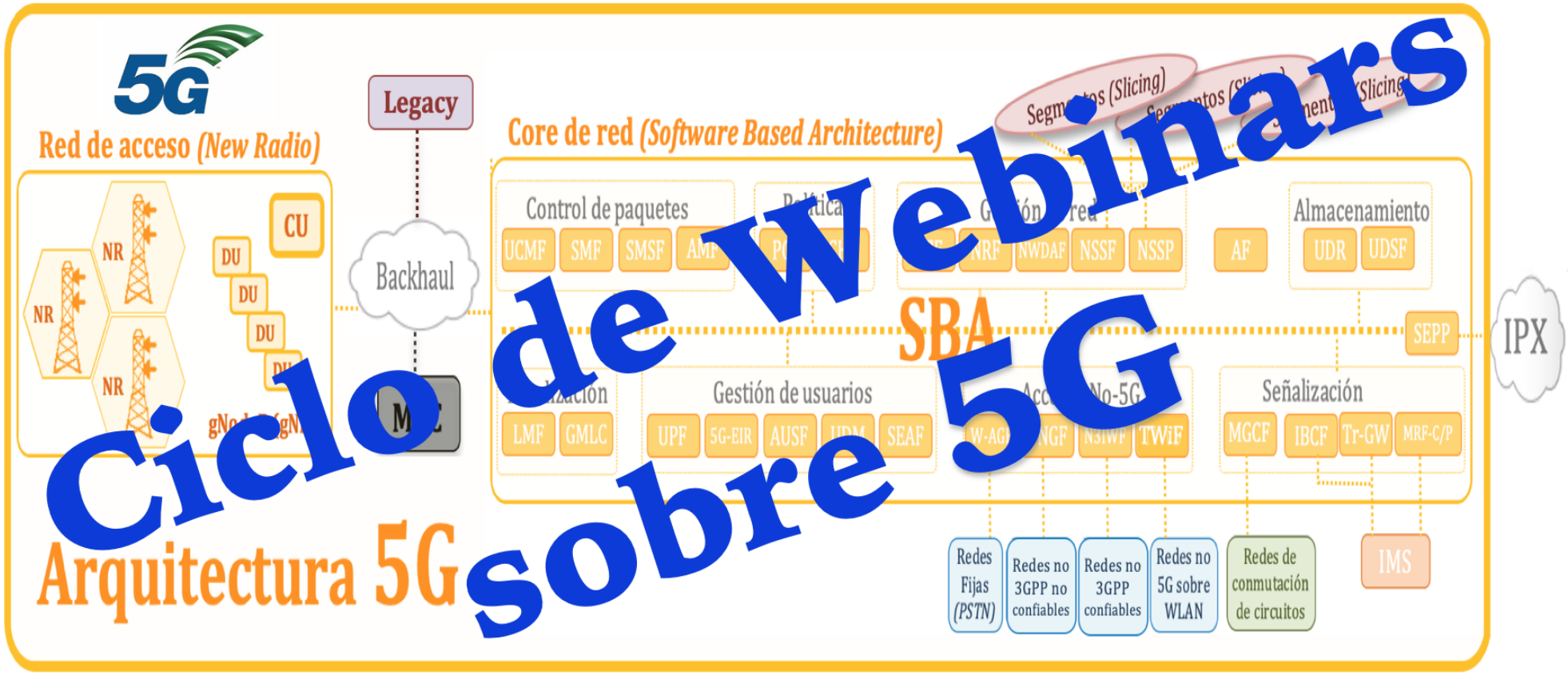
Tema 3: SBA, MEC y Slicing



Ciclo de Webinars sobre 5G

Alejandro Corletti Estrada

acorletti@darFe.es

www.darFe.es

Ciclo de Webinars sobre 5G

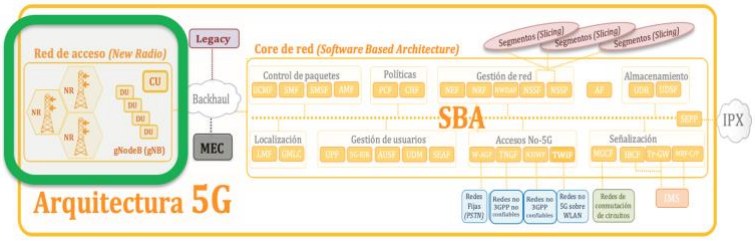
Tema 3: SBA, MEC y Slicing

DESARROLLO DEL CICLO DE WEBINARS

Webinar 1: Presentación y evolución de las tecnologías móviles

Webinar 2: New Radio y gNodeB

- Descripción de diseño de los gNB
- Open RAN
- Antenas compartidas (RAN Sharing)
- Frecuencias licitadas y asignadas
- Empleo de Cloud

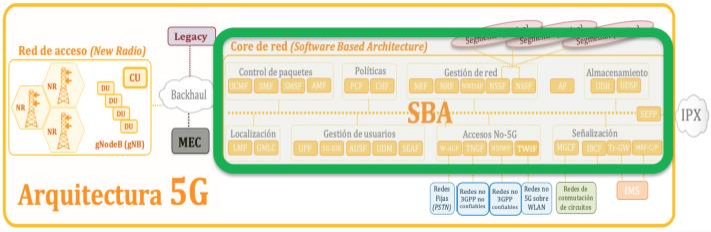


Tema de hoy

Webinar 3: SBA, MEC y Slicing

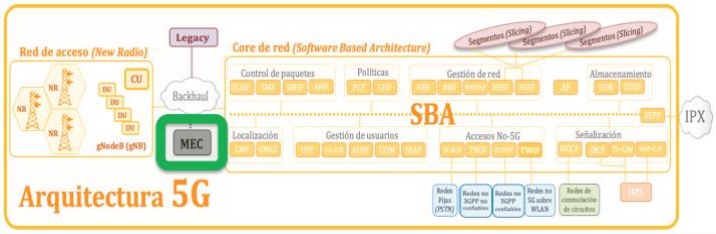
