be used to separate 5G services from the LTE services. In this case, all LTE eNBs will have to be upgraded to ng-eNBs so that they can be connected to 5GC [16].

In core-network-level interworking, a direct interface between the LTE eNB and the NR gNB is not required and the EPC SGW is connected to the 5GC UPF. The UE manages LTE and NR interface connection independently, and can be connected to a single network, either LTE or 5G. When the UE is located in 5G coverage, it can only connect to the 5G network and receive 5G service. When the UE moves out of 5G coverage, it releases NR interface connection and establishes LTE radio interface connection. Although the network to which the UE connects changes, the IP address assigned to the UE stays the same and seamless service can be provided to the user. The core-network-level interworking is necessary in stand-alone architecture models, where NR can be used without relying on LTE network. In this case, single registration or dual registration is possible, as shown in Fig. 1.79. With the single registration, the UE registers with either LTE EPC or 5G networks at any time, and the UE context can be transferred via the control interface between the EPC MME and 5GC AMF when the UE's network association changes. In order to support the single registration, the MME will have to be upgraded in order to support the MME-AMF interface and the SGW needs to be connected to UPF in 5GC. LTE eNB must also be upgraded to support the mobility between the LTE and the 5G networks. N26 interface is an inter-CN interface between the MME and AMF in order to enable interworking between EPC and the 5G core. Support of N26 interface in the network is optional for interworking. N26 supports a subset of the functionalities that are essential for interworking. Networks that support interworking with EPC may support interworking procedures that use the N26 interface or interworking procedures that do not use the N26 interface. Interworking procedures with N26 support provide IP address continuity during inter-system mobility to UEs that support 5GC NAS and EPC NAS. Networks that support interworking procedures without N26 must support procedures to provide IP address continuity during inter-system mobility to the UEs that operate in both single-registration and dual-registration modes [3]. Interworking procedures using N26 interface enable the exchange of MM and SM states between the source and target networks. Handover procedures are supported through N26 interface. When interworking procedures with N26 is used, the UE operates in single-registration mode. The network retains only one valid MM state for the UE, either in the AMF or MME. Either the AMF or the MME is registered in the HSS + UDM. The support for N26 interface between AMF in 5GC and MME in EPC is required to enable seamless session continuity (e.g., for voice services) for inter-system handover. When the UE moves

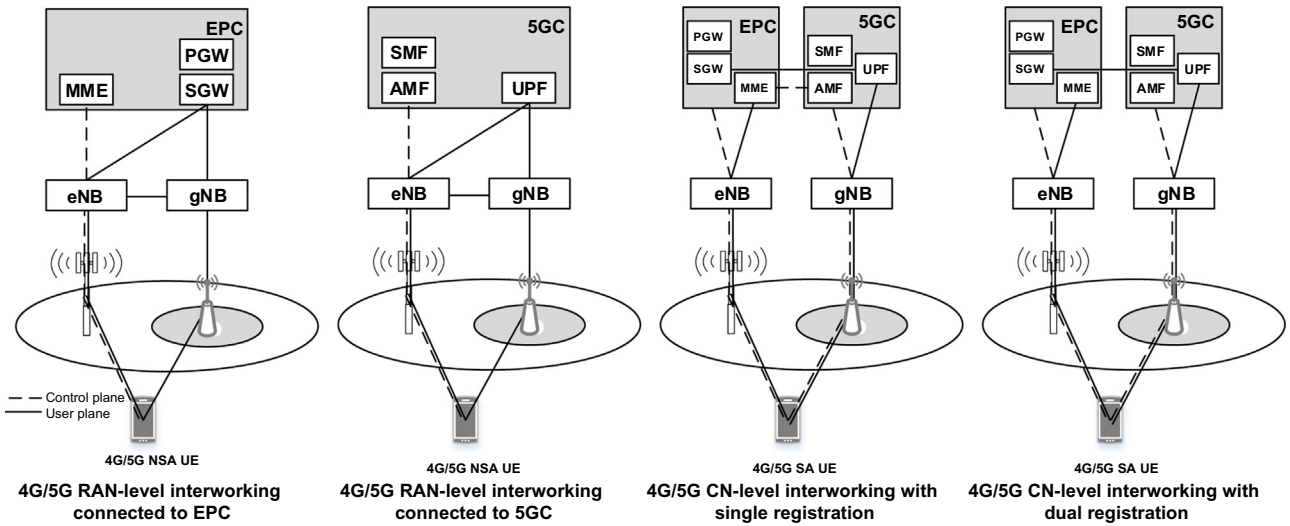


Figure 1.79
RAN-level and core-network-level interworking models [82].

from 5GC to EPC, the SMF determines which PDU sessions can be relocated to the target EPS. The SMF can release the PDU sessions that cannot be transferred as part of the handover. However, the target EPS determines if the PDU session can be successfully moved to the target network.

The dual registration approach requires the UE to register separately with the EPC and the 5GC. Thus it does not need to forward the UE context between MME and AMF, and the interface between MME and AMF is not required. The handover between LTE and 5G systems is decided by the UE. The UE performs normal access procedures after moving to the other network. Therefore, the solution can be supported by LTE eNBs with minimal changes. Furthermore, the impact on EPC to support the dual registration is minimized. However, in order to improve the mobility performance between LTE and 5G, it is necessary to temporarily support dual radio transmission when moving to the other network, although the UE can support dual registration solution even with single radio transmission capability. Deployments based on different 3GPP architecture options (i.e., EPC based or 5GC based) and UEs with different capabilities (EPC NAS and 5GC NAS) may coexist at the same time within one PLMN.

In order to interwork with EPC, the UE that supports both 5GC and EPC NAS can operate in single- or dual-registration mode. In single-registration mode, the UE has only one active MM state (either RM state in 5GC or EMM state in EPC) and it is either in 5GC NAS mode or in EPC NAS mode (when connected to 5GC or EPC, respectively). The UE maintains a single coordinated registration for 5GC and EPC. Accordingly, the UE maps the EPS-GUTI to 5G-GUTI during mobility between EPC and 5GC and vice versa. In dual-registration mode, the UE can handle independent registrations for 5GC and EPC. In this mode, UE maintains 5G-GUTI and EPS-GUTI independently. In this mode, the UE provides native 5G-GUTI, if previously allocated by 5GC, for registration with 5GC and it provides native EPS-GUTI, if previously allocated by EPC, for Attach/TAU with EPC. In this mode, the UE may be registered to 5GC only, EPC only, or to both 5GC and EPC. The support of single registration mode is mandatory for UEs that support both 5GC and EPC NAS. During LTE initial attach procedure, the UE supporting both 5GC and EPC NAS indicates its support of 5G NAS in UE network capability [3].

The Ethernet and unstructured PDU session types are transferred to EPC as non-IP PDN type (when supported by UE and network). The UE sets the PDN type to non-IP when it moves from 5GS to EPS. After the transfer to EPS, the UE and the SMF maintain information about the PDU session type used in 5GS, that is, the information indicating that the PDN connection with non-IP PDN type corresponds to PDU session type of Ethernet or unstructured, respectively. This is to ensure that the appropriate PDU session type will be used if the UE transfers back to the 5GS.

1.4.2 5G Deployments Scenarios and Architecture Options

This section describes 5G network architecture deployment options supporting stand-alone and non-stand-alone mode of operation. These deployment options were extensively discussed in 3GPP and have been prioritized based on their viability and practicality. Each option provides NR access to sufficiently capable UEs either through direct access to gNB/5GC or indirectly via LTE interworking. 3GPP defined both stand-alone and non-stand-alone deployment configurations for NR in 3GPP Rel-15. A stand-alone NR deployment would not require an associated LTE network. The NR-capable UE could use random access to directly establish a radio link with a gNB and attach to the 5GC in order to use network services. The stand-alone NR deployment required a complete set of specifications from 3GPP for all entities and interfaces in the network, which was subsequently defined in 3GPP Rel-15 specifications.

In stand-alone operation (shown as option 2 in Fig. 1.80), the network access procedures closely follow the LTE counterparts. The additional requirements mainly include broadcast of NR system information, which includes a minimum set of parameters and extended set of parameters where the former is periodically broadcast and comprises basic information required for initial access and the scheduling information for other system information; and the latter encompasses other system information that are not transmitted via the broadcast channel, which may either be broadcast or provisioned in a dedicated manner which can be triggered by the network configuration or upon request from the UE. In comparison to LTE system information broadcasting scheme, on-demand broadcasting is a new mechanism introduced in NR to deliver other system information by UE request. For UEs in RRC_CONNECTED state, dedicated RRC signaling is used for the request and delivery of the other system information. For UEs in RRC_IDLE and RRC_INACTIVE states, making the request will trigger a random access procedure [16].

As an interim step for NR deployments, 3GPP has defined a set of non-stand-alone deployment configurations using dual connectivity between NR gNB and LTE eNB (or ng-eNBs). Since initial NR networks will not have full coverage, dual connectivity can be used to combine the coverage advantage of the existing LTE networks with the throughput and latency advantages of the NR. However, it requires more complex UE implementations to allow simultaneous connections with both LTE and NR networks, potentially increasing the cost of the UEs. This will require more complex UE radio capabilities including the ability to simultaneously receive downlink transmissions from NR and LTE base stations on separate frequency bands. The non-stand-alone NR deployments use architectures where NR gNBs are associated with LTE eNBs and do not require separate signaling connections to the 5GC. These architectures are classified based on the control-plane and user-plane connections used between eNB, gNB, EPC, and 5GC.

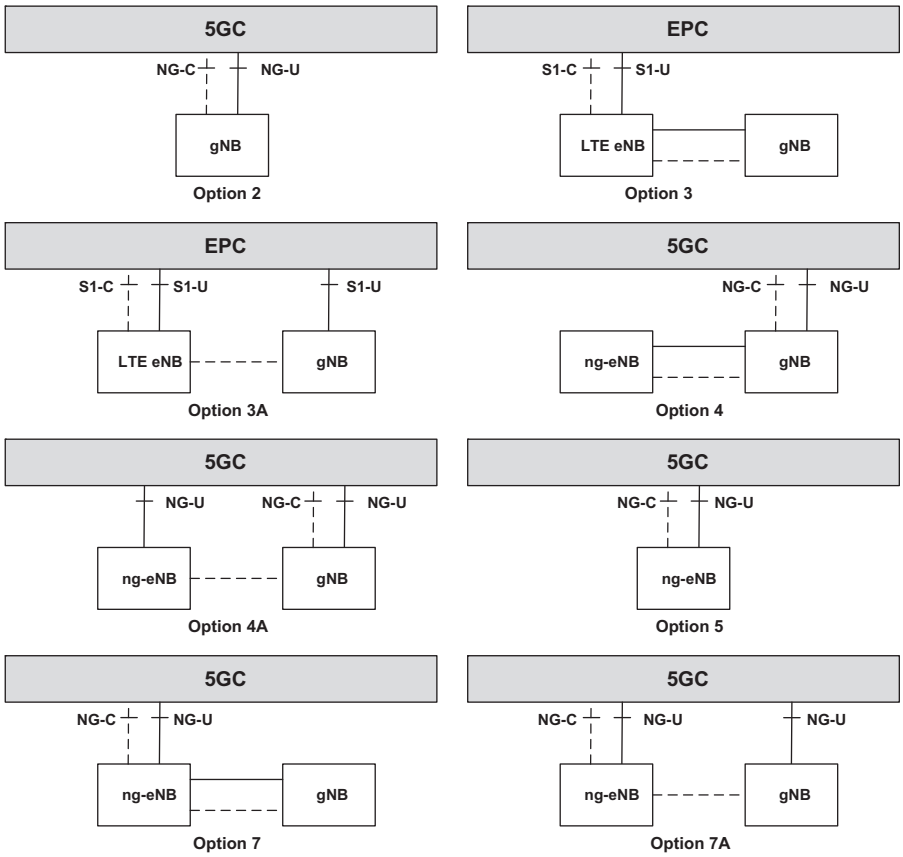


Figure 1.80
NR deployment options [34].

The deployments based on architecture option 3 use EPC as the core network as shown in Fig. 1.80. In this case, S1-C control-plane interface for the UE is established between the LTE eNB and the EPC. The gNB acts as a secondary node connected to the master node represented by the eNB. Control-plane information is exchanged between the LTE eNB and the NR gNB, and no direct control-plane interface exists between the gNB and the EPC. User-plane bearers are supported between eNB and EPC over S1-U. In option 3A, the gNB also terminates user-plane bearers with the EPC. In option 3A, those gNB terminated S1-U bearers may further split and carried over the X2/Xn interface to the eNB and over the LTE air interface. The deployments based on architecture option 3 do not require interface with the 5GC, and allow service over the NR air interface with Uu (i.e., the interface between the UE and the serving gNB) and X2/Xn interfaces defined. As such, this is seen as the most likely architectural scenario for early NR deployments. From control-plane perspective, there is only one RRC state in the UE, which is based on the LTE RRC protocols and there is only one control-plane connection toward the core network.

The deployments based on architecture option 4 are essentially the opposite of option 3, with the gNB and the eNB representing the MCG and the SCG, respectively. The control-plane connection is established between the gNB and the 5GC over the NG-C, and the eNB exchanges control-plane information with gNB over Xn. In option 4A, direct user-plane bearers with the 5GC are terminated at the eNB. In architecture option 5, the ng-eNB (i.e., an LTE eNB compliant with LTE Rel-15 onward) is connected to the 5GC.

The deployments based on architecture option 7 use the same topology as option 3, with the eNB acting as MCG and the gNB acting as SCG. The difference between the two options is that the 5GC serves as the core network instead of the EPC, requiring the eNB upgrade to ng-eNB interfaces with the 5GC. In this scenario, each radio node has its own RRC entity which can generate RRC PDUs to be sent to the UE. Note that RRC PDUs generated by the gNB (SN) can be transported via the LTE Uu interface or NR Uu interface to the UE, if configured. The eNB (MN) always sends the initial SN RRC configuration via MCG SRB (SRB1); however, subsequent reconfigurations may be transported via the MN or SN. Furthermore, the UE can be configured to establish an SRB with the SN (i.e., SRB3) to enable RRC PDUs for the SN to be sent directly between the UE and the SN.

1.5 Network Aspects of Mobility and Power Management

Mobility and power management continue to be the most important aspects of any new cellular standard to ensure seamless connectivity and sustainable power consumption of user terminals as well as overall energy efficiency of the network. In 4G/5G, the states of a UE with respect to mobility and connection establishment are described by NAS and RRC states. Fig. 1.81 shows and compares the EPS and 5GS/NG-RAN NAS and RRC states. There are three states shown in the EPS model, that is, EPS mobility management (EMM),

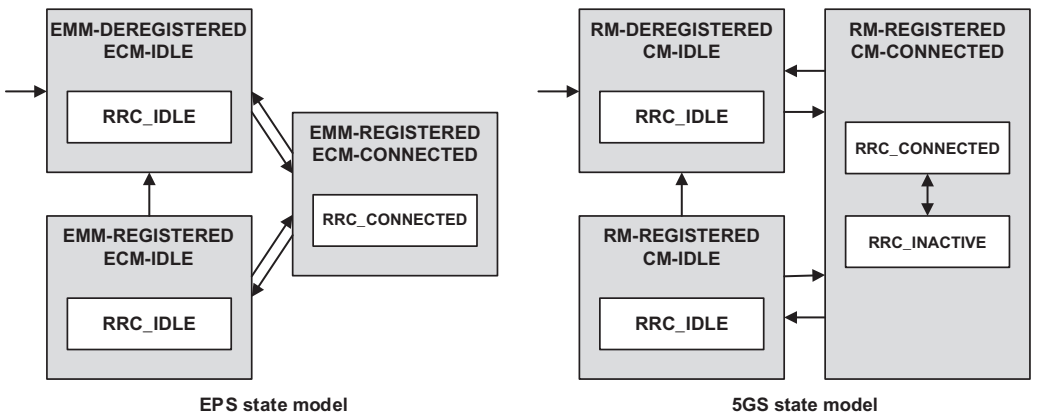


Figure 1.81
Comparison of mobility management states of EPS and 5GS [3].

EPS connection management (ECM), and RRC. The EMM and ECM states are managed by the core network, where the EMM state represents whether a UE is registered in the EPC and the ECM state indicates if NAS signaling connection between the UE and the MME is established. On the other hand, the RRC state is managed by E-UTRAN, and it represents whether there is a connection between the UE and the serving eNB. A UE in the ECM-CONNECTED state needs to be in the RRC_CONNECTED state, because a radio link connection is required in order to establish NAS signaling [3,16].

1.5.1 Mobility Management

In 5GS, the mobility management state of a UE can be either RM-REGISTERED or RM-DEREGISTERED depending on whether the UE is registered in 5GC, which is very similar to EMM-REGISTERED and EMM-DEREGISTERED states in EPC. Two connection management states are used to reflect the NAS signaling connectivity of the UE with the AMF namely CM-IDLE and CM-CONNECTED. A UE in CM-IDLE state has no NAS signaling connection established with the AMF over N1. A UE in CM-CONNECTED state has a NAS signaling connection with the AMF over N1. A NAS signaling connection uses an RRC connection between the UE and the NG-RAN and an NGAP UE association between the access network and the AMF for 3GPP access. NR RRC protocol states consist of three states, where in addition to RRC_IDLE and RRC_CONNECTED states, a third state has been introduced, RRC_INACTIVE, as an intermediate state prior to transition to RRC_IDLE state in order to save UE power and to allow fast connection setup [3,16].

As shown in Fig. 1.81, in EPS, when a UE is in the RRC_CONNECTED state, the serving eNB evaluates the received signal strength measurements from the UE and initiates a handover procedure when the UE's received signal strength goes below a threshold. However, in the RRC_IDLE state, where the eNB is not aware of the UE's location, the UE decides whether to camp on the current cell or to reselect a neighboring target cell based on received signal strength measurements. This procedure is referred to as cell reselection. In EPS, the mobility procedures, that is, as handover in the RRC_CONNECTED state and cell reselection in the RRC_IDLE state, are not flexible, whereas in 5GS, the core network is able to flexibly control whether to perform a handover or cell reselection for a UE in CM-CONNECTED state [3,16].

In EPC, the location of a UE is tracked by the MME. The granularity of location tracking is different depending on the RRC state of the UE. In the RRC_CONNECTED state, the UE's location is tracked at the cell level, whereas in the RRC_IDLE state, its location is tracked at the tracking area level, which is a set of cells belonging to a paging group that simultaneously transmit paging messages. Similarly, 5GC can track the location of a UE at the tracking area level in the CM-IDLE state, whereas the UE's location is known at the level of the serving cell to the core network in the CM-CONNECTED state. In 5GC, when a UE

registers with the network over the 3GPP access, the AMF allocates a set of tracking areas in TAI list to the UE. The AMF takes into account various information (e.g., mobility pattern and allowed/non-allowed area, etc.), when it allocates registration area to the UE, that is, the set of tracking areas in TAI list. In 5GS; however, NG-RAN also supports the location tracking for the UEs in RRC_INACTIVE state. In that state, the core network knows that the UE is somewhere within the NG-RAN, but the NG-RAN node needs a new location tracking functionality to determine the exact location of the UE because the connection between the UE and the NG-RAN node is not active.

In EPS, when downlink traffic for a UE in the RRC_IDLE state arrives at the SGW, the MME performs a paging procedure based on the detected location of the UE. However, 5GS supports two types of paging, namely core-network-initiated paging and access-network-initiated paging. The UE in RRC_IDLE and RRC_INACTIVE states may use DRX in order to reduce power consumption. While in RRC_IDLE, the UE monitors 5GC-initiated paging, in RRC_INACTIVE, the UE is reachable via RAN-initiated paging and 5GC-initiated paging. The RAN and 5GC paging occasions overlap and the same paging mechanism is used. In core-network-initiated paging, the default paging procedure is requested by the core network when the UE is in the CM-IDLE state. The newly introduced RAN-initiated paging mode is used for the UEs in the RRC_INACTIVE state. Since a UE in the RRC_INACTIVE state is in the CM-CONNECTED state (see Fig. 1.81), the core network simply forwards the data or the signaling messages to the corresponding RAN when data or signaling messages arrive for the UE. Therefore, RAN itself generates the paging message and performs paging to find the updated location of the UE, and then sends the data or signaling messages to the UE. The 5GC can transmit additional assistance information for RAN paging [16].

Service area restriction also known as mobility-on-demand, which defines areas where the UE may or may not initiate communication with the network, is a concept to selectively support mobility of devices on a need basis. It includes supporting UE's mobility at a certain level classified as mobility restriction and mobility pattern (or mobility level). The former addresses mobility restriction in terms of allowed, non-allowed, and forbidden areas. The minimum granularity of the area is at tracking area level. In the allowed area, UE can communicate through the control or user planes. The UE cannot send service request and session management signaling in the non-allowed area. However, periodic registration update is possible. It can also respond to the paging messages from the core network. Furthermore, emergency calls or multimedia priority services are allowed. In the forbidden area, UE is not allowed to have any communication with the network except for the emergency services. The mobility pattern is used as a concept to describe the expected mobility of UE in 5GC. Mobility pattern may be used by the AMF to characterize and optimize the UE mobility. The AMF determines and updates mobility pattern of the UE based on subscription of the UE, statistics of the UE mobility, network local policy, and the UE-assisted

information, or any combination of these parameters. The statistics of the UE mobility can be history-based or expected UE moving trajectory. The UE mobility pattern can be used by the AMF to optimize mobility support provided to the UE [16]. This procedure is used for the case where the UE moves from one gNB-DU to another gNB-DU within the same gNB-CU during NR operation.

The Internet of things is an important 5G service category. IoT devices mostly send mobile-originated data. For this type of devices, the mobile-originated only mode is defined in 5GS where the core network determines whether to apply the mobile-originated only mode to a UE during the registration procedure based on the UE subscription data and the network policy. The mobile-originated only mode is allocated to a UE, which does not require mobile-terminated traffic. Therefore, the UE in mobile-originated-only mode does not listen to the paging messages. The core network does not need to manage the UE's location while it is registered in the 5GC. For optimization, the core network may decide to deregister the UE after the mobile-originated data communication is finished, without transferring the UE's state into the CM-IDLE state in the RM-REGISTERED state, because most functions supported in the CM-IDLE state are not relevant to the UE in mobile-originated only mode, for example, UE location tracking and reachability management. In such cases, the UE needs to perform attach procedure whenever the mobile-originated data transmission is necessary to communicate with the core network.

A UE receives services through a PDU session, which is a logical connection between the UE and the data network. In 5GS, various PDU session types are supported, for example, IPv4, IPv6, Ethernet, etc. Unlike EPS, where at least one default session (i.e., default EPS bearer) is always created while the UE attaches to the network, 5GS can establish a session when service is needed irrespective of the attachment procedure of UE, that is, attachment without any PDU session is possible. 5GS also supports UE establishing multiple PDU sessions to the same data network or to different data networks over a single or multiple access networks including 3GPP and non-3GPP access. The number of UPFs for a PDU session is not specified. The deployment with at least one UPF is essential to serve a given PDU session. For a UE with multiple PDU sessions, there is no need for a convergence point like SGW in the EPC. In other words, the user-plane paths of different PDU sessions are completely disjoint. This implies that there is a distinct buffering node per PDU session for the UE in the RRC_IDLE state. In order to ensure slice-aware mobility management when network slicing is supported, a slice ID is introduced as part of the PDU session information that is transferred during mobility signaling. This enables slice-aware admission and congestion control [34].