SBA (Core 5G) (Service Based Architecture)

- Descripción
- Funciones de red (NF)
- Security Edge Protection Proxy (SEPP)
- Empleo de Cloud



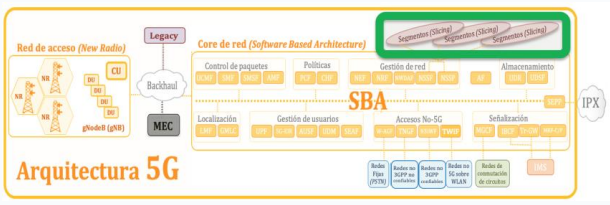
MEC (Multi-access Edge Computing)

- Empleo y detalle de MEC
- Análisis de contratos



Slicing (Segmentos)

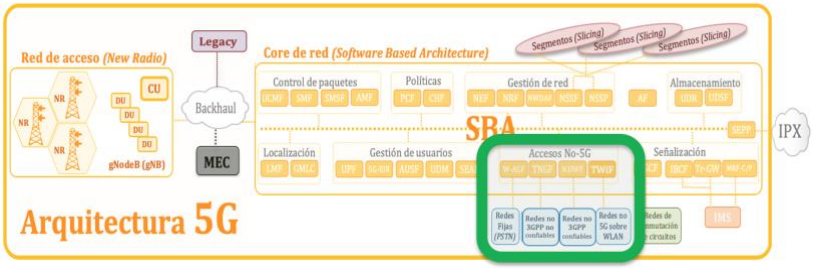
- **mMTC**: massive Machine Type Communication - ***IoT***
- **eMBB**: enhanced Mobile Broadband (eMBB) - ***Eventos***
- **URLLC**: Ultra-Reliable Low Latency Communications - ***Salud***
- **V2X**: Vehicle to X - ***Vehículos autónomos***.
- Plantillas GST (Generic network Slice Template)