LTE–NR interworking is important for stand-alone mode of operation between LTE and NR unlike for dual connectivity where there is simultaneous transmission across both RATs most of the time. Interworking between LTE and NR is not expected to be significantly

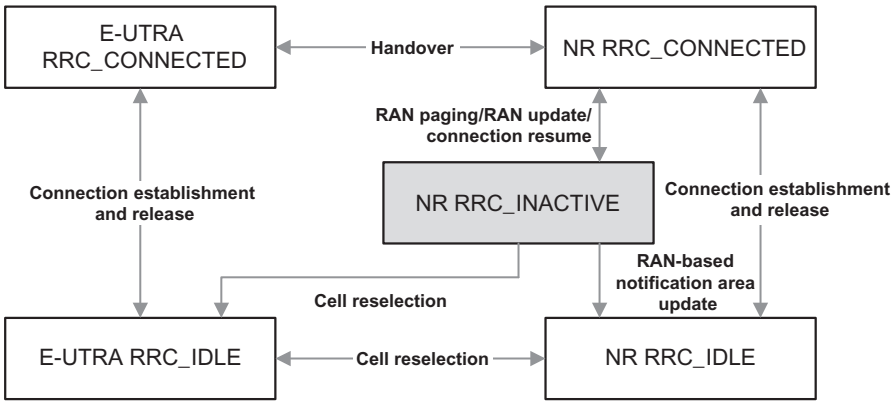


Figure 1.82
LTE–NR mobility state diagram [16,35].

different from what is defined in LTE specifications for interworking with other 3G networks. The inter-RAT mobility is expected to be supported both in idle mode as well as in the connected mode. Fig. 1.82 illustrates possible mobility scenarios across LTE and NR.

RRC_INACTIVE is a new RRC state in NR, in addition to RRC_IDLE and RRC_CONNECTED. It is a state where a UE remains in CM-CONNECTED and is able to move within an area configured by NG-RAN (i.e., RAN-based notification area or RNA) without notifying NG-RAN. The RNA can cover a single cell or multiple cells. In RRC_INACTIVE, the last serving NG-RAN node retains the UE context and the UE-associated NG connection with the serving AMF and UPF. The UE notifies the network via RAN-based notification area update procedure, if it has moved out of the configured RNA. If the last serving gNB receives downlink data from the UPF or downlink signaling from the AMF while the UE is in RRC_INACTIVE state, it pages the UE in the cells corresponding to the RNA and may forward the paging message to the neighbor gNB(s), if the RNA includes cells of neighbor gNB(s) [16]. Connected mode mobility is enabled using Xn interface between LTE eNB and NR gNB where both eNB and gNB are connected to 5G core network. S1/N2-based handover is supported when LTE eNB is connected to EPC and NR gNB is connected to 5GC. Xn and core network handover in 5GC, when both eNB and gNB are connected to 5GC, is transparent to the UE. Seamless handover is possible based on tight interworking between radio access technologies when anchored at 5GC.

1.5.2 Network-Controlled Power Management

Power management schemes are important to sustaining UE services and prolonged UE battery life. In this section, we discuss the power management schemes and strategies used by 5G networks to optimize UE power consumption while satisfying user expectations and

QoS requirements of the applications. During the normal operation, a 5G UE can be in one of the three states of connected, inactive, or idle as explained in the previous section. If there is no data to be transmitted/received, the UE stays in the energy-efficient idle state. In contrast, the connected state is the energy-consuming state, as the UE needs to continuously monitor the link quality of the serving and neighboring cells and to provide periodic reports on the quality and status of the radio link.

Mobile devices in connected mode may be configured with discontinuous reception (DRX) for power saving purposes. The parameters of DRX configuration can be optimized to either maximize power saving or minimize latency performance based on the UE's active applications/services. The DRX cycles are broadly configurable to support a wide range of services with different requirements in terms of power consumption and accessibility delays. The implementation of DRX allows the UE to avoid frequently monitoring the physical downlink control channel, except during specific time intervals configured by higher layers. A typical DRX cycle can be divided into an active time interval and an inactive period. During active time interval, the UE is awake and performs continuous reception, while the inactivity timer has not expired. During this time, the UE is performing continuous reception while waiting for a downlink transmission. The UE then enters the inactive period, if there is no traffic activity longer than the inactivity timer duration, after expiration of on-duration, or if the UE receives a MAC control message and is instructed to enter the DRX mode. When the DRX is configured and the UE is in an active state while in the on-duration interval (see Fig. 1.83), the UE monitors the relevant control channels to detect any downlink allocations and to receive pending transmissions from the serving base station. If no allocations including paging messages are detected within the on-duration, the UE will enter the inactive interval and will follow the DRX configuration to wake up in the next DRX cycle. During inactivity period, the UE first follows the short DRX cycle, if configured, and starts the DRX short cycle timer. After the short cycle timer expires, the UE follows the long DRX cycle. If no short DRX cycle is configured, the UE directly enters the long DRX cycle.

It is necessary to optimize the DRX parameters according to the QoS requirements of various services such as VoIP, web browsing and video streaming, where each has a different traffic model and specific QoS requirements, which may significantly impact the configuration of DRX parameters. The services with low delay requirement can be dealt with by activating the UE more frequently to monitor downlink allocations with short DRX cycle setting. While delay-tolerant services can achieve high energy-saving gains by waking up the UE to monitor downlink allocations with long DRX cycle configuration. Therefore, the best trade-off between power saving and responsiveness of the UEs should be made to optimally configure DRX parameters. 3GPP releases define the DRX configuration per UE. When multiple data bearers are established, DRX is enabled only when all the data bearers met their corresponding DRX inactivity timer condition, and the shortest DRX cycles

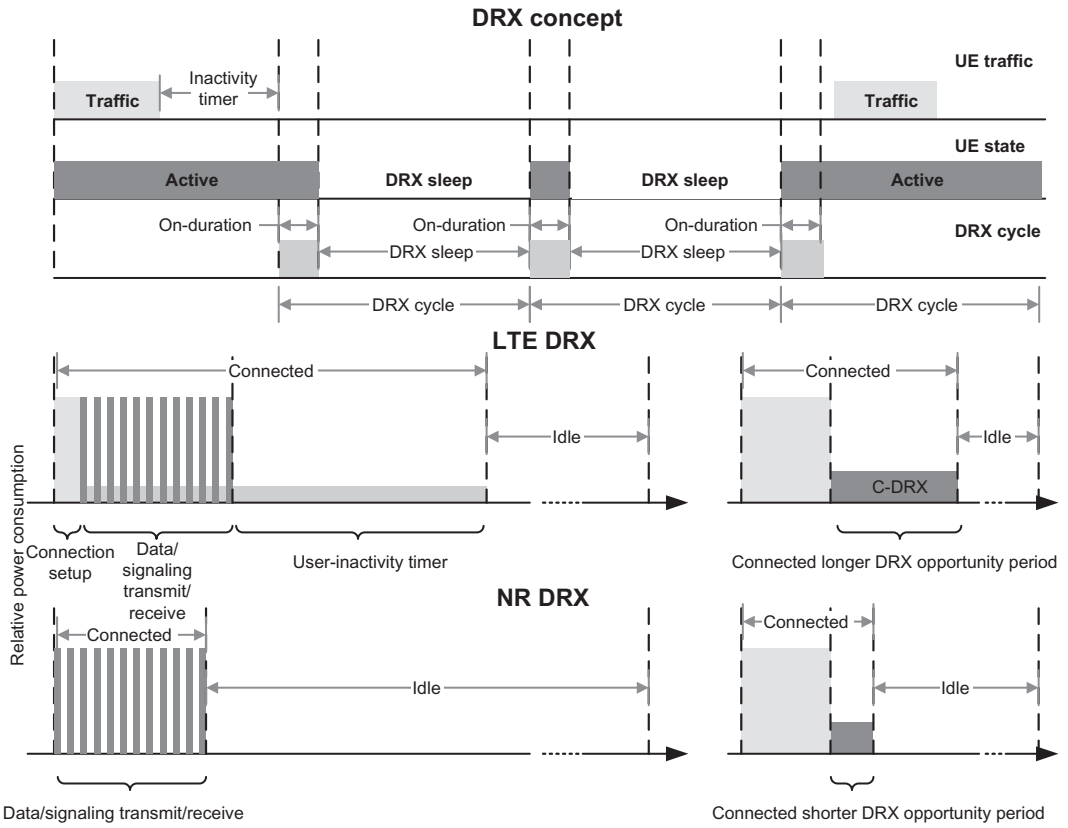


Figure 1.83
DRX concept and comparison of LTE and NR DRX schemes (example) [16,82].

among all the data bearers are followed. This solution is simple and effective for non-CA scenarios. In CA scenarios, the UE may operate over several component carriers and supports separate RF transceivers for each RF carrier. The baseline UE-specific DRX mechanism is no longer suitable to achieve higher energy-saving gains since the same DRX setting has to be configured for all component carriers according to the delay requirement of all applications running on the UE. The UE has to wake up the RF circuitries for all RF carriers at the same time to monitor possible downlink allocations. When bandwidth adaptation is configured in NR, the UE only has to monitor the downlink control channel on the [single] active bandwidth part, thus it does not have to monitor downlink control channels on the entire downlink frequency bands used in the cell. A bandwidth part inactivity timer (independent of DRX inactivity-timer described earlier) is used to switch the active bandwidth part to the default one, that is, the timer is restarted upon successful downlink control channel decoding and switching to the default bandwidth part occurs upon its expiration (see Fig. 1.83).

The percentage of time spent in the connected and idle states depends on a number of parameters controlled by the network including paging occasions, DRX cycles, user-inactivity timer, etc. The user-inactivity timer determines how long the UE stays in the connected state after it receives or transmits the last data packet. When the timer expires, the gNB releases the RRC connection and the UE immediately transitions to the idle state. The shorter the user-inactivity timer, the longer the UE battery life. However, if a new packet arrives the gNB queue shortly after the UE transitions to the idle state, the core network has to page the UE with network and radio signaling, causing extra service latency to transition to the connected state. In other words, the length of the user-inactivity timer determines a trade-off between UE energy consumption and connection latency as well as network control signaling overhead. Whenever the latency requirement can be relaxed, the DRX can provide further power savings. This will reduce the active duty cycle for downlink control channel monitoring, and if cross-slot scheduling is configured, then data channel reception is only needed when UE data is present. With this configuration the UE modem/transceivers may spend approximately 90% of time in a low-power sleep mode, but the penalty would be the substantially increased latency. The UE in RRC_IDLE and RRC_INACTIVE states may use DRX in order to reduce power consumption. While in RRC_IDLE, the UE monitors 5GC-initiated paging, in RRC_INACTIVE the UE is reachable via RAN-initiated paging and 5GC-initiated paging. The RAN and 5GC paging occasions overlap and same paging mechanism is used. The UE monitors one paging occasion per DRX cycle to receive the paging message. Paging DRX cycle length is configurable and a default DRX cycle for core-network-initiated paging is sent via system information. A UE-specific DRX cycle for core-network-initiated paging can be configured via UE dedicated signaling. The NG-RAN can configure a UE with a DRX cycle for RAN-initiated paging, which can be UE specific. The number of paging occasions in a DRX cycle is configured and signaled via system information. A network may assign UEs to the paging occasions based on UE identities when multiple paging occasions are configured in the DRX cycle. When DRX is configured, the UE does not have to continuously monitor downlink control channels. If the UE detects a relevant downlink control channel, it stays awake and starts the inactivity timer.

The DRX mechanism is characterized by several parameters such as *on-duration*, which is the time interval that the UE waits for, after waking up, to receive possible downlink control channels; *inactivity-timer*, which measures the duration of time from the last successful detection that the UE waits to successfully decode a downlink control channel. If the UE fails to detect a relevant downlink allocation, it goes back to sleep mode; *retransmission-timer* measures the duration of time when a HARQ retransmission is expected; and *cycle*, which specifies the periodic repetition of the on-duration followed by a possible period of inactivity [16].

1.6 Quality-of-Service Framework

We begin this section with a review of QoS framework in LTE to set the stage for the 5G QoS framework. As shown in Fig. 1.84, in EPC, the user traffic is classified into different SDFs each associated with different QoS classes based on the type of the service that is being provided through the SDFs. Different QoS rules are then applied to each SDF. Since SDFs are delivered through EPS bearers in an LTE network, the EPS bearer QoS has to be controlled in a way that SDF QoS is maintained. In an LTE network, the user traffic (IP flows or IP packets) is classified into SDF traffic and EPS bearer traffic. An SDF refers to a group of IP flows associated with a service that a user is utilizing, whereas an EPS bearer refers to IP flows of aggregated SDFs that have the same QoS class. The SDF and EPS bearers are detected by matching the IP flows against the packet filters, that is, SDF templates for SDFs or traffic flow templates (TFTs) for EPS bearers. These packet filters are preconfigured by network operators in accordance with their policy and each of them typically consists of 5-tuple (source IP address, destination IP address, source port number, destination port number, and protocol ID). In other words, in LTE network, IP flows with the same service characteristics that match the packet filters of an SDF template are designated to an SDF. SDFs that match the packet filters of a TFT are mapped to an EPS bearer, in order to be delivered to the UE. SDFs with the same QoS class are delivered, as aggregated, through an EPS bearer, whereas the ones with different QoS class are delivered through different EPS bearers. In LTE, there are two types of EPS bearers, default and dedicated. When a UE attaches to the LTE network, an IP address is assigned for PDN connection and a default EPS bearer is established at the same time [58,59].

In an LTE network, the QoS parameters are defined at service and bearer levels. SDF QoS parameters are service-level QoS parameters, whereas EPS bearer QoS parameters are bearer-level QoS parameters. Service level and bearer level are also called as SDF level and SDF aggregate level, respectively. An SDF aggregate refers to a group of SDFs which have

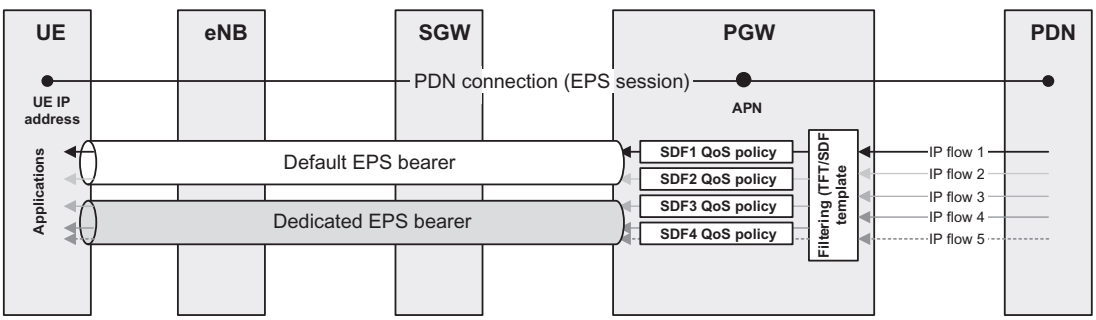


Figure 1.84
QoS architecture and process in LTE [59].

the same QCI and ARP values and belong to one EPS session. Both QCI and ARP are the basic QoS parameters applied to all SDFs and EPS bearers. The QoS class identifier (QCI) is particularly important because it serves as a reference that indicates the performance characteristics of SDFs and EPS bearers. In addition to these two basic parameters, there are other QoS parameters, such as GBR, maximum bit rate (MBR), and aggregated maximum bit rate (AMBR) that specify the bandwidth (or bit rate) characteristics of SDFs and EPS bearers. The SDF and EPS bearer QoS parameters are as follows: SDF QoS parameters (QCI, ARP, GBR, and MBR) and EPS bearer QoS parameters (QCI, ARP, GBR, MBR, APN-AMBR, and UE-AMBR). The QCI and ARP are applied to all EPS bearers. An EPS bearer is classified as a GBR bearer or a non-GBR bearer depending on the resource type specified by its QCI. A default bearer must be non-GBR, while a dedicated bearer can be either GBR or non-GBR. Other than QCI and ARP, there are other QoS parameters for EPS bearers including MBR and GBR indicating the bandwidth (or bit rate) of an EPS bearer, and AMBR indicating the total bandwidth of multiple EPS bearers. The MBR and GBR are the maximum and the guaranteed bandwidths of an EPS bearer, respectively, and AMBR is the maximum total bandwidth of multiple EPS bearers [16,59].

Fig. 1.85 illustrates the QoS parameters applied to SDFs and EPS bearers. In this figure, the UE is connected to two PDNs. The UE has two IP addresses: IP address 1 assigned by PGW-1 for use in PDN-1, and IP address 2 assigned by PGW-2 for use in PDN-2. The UE has one default bearer and two dedicated bearers established for each PDN. The IP flows (user traffic) are filtered into SDFs in the PGW by using SDF templates. There are two groups of SDFs, each received from PDN-1 and PDN-2. For these SDFs, network resources are allocated and packet forwarding is treated according to the QoS rules set in the PGW. The SDFs are then mapped to EPS bearers based on their specified QCI and ARP. In case of PDN-1, as shown in the figure, the SDFs 1 and 2 are mapped to the default bearer, SDFs 3 and 4 are mapped to the non-GBR dedicated bearer, and SDF 5 is mapped to the GBR dedicated bearer, all forwarded to the UE. Such traffic mapped from SDF to EPS bearer is defined by using traffic filter template. All user traffic is subject to the EPS bearer QoS while being delivered through the EPS bearers. All non-GBR bearers associated with a PDN are controlled by the maximum APN-AMBR that they share while the ones associated with a UE are controlled by the maximum UE-AMBR that they share. In LTE, all QoS parameters for SDFs are provisioned by policy and charging rules function of the EPC [59].

The NG-RAN general QoS framework, both for NR connected to 5GC and for LTE connected to 5GC scenarios, is depicted in Fig. 1.86. For each UE, 5GC establishes one or more PDU sessions and the NG-RAN establishes one or more data radio bearers per PDU session. The NG-RAN maps packets belonging to different PDU sessions to different DRBs and establishes at least one default DRB for each PDU session. The NAS-level packet filters in the UE and in the 5GC associate uplink and downlink packets with QoS flows.

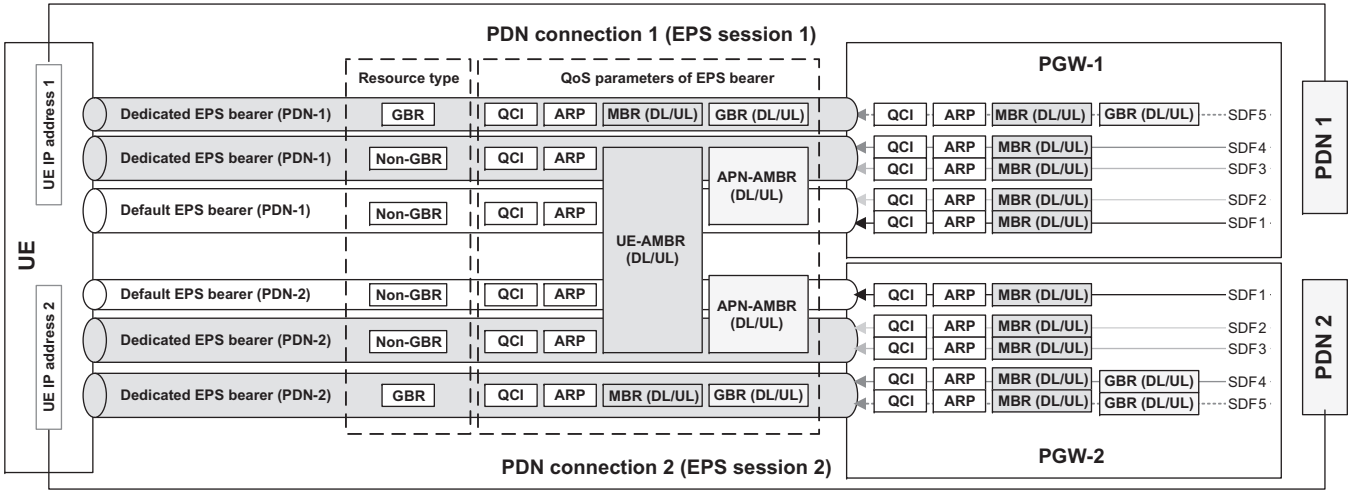


Figure 1.85
QoS parameters in LTE [59].

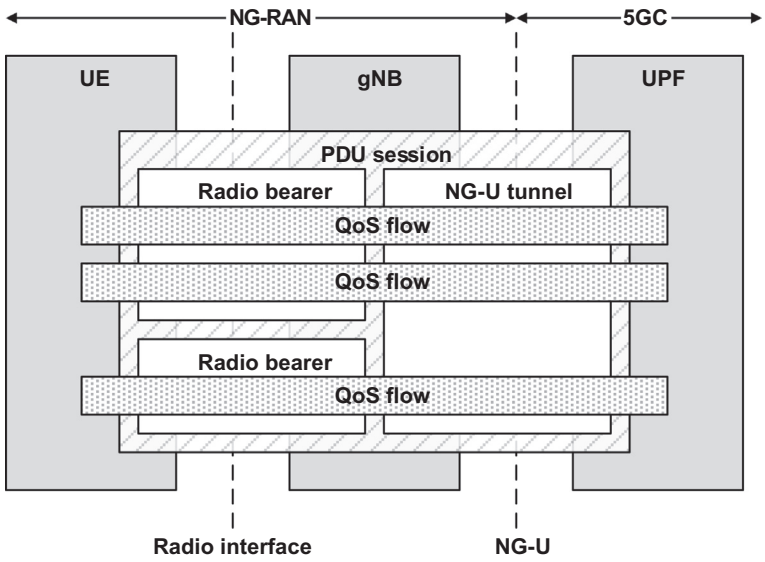


Figure 1.86
QoS framework in NR [16].

The AS-level mapping rules in the UE and in the NG-RAN associate uplink and downlink QoS flows with DRBs.

At NAS level, the QoS flow is the finest granularity for QoS differentiation in a PDU session. A QoS flow is identified within a PDU session by a QFI transferred in encapsulated format over NG-U. NG-RAN and 5GC ensure quality of service (e.g., reliability and maximum tolerable delay) by mapping packets to appropriate QoS flows and DRBs. There is a two-step mapping of IP-flows to QoS flows (NAS level) and from QoS flows to DRBs (AS level). At NAS level, a QoS flow is characterized by a QoS profile which is provided by 5GC to NG-RAN as well as a set of QoS rule(s) which are provided by 5GC to the UE. The QoS profile is used by NG-RAN to determine the treatment on the radio interface while the QoS rules define the mapping between uplink user-plane traffic and QoS flows in the UE. A QoS flow may either be GBR or non-GBR depending on its profile.

The QoS profile of a QoS flow contains QoS parameters, that is, a 5G QoS identifier (5QI) and an ARP. In case of a GBR QoS flow, the QoS parameters are guaranteed flow bit rate (GFBR) and maximum flow bit rate (MFBR) for uplink and downlink. In case of non-GBR, the QoS parameters include the newly defined reflective QoS attribute (RQA). The RQA, when included, indicates that some and not necessarily all traffic carried on this QoS flow is subject to reflective QoS at NAS level. At AS level, the DRB defines the packet treatment on the radio interface. A DRB serves packets with the same packet forwarding treatment. Separate DRBs may be established for QoS flows requiring different packet

forwarding treatments. In the downlink, the NG-RAN maps QoS flows to DRBs based on NG-U marking (QFI) and the associated QoS profiles. In the uplink, the UE marks uplink packets over the radio interface with the QFI for the purposes of marking forwarded packets to the core network. When reflective QoS is used, a 5G UE can create a QoS rule for the uplink traffic based on the received downlink traffic without generating control-plane signaling overhead, as shown in Fig. 1.87 [16].

In the uplink, the NG-RAN may control the mapping of QoS flows to DRB in two different ways. Reflective mapping where for each DRB the UE monitors the QFI(s) of the downlink packets and applies the same mapping in the uplink, that is, for a DRB, the UE maps the uplink packets belonging to the QoS flows(s) corresponding to the QFI(s) and PDU session observed in the downlink packets for that DRB. To enable reflective mapping, the NG-RAN marks downlink packets over the air interface with QFI. In addition to the reflective mapping, the NG-RAN may configure an uplink QoS flow to DRB mapping via RRC signaling. The UE always applies the latest update of the mapping rules regardless of whether it is performed via reflective mapping or explicit configuration. For each PDU session, a default DRB is configured. If an incoming uplink packet matches neither an RRC configured nor a reflective QoS flow ID to DRB mapping, the UE maps that packet to the default DRB of the PDU session. Within each PDU session, it is up to NG-RAN to decide how to map multiple QoS flows to a DRB. The NG-RAN may map a GBR flow and a non-GBR flow, or more than one GBR flow to the same DRB. The time when a non-default DRB between NG-RAN and UE is established for QoS flow can be different from the time when the PDU session is established. It is up to NG-RAN to decide when non-default DRBs are established. In dual connectivity scenarios, the QoS flows belonging to the same PDU session can be mapped to different bearer types and, consequently, there can be two different SDAP entities configured for the same PDU session, that is, one for MCG and another one for SCG [16].