Webinar 4: Accesos y autenticación

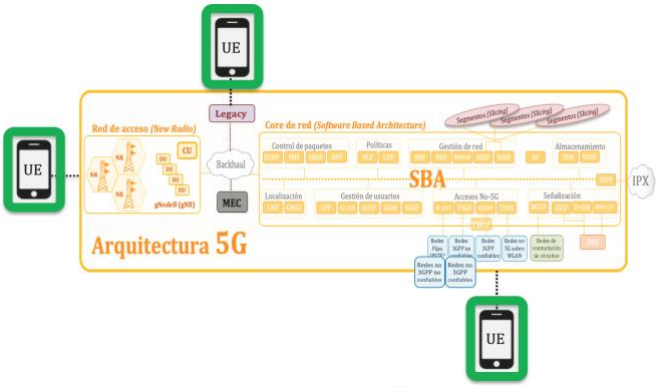
Otros accesos

- Small Cell
- Accesos Non-3GPP Trusted
- Accesos Non-3GPP No Trusted
- Accesos desde red Fija
- Otros



Accesos UE (User Equipment)

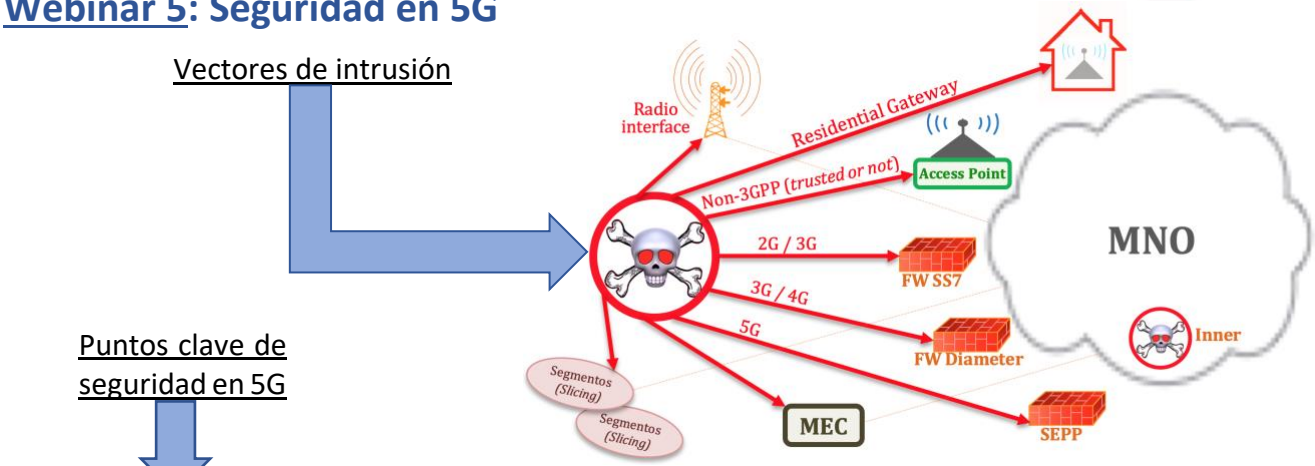
- a. UICC 4G heredado con aplicación USIM
- b. 4G UICC actualizado con la aplicación USIM
- c. 5G UICC con aplicación USIM

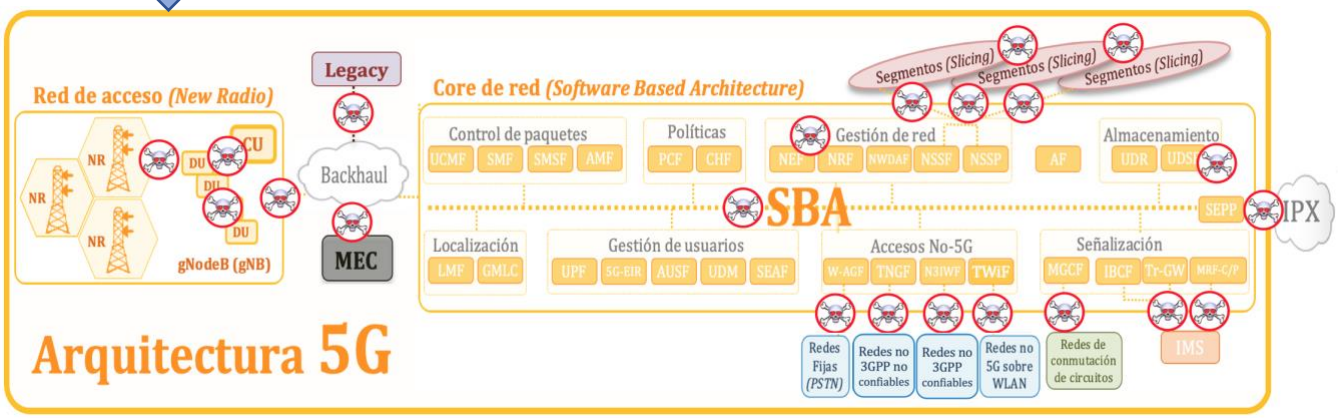


Webinar 5: Seguridad en 5G

Vectores de intrusión

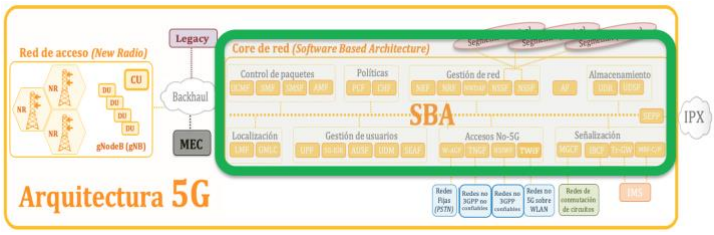
Puntos clave de seguridad en 5G





1. SBA (Core 5G) (Service Based Architecture).

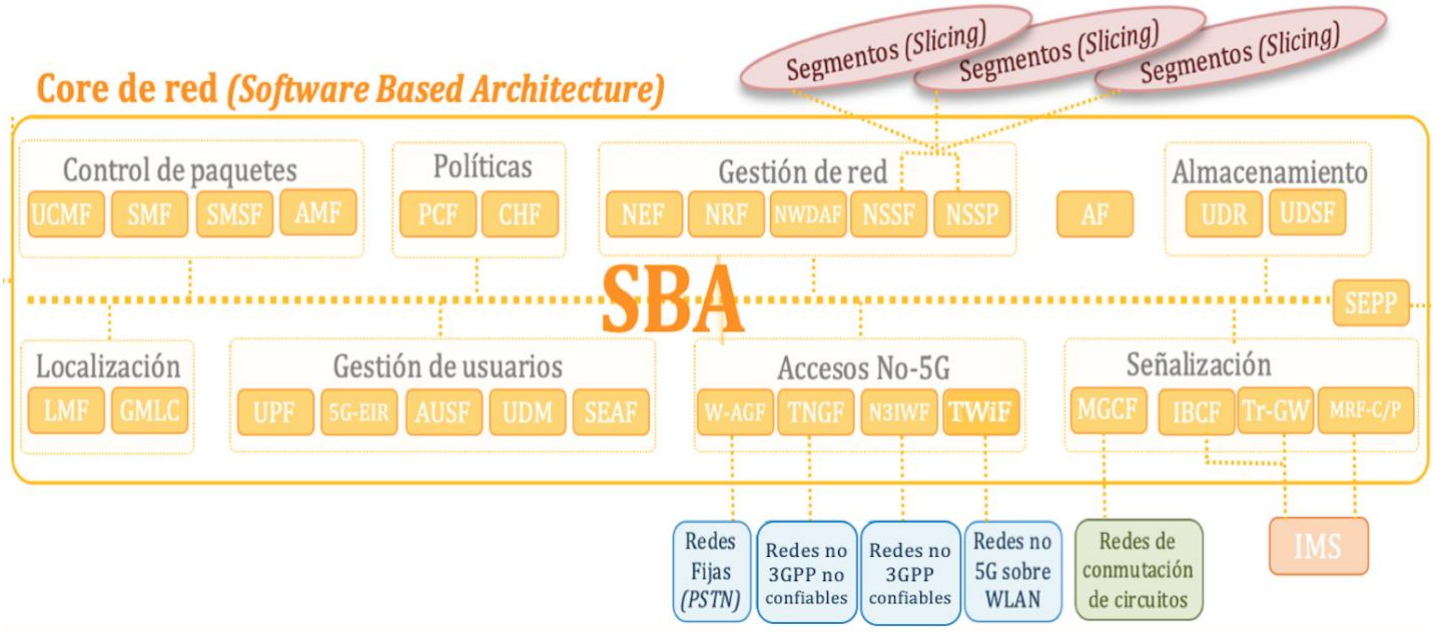
- Descripción
- Funciones de red (NF)
- Security Edge Protection Proxy (SEPP)
- Empleo de Cloud