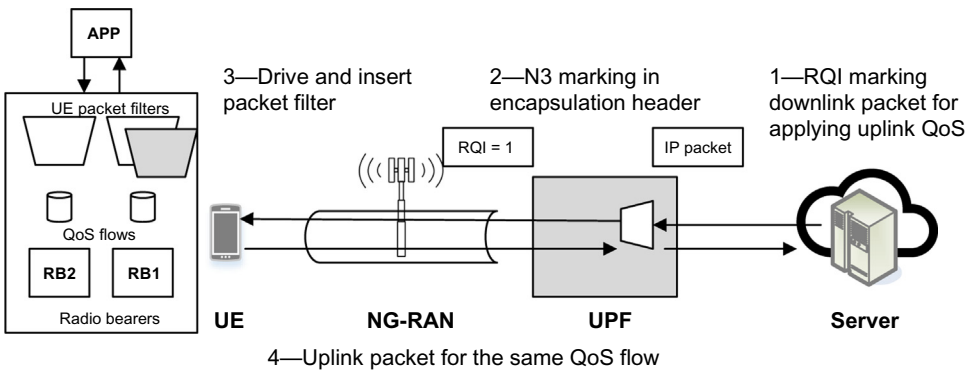


Figure 1.87
Illustration of the reflective QoS concept (example) [82].

As we mentioned earlier, the 5G QoS model is based on QoS flows. The 5G QoS model supports both QoS flows that require GBFR QoS flows and QoS flows that do not require guaranteed flow bit rate (non-GBFR QoS flows). The 5G QoS model also supports reflective QoS. The QoS flow is the finest granularity to differentiate QoS classes in the PDU session. A QFI is used to identify a QoS flow in the 5G system. User-plane traffic with the same QFI within a PDU session receives the same traffic forwarding treatment (e.g., scheduling and admission control). The QFI is carried in an encapsulated header format on N3 (and N9), that is, without any changes to the end-to-end packet header. The QFI is used for all PDU session types and is unique within a PDU session. The QFI may be dynamically assigned or may be equal to the 5QI. Monitoring of user-plane traffic (e.g., MFBR enforcement) is not considered as QoS differentiation and is done by UPFs on an SDF-level basis. Within the 5GS, a QoS flow is controlled by the SMF and may be preconfigured, established via the PDU session establishment procedure, or the PDU session modification procedures. Any QoS flow is characterized by a QoS profile provided by the SMF to the AN via the AMF over N2 reference point or is preconfigured in the AN; one or more QoS rule(s) which can be provided by the SMF to the UE via the AMF over N1 reference point and/or derived by the UE by applying reflective QoS control; and one or more SDF templates provided by the SMF to the UPF. In 5GS, the QoS flow of the default QoS rule is required to be established for a PDU session and to remain active throughout the lifetime of the PDU session. The QoS flow of the default QoS rule is a non-GBR QoS flow [3].

A QoS flow may be either GBR or non-GBR depending on its QoS profile, which contains the corresponding QoS parameters. For each QoS flow, the QoS profile includes the following parameters [3]:

- 5G QoS identifier (5QI)
- ARP
- For each non-GBR QoS flow, the QoS profile may include RQA
- For each GBR QoS flow, the QoS profile includes GFBR and MFBR for uplink and downlink
- In case of a GBR QoS flow only, the QoS parameters may include notification control and maximum packet loss rate for uplink and downlink

Each QoS profile has one corresponding QFI, which is not included in the QoS profile itself. The 5QI value may indicate that a QoS flow has signaled QoS characteristics, and if so, the QoS characteristics are included in the QoS profile.

The UE performs classification and marking of uplink user-plane traffic, that is, the association of uplink traffic to QoS flows based on the QoS rules. These QoS rules may be explicitly provided to the UE via the PDU session establishment/modification procedure, preconfigured in the UE or implicitly derived by the UE by applying reflective QoS. A QoS rule contains a QoS rule identifier which is unique within the PDU session, the QFI of the associated QoS flow and

except for the default QoS rule a packet filter set[77] for uplink and optionally for downlink and a precedence value.[78] Furthermore, for a dynamically assigned QFI, the QoS rule contains the QoS parameters relevant to the UE (e.g., 5QI, GBR and MBR, and the averaging window[79]). There are more than one QoS rule associated with the same QoS flow. A default QoS rule is required for each PDU session and associated with the QoS flow of the default QoS rule. The default QoS rule is the only QoS rule of a PDU session that may contain no packet filter set in which case, the highest precedence value is used. If the default QoS rule does not contain a packet filter set, the default QoS rule defines the treatment of packets that do not match any other QoS rules in a PDU session. If the default QoS rule does not contain a packet filter, the reflective QoS is not applied to the QoS flow of the default QoS rule.

The SMF performs binding of SDFs to QoS flows based on the QoS and service requirements. The SMF assigns the QFI for a new QoS flow and derives its QoS profile from the information provided by the PCF.[80] The SMF provides the QFI along with the QoS profile and a transport-level packet marking value for uplink traffic to the AN. The SMF further provides the SDF template, that is, the packet filter set associated with the SDF received from the PCF together with the SDF precedence value, the QoS-related information, and the corresponding packet marking information, that is, the QFI, the transport level packet marking value for downlink traffic and optionally the reflective QoS indication to the UPF enabling classification, bandwidth enforcement and marking of user-plane traffic. For each SDF, when applicable, the SMF generates a QoS rule. Each of these QoS rules contain the QoS rule identifier, the QFI of the QoS flow, the packet filter set of the uplink part of the SDF template, and optionally the packet filter set for the downlink part of the SDF template, as well as the QoS rule priority value set to the SDF precedence value. The QoS rules are then provided to the UE. The principle of classification and marking of user-plane traffic and mapping of QoS flows to AN resources is illustrated in Fig. 1.88 [3].

[77] A packet filter set is used in the quality of service rules or service data flow template to identify a quality of service flow. The packet filter set may contain packet filters for the downlink direction, the uplink direction, or packet filters that are applicable to both directions. There are two types of packet filter set, that is, IP packet filter set and Ethernet packet filter set, corresponding to those protocol data unit session types.

[78] The quality of service rule precedence value and the service data flow template precedence value determine the order in which a quality of service rule or a service data flow template, respectively, is evaluated. The evaluation of the quality of service rules or service data flow templates is performed in the increasing order of their precedence value.

[79] The averaging window is defined only for guaranteed bit rate quality of service flows and represents the duration over which the guaranteed flow bit rate and maximum flow bit rate are calculated. The averaging window may be signaled along with 5 QoS identifiers to the access network and user-plane function, and if it is not received, a predefined value will be applied.

[80] Policy control function provides policy framework incorporating network slicing, roaming and mobility management and is equivalent to policy and charging rules function in evolved packet core.

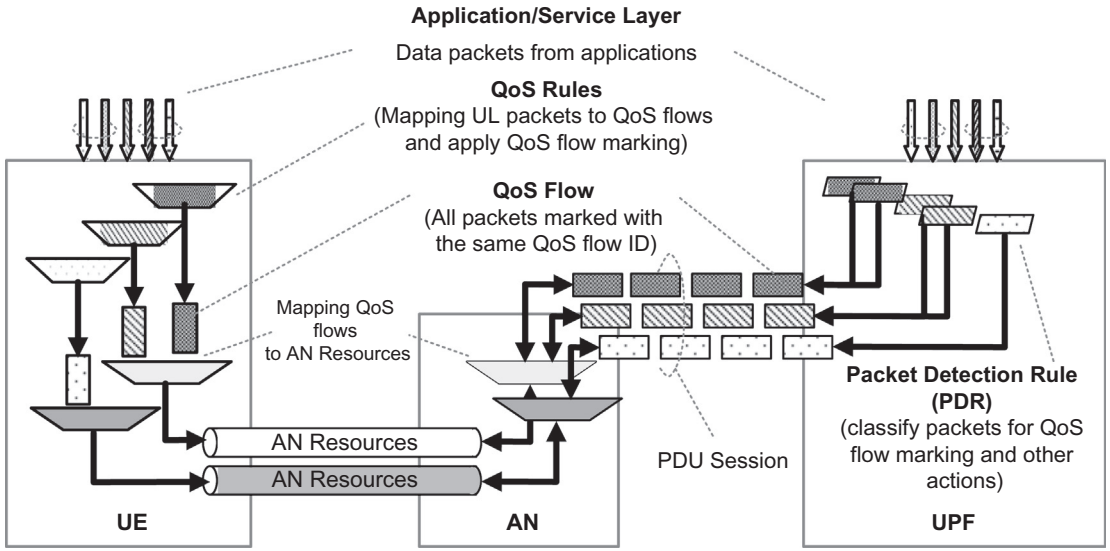


Figure 1.88
Classification and user-plane marking of QoS flows and mapping to access network resources [3].

In the downlink direction, the incoming data packets are classified by the UPF based on the Packet Filter Sets of the packet detection rules (PDRs) in the order of their precedence (without initiating additional N4 signaling). Note that packet detection rules contain information that is necessary to classify the PDU(s) arriving at the UPF. The UPF conveys the classification information of the user-plane traffic, corresponding to a QoS flow, through N3 (and N9) user-plane marking using QFI. The AN binds QoS flows to AN resources, that is, data radio bearers in 3GPP radio access. There is no one-to-one relationship between QoS flows and the AN resources, and it is the responsibility of the AN to establish the necessary AN resources that QoS flows can be mapped to. If a match cannot be found and all QoS flows are associated with a downlink packet filter set, the UPF will discard the downlink data packet.

In the uplink direction and for PDU sessions of type IP or Ethernet, the UE evaluates the uplink packets against the packet filter set in the QoS rules based on the precedence value of QoS rules in increasing order until a matching QoS rule is found (i.e., to find out which packet filter matches the uplink packet). The UE uses the QFI in the corresponding matching QoS rule to bind the uplink packet to a QoS flow. The UE then binds QoS flows to the AN resources. If no matching QoS rule is found, the UE discards the uplink data packet. The UPF maps user-plane traffic to QoS flows based on the PDRs [3] and performs session-AMBR enforcement and PDU counting for charging. The UPF further transmits the PDUs of the PDU session in a single tunnel between 5GC and access network. The UPF includes the QFI in the encapsulation header and it may further include an indication for reflective QoS activation. The UPF performs transport-level packet marking in downlink, which is based on the 5QI and ARP of the associated QoS flow. The access network maps PDUs from QoS flows to access-specific resources based on the QFI and the associated 5G QoS characteristics and parameters.

The UE uses the stored QoS rules to determine mapping between uplink user-plane traffic and QoS flows. The UE marks the uplink PDU with the QFI of the QoS rule containing the matching packet filter and transmits the uplink PDUs using the corresponding access-specific resource for the QoS flow based on the mapping provided by RAN. The access network transmits the PDUs to UPF. The access network includes the QFI value, in the encapsulation header of the uplink PDU when sending an uplink packet from the access network to the core network. The access network performs transport-level packet marking in the uplink, which may be based on the 5QI and ARP of the associated QoS flow. The UPF verifies whether QFIs in the uplink PDUs are aligned with the QoS rules provided to the UE or implicitly derived by the UE (e.g., in case of reflective QoS) and performs session-AMBR enforcement and counting of packets for charging.

The 5G QoS parameters can be further described in detail as follows [3]:

- 5QI is a scalar that is used as a reference to 5G QoS characteristics, that is, access node-specific parameters that control QoS forwarding treatment for the QoS flow (e.g., scheduling weights, admission thresholds, queue management thresholds, link layer

Table 1.4: 5QI to QoS characteristics mapping [3].