Descripción.

La red central (core de red) de 5G se basa en un nuevo modelo arquitectónico, llamado **SBA** (Service Based Architecture). Es esencialmente un marco en el que la funcionalidad del plano de control de la red 5G y los repositorios de datos se implementan mediante un conjunto de funciones de red (**NF**: Network Functions) interconectadas.

A continuación se presenta una imagen que contiene únicamente el SBA:



Funciones de red (NF).

Las funciones básicas que ofrece SBA son:

- **AF** (Application Function); Funciones generales o específicas para las aplicaciones.
- **AMF** (Access Management Function): gestiona el registro de UE, el contexto de señalización de NAS, la gestión de movilidad de UE, p. rastrea la ubicación del UE y proporciona eventos de movilidad a otras NF. La funcionalidad del AMF se parece a la del 4G MME.
- **AUSF** (Authentication Server Function): Servidor que atiende las funciones de Autenticación.
- **GMLC** (Gateway Mobile Location Center): admite servicios basados en la ubicación. También existe en 4G.
- **IBCF** (Interconnect Border Control Function): Función basada en SIP, controla la parte de estado de la llamada que pertenece al control de conexión para las redes fijas con VoIP.

- **NEF** (Network Exposure Function): proporciona un puente hacia las verticales para acceso a los datos y funcionalidades del núcleo 5G. Expone datos a terceros, asigna identificadores y convierte protocolos. El NEF puede verse como una evolución de la función de exposición de **SCEF** (Service Capabilities Exposure Function) para servir a una gama más amplia de verticales.
- **PCF** (Policy Control Function): gestión de políticas para suscriptores y, en el futuro, también para segmentos. Esto incluye la selección de rutas de tráfico, reenvío de tráfico, políticas de itinerancia, tarifas y políticas de calidad de servicio (QoS). Este nodo corresponde a la función de reglas de política y cargo (PCRF) en 4G.
- **N3IWF** (Non-3GPP Interworking Function): responsable del interfuncionamiento entre redes no-3GPP que no confiables y el SBA.
- **NRF** (Network Repository Function): admite el descubrimiento de servicios, la autorización del consumidor de NF y mantiene los perfiles de NF, los servicios y la lista de instancias de NF. Actúa como el servidor de autorización OAuth 2.0. Esta es una nueva entidad en 5G.
- (**NSSF**: Network Slice Selection Function): función que ayuda en la selección de instancias de segmento de red adecuadas para los usuarios y en la asignación de las funciones de gestión de acceso (**AMF**) necesarias
- **SEAF** (Security Anchor Functionality): Funcionalidad de anlcaje de claves.
- **SEPP** (Security Edge Protection Proxy): negocia y protege las conexiones con redes externas. Analiza mensajes y previene ataques. Esta es una entidad nueva en 5G, pero existen firewalls para generaciones de redes anteriores.
- **SMF** (Session Management Function): Realiza el establecimiento, modificación y liberación de sesiones. La asignación de la dirección IP y la gestión de la UE hace que la recopilación de datos de carga, la dirección del tráfico y el enrutamiento en la UPF. El SMF corresponde a la parte del plano de control del 4G PGW.
- **TNGF** (Trusted WLAN Gateway Function):
- **Tr-GW** (Transition Gateway): Proporciona funciones como traducción de dirección/puerto de red y traducción de protocolo Ipv4/IPv6. Tr-GW también se conoce como Network-SBG (N-SBG).
- **UDM** (Unified Data Management): admite el acceso al almacenamiento de datos, p. Ej. para la gestión de suscripción (incluido el acceso a datos de suscripción en UDR), autorización de acceso y servicio, almacenamiento y gestión de identificación de usuario, autenticación de usuario. El UDM en 5G corresponde al 4G HSS.
- **UDR** (Unified Data Repository): admite el almacenamiento y la recuperación de datos de políticas, datos de suscripción y datos para la exposición a verticales a través de NEF. El UDR corresponde al 4G-UDR o al HLR, dependiendo de la implementación real del frontend de la base de datos.
- **UPF** (User Plane Function): proporciona el punto de sesión de la PDU externa de interconexión a las redes de datos. Realiza inspección de paquetes y aplicación de políticas y reglas de QoS para el plano del usuario. La UPF corresponde a la parte del plano de usuario del 4G PGW.
- **UCMF** (UE (radio) Capability Management Function)