5QI Value	Resource Type	Default Priority Level	Packet Delay Budget (ms)	Packet Error Rate	Default Maximum Data Burst Volume (Bytes)	Default Averaging Window (ms)	Example Services
1	GBR	20	100	10^{-2}	N/A	2000	Conversational Voice
2		40	150	10^{-3}	N/A	2000	Conversational Video (Live Streaming)
3		30	50	10^{-3}	N/A	2000	Real-time Gaming, V2X Messages, Electricity Distribution, Process Automation
4		50	300	10^{-6}	N/A	2000	Non-Conversational Video (Buffered Streaming)
65		7	75	10^{-2}	N/A	2000	Mission-critical User-plane Push-to-Talk Voice
66		20	100	10^{-2}	N/A	2000	Non-mission-critical User-plane Push-to-Talk Voice
67		15	100	10^{-3}	N/A	2000	Mission-critical Video
75		–	–	–	–	–	–
5	Non-GBR	10	100	10^{-6}	N/A	N/A	IMS Signaling
6		60	300	10^{-6}	N/A	N/A	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		70	100	10^{-3}	N/A	N/A	Voice, Video (Live Streaming) Interactive Gaming
8		80	300	10^{-6}	N/A	N/A	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9		90					
69		5	60	10^{-6}	N/A	N/A	Mission-critical Delay Sensitive Signaling
70		55	200	10^{-6}	N/A	N/A	Mission-critical Data
79		65	50	10^{-2}	N/A	N/A	V2X Messages
80		68	10	10^{-6}	N/A	N/A	Low-latency eMBB Applications, Augmented Reality
82	Delay	19	10	10^{-4}	255	2000	Discrete Automation
83	Critical	22	10	10^{-4}	1354	2000	Discrete Automation
84	GBR	24	30	10^{-5}	1354	2000	Intelligent Transport Systems
85		21	5	10^{-5}	255	2000	Electricity Distribution

protocol configuration, etc.). The 5QI values have one-to-one mapping to standardized combination of 5G QoS attributes, as shown in Table 1.4. The 5G QoS characteristics for preconfigured 5QI values are preset in the AN, whereas the dynamically assigned 5QI values are signaled as part of the QoS profile.

- The ARP contains information about the priority level, the preemption capability and the preemption susceptibility. The priority level defines the relative importance of a resource request. This allows deciding whether a new QoS flow may be accepted or should be rejected in case of resource limitation, which is typically used for admission control of GBR traffic. It may also be used to decide which of the existing QoS flows to preempt in limited resource scenarios. The range of the ARP priority level is from 1 to 15, with 1 as the highest priority level. The preemption capability information defines if an SDF may use the resources that were already assigned to another SDF with a lower priority level. The preemption susceptibility information defines whether an SDF may lose the resources assigned to it in order to admit an SDF with higher priority level.
- The RQA is an optional parameter, which indicates that certain traffic carried in this QoS flow is subject to reflective QoS. The access network enables the transfer of the RQI for AN resource corresponding to this QoS flow when RQA is signaled. The RQA may be signaled to the NG-RAN via N2 reference point upon UE context establishment in NG-RAN and upon QoS flow establishment or modification.
- The notification control indicates whether notifications are requested from the RAN when the GFBR requirement can no longer be satisfied for a QoS flow during its lifetime. If the notification control is enabled for a given GBR QoS flow and the NG-RAN determines that the GFBR cannot be satisfied, the AN sends a notification to the SMF, where 5GC upon receiving the notification may initiate an N2 signaling to modify or remove the QoS flow.
- Each PDU session of a UE is associated with a session aggregate maximum bit rate (session-AMBR). The subscribed session-AMBR is a subscription parameter which is retrieved by the SMF from UDM. The SMF may use the subscribed session-AMBR or modify it based on local policy or use the authorized session-AMBR received from PCF. The session-AMBR limits the aggregate bit rate that can be expected across all non-GBR QoS flows for a specific PDU session.
- For GBR QoS flows, the 5G QoS profile includes DL/UL GFBR and DL/UL MFBR. The GFBR denotes the bit rate that may be expected to be provided by a GBR QoS flow. The MFBR limits the bit rate that may be expected to be provided by a GBR QoS flow, which means that the excess traffic may be discarded by a rate shaping function. The GFBR and MFBR parameters are signaled to the AN in the QoS profile and signaled to the UE as QoS flow level for each individual QoS flow.
- For each PDU session, the SMF retrieves the default 5QI and ARP from UDM. The SMF may change the default 5QI/ARP based on local configuration or interaction with the PCF. The default 5QI is derived from the standardized range of values for non-GBR 5QIs.

- The DL/UL maximum packet loss rate indicates the maximum rate for lost packets of the QoS flow that can be tolerated in the downlink or uplink, which is provided to the QoS flow, if it is compliant to GFBR.

The 5G QoS characteristics describe the packet forwarding treatment that a QoS flow receives between the UE and the UPF, which are described in terms of the following performance metrics [3]:

- Resource type (GBR, delay critical GBR, or non-GBR) determines whether dedicated network resources related to QoS flow-level GFBR value are permanently allocated, for example, by an admission control function in a base station. The GBR QoS flow is often dynamically authorized, which requires dynamic policy and charging control. A non-GBR QoS flow may be pre-authorized through static policy and charging control. There are two types of GBR resource types, GBR and delay critical GBR, where both resource types are treated in the same manner, except that the definition of PDB and packet error rate (PER) are different.
- Priority level indicates the resource scheduling priority among QoS flows. The priority levels are used to differentiate between QoS flows of the same UE and they are also used to differentiate between QoS flows from different UEs. Once all QoS requirements are satisfied for the GBR QoS flows, additional resources can be used for any remaining traffic in an implementation-specific manner. In addition, the scheduler may prioritize QoS flows based on other parameters such as resource type, radio condition, etc. in order to optimize application performance and network capacity.
- The packet delay budget defines an upper bound for the time that a packet may be delayed between the UE and the UPF that terminates N6 interface. The value of the PDB is the same in downlink and uplink for a certain 5QI. The PDB is used to support the configuration of scheduling and link layer functions (e.g., configuration of scheduling priority weights and HARQ target operating points). For a delay-sensitive GBR flow, a packet delayed more than PDB is considered as a lost packet, if the data burst is not exceeding the MDBV within the period of PDB and the QoS flow is not exceeding the GFBR. For GBR QoS flows with GBR resource type, the PDB is interpreted as a maximum delay with a confidence interval of 98%.
- The packet error rate defines an upper bound for the rate of PDUs or IP packets that have been processed by the sender of a link layer protocol, but are not successfully delivered by the corresponding receiver to the upper layers. Therefore, the PER defines an upper bound for non-congestion related packet losses. The purpose of the PER is to find appropriate link layer protocol configurations. For some 5QI values, the target PER is the same in the downlink and uplink. For QoS flows with delay-sensitive GBR resource type, a packet which is delayed more than PDB is dropped and included in the PER calculation, unless the data burst is exceeding the MDBV within the period of PDB or the QoS flow is exceeding the GFBR.

- Averaging window is defined only for GBR QoS flows and denotes the time interval over which the GFBR and MFBR are calculated. The averaging window may be signaled with 5QIs to the AN and the UPF and if it is not received a predefined value is used.
- The maximum data burst volume (MDBV) is associated with each GBR QoS flow with delay-sensitive resource type. The MDBV denotes the largest amount of data that a 5G-AN is required to serve within a period of 5G-AN PDB (i.e., 5G-AN part of the PDB). Each standardized 5QI of delay-sensitive GBR resource type is associated with a default value for the MDBV. The MDBV may also be signaled together with a standardized or pre-configured 5QI to the AN.

Reflective QoS enables a UE to map uplink user-plane traffic to QoS flows without SMF provided QoS rules, which is applied to IP and Ethernet PDU sessions. The support of reflective QoS over the access network is controlled by 5GC. The UE derives the reflective QoS rule from the received downlink traffic. It must be noted that it is possible to apply reflective QoS and non-reflective QoS concurrently within the same PDU session. For user traffic that is subject to reflective QoS, the uplink packets are assigned the same QoS marking as the reflected downlink packets. Reflective QoS is controlled on per-packet basis using the RQI in the encapsulation header on N3 reference point together with the QFI and a reflective QoS timer (RQ timer) value that is either signaled to the UE upon PDU session establishment or set to a default value.

To summarize this section, as we discussed 5G session management supports a PDU connectivity service that provides PDU exchange between a UE and a data network. In 5GC, the SMF is responsible for handling session management procedures. There is a notable difference in session management between EPC and 5GC. In EPC, the entire session is maintained by a single MME in a centralized manner, so that the user-plane path is established via a centralized PGW. This potentially results in congestion of backhaul traffic at the PGW, whereas in 5GC, different PDU sessions can be maintained by conceivably different SMFs, and their user-plane paths are established via multiple UPFs. This can distribute the cellular operator's backhaul traffic within the 5GC and reduce the perceived latency by the user. Compared to LTE's QoS framework, which is bearer-based and uses control-plane signaling, the 5G system adopts the QoS flow-based framework, and uses both control-plane and user-plane (i.e., reflective QoS) signaling in order to satisfy various application/service QoS requirements. The QoS flow-based framework enables flexible mapping of QoS flows to DRB(s) by decoupling the QoS flow and the radio bearer, allowing more flexible QoS characteristics. When reflective QoS is used, the 5G UE can create a QoS rule for the uplink traffic based on the received downlink traffic without generating control-plane signaling overhead. Table 1.5 summarizes and compares the EPS and 5GS QoS and session management features.

Table 1.5: Comparison of LTE and NR QoS and session management characteristics [71].

	RAN-Level Interworking		5G SA With Core-Network-Level Interworking
	With EPC	With 5GC	
Network slicing	Per device (dedicated core)	Per service (enabling third-party service)	Per service (enabling third-party service)
Session management	Limited and centralized	Flexible and distributed (lower cost, lower latency)	Flexible and distributed (lower cost, lower latency)
QoS	Per-bearer Network-initiated	Per-flow UE/network-initiated (dynamic QoS)	Per-flow UE/network-initiated (dynamic QoS)

1.7 Security Framework

We begin this section with a review of security framework in LTE to set the stage for the 5G security framework discussion. Fig. 1.89 shows the scope and overall concept of the LTE security architecture. In LTE, the authentication function performs mutual authentication between the UE and the network. The NAS security performs integrity protection/verification and ciphering (encryption/decryption) of NAS signaling between the UE and the MME. The AS security is responsible for integrity protection/verification and ciphering of RRC signaling between the UE and the eNB and further performs ciphering of user traffic between the UE and the eNB.

In 3GPP networks, authentication refers to the process of determining whether a user is an authorized subscriber to the network that it is trying to access. Among various authentication procedures, EPS AKA procedure is used in LTE networks for mutual authentication between users and networks. The EPS AKA procedure consists of two steps: (1) the home subscriber server (HSS) generates EPS authentication vector(s) (RAND, AUTN, XRES, K_{ASME}) and delivers them to the MME and (2) the MME selects one of the authentication vectors and uses it for mutual authentication with the UE and shares the same authentication key (K_{ASME}). Mutual authentication is the process in which a network and a user authenticate each other. In LTE networks, since the identification of the user's serving network is required when generating authentication vectors, authentication of the network by the user is performed in addition to authentication of the user by the network. Access security management entity (ASME) is an entity that receives top-level key(s) from the HSS to be used in an AN. In EPS, the MME serves as the ASME and K_{ASME} is used as the top-level key in the AN. The MME conducts mutual authentication with the UE on behalf of the HSS using K_{ASME}. Once mutually authenticated, the UE and MME share the same K_{ASME} as an authentication key.