SBA se basa en funcionalidades de entidades de red que se convierten en servicios expuestos y ofrecidos a otras entidades de red. Estas funciones de red exponen su funcionalidad a través de interfaces basadas en servicios (**SBI**: Service Based Interfaces) a través de un bus de mensajes SBI que implementa **API RESTful** sobre **HTTP/2**. El marco de la **API REST** (Representational State Transfer) es un enfoque bien conocido y comúnmente utilizado por entidades externas en la industria de las telecomunicaciones, por ejemplo por proveedores de servicios web como Amazon.

Esencialmente, todas las NF pueden comunicarse entre sí mediante una solicitud/respuesta o interacciones de suscripción/notificación entre los consumidores y productores de servicios de NF. Desde el punto de vista de la seguridad, dicha comunicación requiere la protección de la confidencialidad y la integridad de los mensajes intercambiados, así como un fuerte mecanismo de autenticación y autorización.

En las especificaciones de seguridad 3GPP (TS 33.501), los requisitos para la seguridad del core de red se definen en la cláusula 5.9. En la sección 13 de la especificación técnica se proporciona una descripción más detallada de los procedimientos y aspectos de seguridad y se hace referencia a ellos en las secciones siguientes.

Otro documento de especificación que es importante es **TS 33.122**, que define los aspectos de seguridad del marco de API común (**CAPIF**: common API framework) para las API de 3GPP. CAPIF se introduce con el propósito de estandarizar la funcionalidad expuesta a través de las API. Esta especificación define varios requisitos de seguridad comunes, relacionados principalmente con la autenticación y autorización, pero también relacionados con el ocultamiento de topología.

Figure 12: Secure communication between network functions in 5G core SBA (simplified scheme)

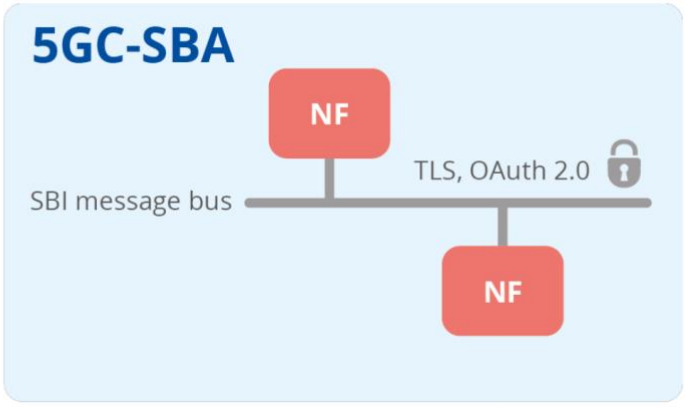


Imagen tomada de: ENISA Report - Security in 5G Specifications.pdf

Security Edge Protection Proxy (SEPP)

En el modelo de arquitectura de seguridad 5G, se introduce un nuevo elemento de arquitectura: Security Edge Protection Proxy (**SEPP**). **SEPP** actúa como puerta de enlace de seguridad en las interconexiones entre la "home network" y las redes visitadas.