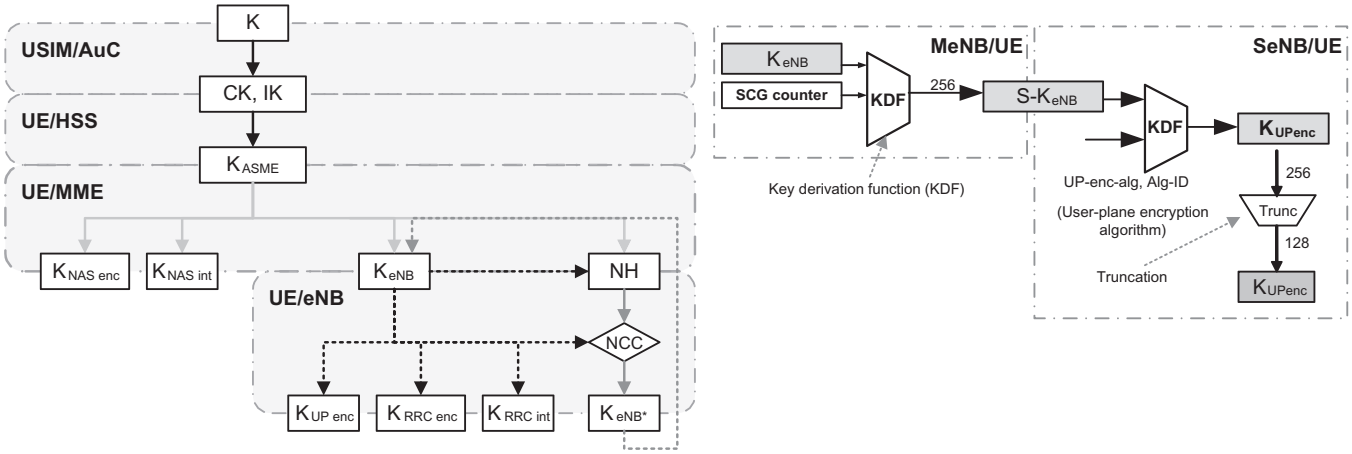


Figure 1.89
Key derivation in LTE and dual connectivity [56,57].

NAS security is designed to securely deliver signaling messages between the UE and the MME over the radio link and to perform integrity protection/verification as well as ciphering of NAS signaling messages. Different keys are used for integrity verification and ciphering. While integrity verification is a mandatory function, ciphering is an optional function. The NAS security keys, such as integrity key (K_{NASint}) and ciphering key (K_{NASenc}), are derived by the UEs and the MMEs from K_{ASME} (see Fig. 1.89). In Fig. 1.89, next hop (NH) key is used by the UE and eNB in the derivation of K_{eNB^*} for provisioning forward security. The NH is derived by UE and MME from K_{ASME} and K_{eNB} when the security context is established, or from K_{ASME} and the previous NH. The NH chaining count (NCC) is a counter related to NH, that is, the number of key chaining that has been performed, which allows the UE to be synchronized with the eNB and to determine whether the next K_{eNB^*} needs to be based on the current K_{eNB} or a fresh NH value [56,57].

AS security is used to ensure secure delivery of data between a UE and an eNB over the radio interface. It includes both integrity check and ciphering of RRC signaling messages over the control plane, and only ciphering of IP packets over the user plane. Different keys are used for integrity check/ciphering of RRC signaling messages and ciphering of IP packets. Integrity verification is mandatory, but ciphering is optional. AS security keys, such as K_{RRCint}, K_{RRCenc}, and K_{UPenc}, are derived from K_{eNB} by a UE and an eNB. K_{RRCint} and K_{RRCenc} are used for integrity check and ciphering of control-plane information (i.e., RRC signaling messages), and K_{UPenc} is used for ciphering of user-plane data (i.e., IP packets). Integrity verification and ciphering are performed at the PDCP sublayer.

Key derivation for dual connectivity SCG bearers is depicted in Fig. 1.89, where SCG counter is a counter used as freshness input into S-K_{eNB} derivations. For SCG bearers in dual connectivity, the user-plane keys are updated upon SCG change by conveying the value of the SCG counter to be used in key derivation to the UE via RRC signaling. When K_{eNB} is refreshed, SCG counter is reset and S-K_{eNB} is derived from the K_{eNB}. The SCG bearers in dual connectivity scenarios share a common pool of radio bearer identities (DRB IDs) with the MCG bearers. When no new DRB ID can be allocated for an SCG bearer without guaranteeing COUNT reuse avoidance, the MeNB derives a new S-K_{eNB}. The SeNB informs MeNB when the uplink or downlink PDCP COUNTs are about to wrap around. In that case, the MeNB updates the S-K_{eNB}. To update the S-K_{eNB}, the MeNB increases the SCG counter and uses it to derive a new S-K_{eNB} from the currently active K_{eNB} in the MeNB. The MeNB sends the freshly derived S-K_{eNB} to the SeNB. The newly derived S-K_{eNB} is then used by the SeNB in computing a new encryption key K_{UPenc} which is used for all DRBs in the SeNB for the target UE. Furthermore, when the SCG counter approaches its maximum value, the MeNB refreshes the currently active K_{eNB}, before any further S-K_{eNB} is derived [56,57].

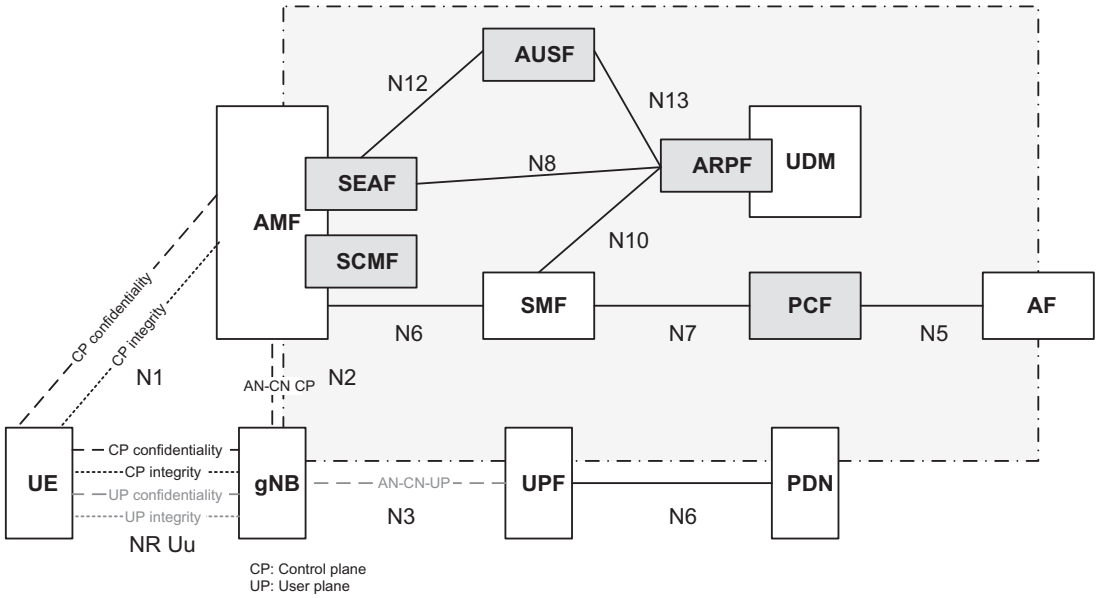


Figure 1.90
5GS security architecture and termination points [54].

Fig. 1.90 shows 5G security architecture including the new security entities: SEAF, AUSF, authentication credential repository and processing function (ARPF), security context management function (SCMF), and security policy control function (SPCF).

5GC has introduced a new security anchor called SEAF, which may be co-located with the AMF. The SEAF will create, for the primary authentication, a unified anchor key K_{SEAF} (common for all access links) that can be used by the UE and the serving network to protect the subsequent communications. It is possible to generate two anchor keys for certain scenarios where a UE is connected to 3GPP access (visited network) and to a non-3GPP access (home network). For normal roaming scenarios, the SEAF is located in the visited network. The AUSF terminates requests from the SEAF and further interacts with the ARPF. Depending on how the authentication functionality is split, the AUSF and the ARPF may be co-located, but an interface similar to SWx interface is defined for EAP-AKA and EAP-AKA′. The ARPF is co-located with the UDM and stores long-term security credentials such as the key K in EPS AKA or EAP-AKA for authentication. It can run cryptographic algorithms using long-term security credentials as input and can create the authentication vectors. Another new functional entity is the SCMF, which may be co-located with the SEAF in the AMF and retrieve a key from the SEAF, which is used to derive further access network specific keys. The SPCF provides the security policy to the network entities (e.g., SMF, AMF) and/or to the UE depending on the application-level input from the AF and may be stand-alone or co-located with the PCF. The security policy may include

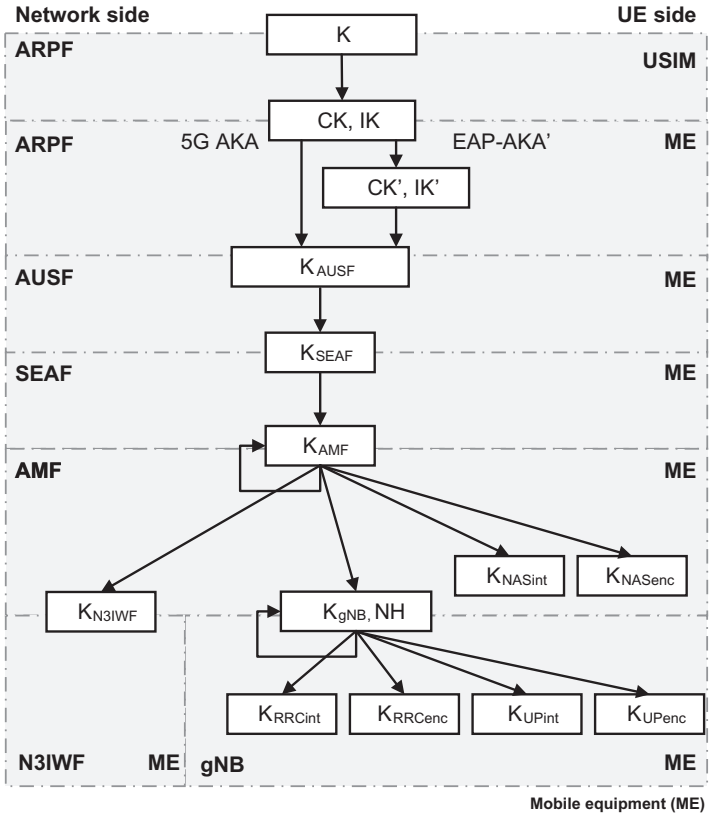


Figure 1.91
Key hierarchy in 5GS [9].

information about AUSF selection, confidentiality protection algorithm, integrity protection algorithm, key length and key life cycle. Fig. 1.91 shows the key hierarchy in 5GS [54].

The new security anchor key K_{SEAF} is used to further derive the access network key K_{AN} and the NAS keys K_{NAS}. There is only one NAS security termination entity, which is the AMF. The user-plane data on the radio bearer can be secured on a per session basis with the key K_{UP}. A session can belong to the same or different network slices. All key sets for NAS, RRC, and user-plane consist of an integrity key and a confidentiality key for encryption. Recall that the termination point of the user-plane security is at eNB in LTE networks. However, the gateway location may vary in order to provide different type of services, and the gNB may be located at the edge, that is, an exposed environment. Thus, the termination point of user-plane security should be reconsidered with the principle that security termination is in the entity where the traffic terminates. The user-plane security terminates at PDCP sublayer of gNB. This is aligned with LTE security framework that radio interface security

is provided by the PDCP layer for control and user planes. This mechanism allows provisioning the security termination point in a CU of the gNB that typically resides in a secure location.

The key hierarchy shown in Fig. 1.90 includes the following keys: K_{SEAF}, K_{AMF}, K_{NASint}, K_{NASenc}, K_{N3IWF}, K_{gNB}, K_{RRCint}, K_{RRCenc}, K_{UPint}, and K_{UPenc}, which can be divided into the following groups [9]:

- Keys for NAS signaling include K_{NASint}, which is a key that is used for the protection of NAS signaling with a particular integrity algorithm, as well as K_{NASenc} which is a key that is used for the protection of NAS signaling with a particular encryption algorithm.
- Keys for user-plane traffic include K_{UPenc}, which is a key that is used for the protection of user-plane traffic with a particular encryption algorithm, as well as K_{UPint} which is a key that is used for the protection of user-plane traffic between mobile equipment and gNB with a particular integrity algorithm.
- Keys for RRC signaling include K_{RRCint} which is a key that is used for the protection of RRC signaling with a particular integrity algorithm, as well as K_{RRCenc} which is a key that is used for the protection of RRC signaling with a particular encryption algorithm.
- Intermediate keys include next hop (NH), which is a key that is derived by mobile equipment and AMF to provide forward security as well as K_{gNB}^{*} which is a key that is derived by mobile equipment and gNB when performing a horizontal or vertical key derivation.

When a UE obtains services in RRC idle mode, it does not validate the eNB, which may result in camping on a wrong base station, ultimately leading to denial of service attack. In current LTE systems, the RAN security has been focused on RRC_CONNECTED state, which has been improved in 5G security framework.

The purpose of the primary authentication and key agreement procedures is to enable mutual authentication between the UE and the network and to provide key derivation material that can be used between the UE and network in subsequent security procedures. The keying material generated by the primary authentication and key agreement procedure results in an anchor key called the K_{SEAF} provided by the AUSF to SEAF. Keys for more than one security context can be derived from the K_{SEAF} with no need for a new authentication.

In 5G systems, the storage of credentials and identities for both human and machine type devices is required in the UE. The credentials and identities can be stolen through hardware/software attacks. Such security threats can impact the subscriber and/or the network. 3GPP UE security framework provides the following features for storage of UE credentials: integrity protection of the subscription credential(s); confidentiality protection of the

long-term key(s) of the subscription credential(s); and execution of the authentication algorithm(s) that make use of the subscription credentials. These features must be implemented in the UE, with using a tamper resistant secure hardware component. The subscriber identity module (SIM) functions for 5G are inherited from previous standards. Similar to LTE systems, the 5G USIM will be able to generate symmetric keys. It may also be able to generate new asymmetric key pairs and even new trusted public keys.

Network slicing requires basic security from the UE side when accessing a slice; however, this is not trivial and there are new security challenges. The slice isolation must be ensured for network slices, without which attackers who access to one slice may attempt an attack to other slices. Proper isolation will enable integrity and confidentiality protection. Moreover, it should be ensured that resources of the network infrastructure or an NSI are not impacted from another slice instance, to minimize attacks and to provide availability. 5G UE can simultaneously access to different network slices for multiple services. Such access can be via various type of RANs including both 3GPP and non-3GPP access. When the network slice selection data is tampered, unauthorized UEs may use such information to establish connection with the network slice and consume network resources. On the other hand, the advantage of network slicing is that operators are able to provide customized security for each slice. Different access authentication and authorization can be provided within different network slice tenants that can be extended to host applications. In order to support network-controlled privacy of slice information for the slices that the UE can access, the UE must be made aware or configured with privacy considerations that apply to NSSAI. The UE must not include NSSAI in NAS signaling or unprotected RRC signaling unless it has a NAS security context setup [3].

References

3GPP Specifications[81]

[1] 3GPP TS 23.214, Architecture enhancements for control and user plane separation of EPC nodes, Stage 2 (Release 15), September 2017.
[2] 3GPP TS 23.402, Architecture enhancements for non-3GPP accesses (Release 15), March 2018.
[3] 3GPP TS 23.501, System architecture for the 5G system (Release 15), December 2018.
[4] 3GPP TS 23.502, Procedures for the 5G system (Release 15), April 2019.
[5] 3GPP TR 23.714, Study on control and user plane separation of EPC nodes (Release 14), June 2016.
[6] 3GPP TR 23.799, Study on architecture for next generation system (Release 14), December 2016.
[7] 3GPP TR 28.801, Study on management and orchestration of network slicing for next generation network (Release 15), January 2018.
[8] 3GPP TS 29.244, Interface between the control plane and the user plane of EPC nodes, Stage 3 (Release 15), March 2019.
[9] 3GPP TS 33.501, Security architecture and procedures for 5G system (Release 15), December 2018.
[10] 3GPP TR 33.899, Study on the security aspects of the next generation system (Release 14), August 2017.

[81] 3GPP specifications can be accessed at the following URL: http://www.3gpp.org/ftp/Specs/archive/.

[11] 3GPP TS 36.104, Evolved universal terrestrial radio access (E-UTRA), Base Station (BS) Radio Transmission and Reception (Release 15), June 2018.
[12] 3GPP TR 36.932, Scenarios and requirements for small cell enhancements for E-UTRA and E-UTRAN (Release 14), March 2017.
[13] 3GPP TS 37.340, Multi-connectivity, Stage 2 (Release 15), January 2018.
[14] 3GPP TS 38.104, NR; base station (BS) radio transmission and reception (Release 15), January 2018.
[15] 3GPP TS 38.401, NG-RAN, architecture description (Release 15), December 2018.
[16] 3GPP TS 38.300 NR, Overall description, Stage-2 (Release 15), December 2018.
[17] 3GPP TS 38.410 NG-RAN, NG general aspects and principles (Release 15), December 2018.
[18] 3GPP TS 38.411 NG-RAN, NG layer 1 (Release 15), December 2018.
[19] 3GPP TS 38.412 NG-RAN, NG signaling transport (Release 15), December 2018.
[20] 3GPP TS 38.413 NG-RAN, NG application protocol (NGAP) (Release 15), December 2018.
[21] 3GPP TS 38.414 NG-RAN, NG data transport (Release 15), December 2018.
[22] 3GPP TS 38.420 NG-RAN, Xn general aspects and principles (Release 15), December 2018.
[23] 3GPP TS 38.421 NG-RAN, Xn layer 1 (Release 15), December 2018.
[24] 3GPP TS 38.422 NG-RAN, Xn signaling transport (Release 15), December 2018.
[25] 3GPP TS 38.423 NG-RAN, Xn application protocol (XnAP) (Release 15), December 2018.
[26] 3GPP TS 38.424 NG-RAN, Xn data transport (Release 15), December 2018.
[27] 3GPP TS 38.425 NG-RAN, Xn interface user plane protocol (Release 15), December 2018.
[28] 3GPP TS 38.470 NG-RAN, F1 general aspects and principles (Release 15), December 2018.
[29] 3GPP TS 38.471 NG-RAN, F1 layer 1 (Release 15), December 2018.
[30] 3GPP TS 38.472 NG-RAN, F1 signaling transport (Release 15), December 2018.
[31] 3GPP TS 38.473 NG-RAN, F1 application protocol (XnAP) (Release 15), December 2018.
[32] 3GPP TS 38.474 NG-RAN, F1 data transport (Release 15), December 2018.
[33] 3GPP TS 38.475 NG-RAN, F1 interface user plane protocol (Release 15), December 2018.
[34] 3GPP TR 38.801, Study on new radio access technology: radio access architecture and interfaces (Release 14), March 2017.
[35] 3GPP TR 38.804, Study on new radio access technology radio interface protocol aspects (Release 14), March 2017.
[36] 3GPP TR 38.806, Study of separation of NR control plane (CP) and user plane (UP) for split option 2 (Release 15), December 2017.

ETSI Specifications[82]

[37] ETSI GS NFV-SWA 001, Network functions virtualization (NFV), virtual network functions architecture, December 2014.
[38] ETSI GS NFV-IFA 001, Network functions virtualization (NFV), acceleration technologies, report on acceleration technologies & use cases, December 2015.
[39] ETSI GS NFV-IFA 002, Network functions virtualization (NFV) Release 2, Acceleration Technologies, VNF Interfaces Specification, August 2017.
[40] ETSI GS NFV-INF 001, Network functions virtualization (NFV), Infrastructure Overview, January 2015.
[41] ETSI GS NFV 002, Network functions virtualization (NFV), Architectural Framework, December 2014.
[42] ETSI, Network functions virtualization, White Paper on NFV Priorities for 5G, February 2017.
[43] ETSI, Network functions virtualization, Introductory White Paper, October 2012.
[44] ETSI, Network functions virtualization, White Paper, October 2014.
[45] ETSI GS MEC-IEG 004, Mobile-edge computing (MEC), Service Scenarios, November 2015.
[46] ETSI GS MEC 003, Mobile edge computing (MEC), Framework and Reference Architecture, March 2016.

[82] ETSI specifications can be accessed at the following URL: http://www.etsi.org/deliver/.

Articles, Books, White Papers, and Application Notes

[47] China Mobile Research Institute, Toward 5G C-RAN: Requirements, Architecture and Challenges, November 2016.
[48] SDN, NFV, and MEC on SDxCentral. available at: <https://www.sdxcentral.com/>.
[49] Open Networking Foundation, OpenFlow Switch Specification, version 1.5.1, March 2015.
[50] Y. Chao Hu, et al., Mobile edge computing: a key technology towards 5G, ETSI White Paper No. 11, September 2015.
[51] 5G network architecture, a high-level perspective, Huawei Technologies Co., Ltd., 2016.
[52] K. Miyamoto, et al., Analysis of mobile fronthaul bandwidth and wireless transmission performance in split-PHY processing architecture, Optics Express 24 (2) (2016) 1261−1268.
[53] D. Sabella, et al., Mobile-edge computing architecture, the role of MEC in the Internet of Things, IEEE Consumer Electron Mag. 5 (4) (2016).
[54] X. Zhang, et al., Overview of 5G security in 3GPP, in: IEEE Conference on Standards for Communications and Networking (CSCN), September 2017.
[55] J. Kim, et al., 3GPP SA2 architecture and functions for 5G mobile communication system, The Korean Institute of Communications Information Sciences, 2017.
[56] LTE security I: LTE security concept and LTE authentication, NMC Consulting Group, July 2013.
[57] LTE security II: NAS and AS security, NMC Consulting Group, July 2013.
[58] LTE network architecture, NMC Consulting Group, July 2013.
[59] LTE QoS-SDF and EPS bearer QoS, NMC Consulting Group, September 2013.
[60] Emergence of C-RAN: separation of baseband and radio, and baseband centralization, NMC Consulting Group, March 2014.
[61] The benefits of cloud-RAN architecture in mobile network expansion, Fujitsu Network Communications Inc., 2014.
[62] NGMN Alliance, 5G end-to-end architecture framework, October 2017.
[63] NGMN Alliance, Service-based architecture in 5G, January 2018.
[64] NGMN Alliance, Update to NGMN description of network slicing concept, October 2016.
[65] NGMN Alliance, NGMN paper on edge computing, October 2016.
[66] NGMN Alliance, Backhaul provisioning for LTE-advanced & small cells, October 2015.
[67] NGMN Alliance, Project RAN evolution: further study on critical C-RAN technologies, March 2015.
[68] J. Liu, et al., Ultra-dense networks (UDNs) for 5G, IEEE 5G Tech Focus 1 (1) (2017) 6.
[69] J. Wannstrom, et al., HetNet/small cells. Available from: <http://www.3gpp.org/hetnet>.
[70] N.T. Le, et al., Survey of promising technologies for 5G networks, Mobile Information Systems 2016 (2016) 6 pp.
[71] V.G. Nguyen, K.J. Grinnemo, SDN/NFV-based mobile packet core network architectures: a survey, IEEE Commun. Surv. Tutor 19 (3) (2017) 1567−1602.
[72] J.E. Mitchell, Integrated wireless backhaul over optical access networks, J Lightw. Technol. 32 (20) (2014) 3373−3382.
[73] R. Trivisonno, et al., Network slicing for 5G systems, in: IEEE Conference on Standards for Communications and Networking (CSCN), 2017.
[74] 5G Service-Guaranteed Network Slicing, White Paper, Huawei Technologies Co., Ltd., February 2017.
[75] CPRI Specification V7.0, Common Public Radio Interface (CPRI): Interface Specification, October 2015.
[76] eCPRI Specification V1.2, Common Public Radio Interface: eCPRI Interface Specification, June 2018.
[77] IEEE Std 1914.3-2018, Standard for radio over Ethernet encapsulations and mappings, September 2018.
[78] IEEE P1914.1/D4.1, Draft standard for packet-based fronthaul transport networks, April 2019.
[79] D. Anzaldo, Backhaul alternatives for HetNet small cells, Part 1 and 2, Microwaves & RF, September 2015.
[80] Wireless Backhaul Spectrum Policy Recommendations and Analysis Report, GSMA, November 2014.
[81] R. Ravindran, et al., Realizing ICN in 3GPP's 5G NextGen core architecture, Cornell University Library, November 2017.

[82] 4G-5G Interworking, RAN-level and CN-level Interworking, Samsung, June 2017.
[83] Nomor Research, 5G RAN Architecture Interfaces and eCPRI, September 2017.
[84] R. Vaez-Ghaemi, The evolution of fronthaul networks, Viavi Solutions, June 2017.
[85] Sujuan Feng and Eiko Seidel, Self-Organizing Networks (SON) in 3GPP Long Term Evolution, Nomor Research GmbH, May 2008.