Las funciones admitidas por los SEPP incluyen autenticación de extremo a extremo, protección de integridad y confidencialidad mediante firmas y cifrado de todos los mensajes de roaming HTTP/2; y mecanismos de gestión de claves para establecer las claves

criptográficas necesarias y realizar los procedimientos de negociación de la capacidad de seguridad. Los SEPP también son compatibles con la prevención de ataques y también proporcionan ocultación de topología.

Figure 14: Secure communication between two SEPPs (simplified scheme)

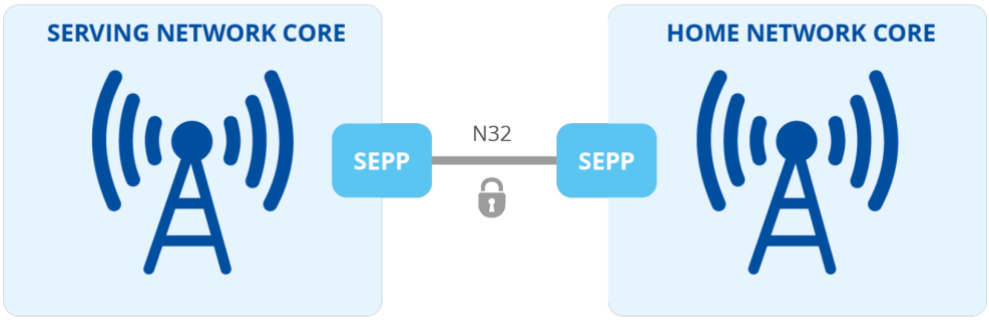
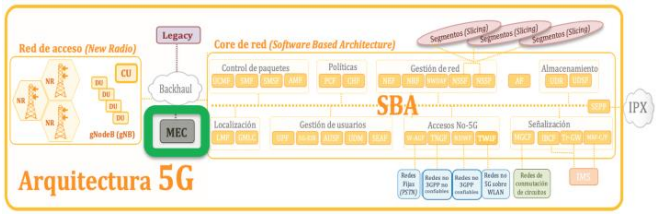


Imagen tomada de: ENISA Report - Security in 5G Specifications.pdf

2. MEC (Multi-access Edge Computing).



MEC ofrece a:

- Desarrolladores de aplicaciones y
- Proveedores de contenido

Capacidades de computación en la nube y un entorno de servicios de TI en el borde de la red. Este entorno se caracteriza por una latencia ultra baja y un gran ancho de banda, así como por el acceso en tiempo real a la información de la red de radio que las aplicaciones pueden aprovechar.

Los operadores pueden abrir su borde de Red de Acceso de Radio (**RAN**: Radio Access Network) a terceros autorizados, lo que les permite implementar de manera flexible y rápida aplicaciones y servicios innovadores para suscriptores móviles, empresas y segmentos verticales.

MEC es un desarrollo natural en la evolución de las estaciones base móviles y la convergencia de las redes de telecomunicaciones y TI. Permitirá nuevos segmentos comerciales verticales y servicios para consumidores y clientes empresariales. Los casos de uso incluyen:

- Análisis de video
- Servicios de localización
- Internet de las cosas (IoT)
- Realidad aumentada
- Distribución optimizada de contenido local y
- Almacenamiento en caché de datos

Permite de forma exclusiva que las aplicaciones de software aprovechen el contenido local y la información en tiempo real sobre las condiciones de la red de acceso local. Al implementar varios servicios y almacenar en caché el contenido en el borde de la red, las redes centrales móviles se alivian de una mayor congestión y pueden servir de manera eficiente a los propósitos locales.

Los estándares de la industria MEC y el despliegue de plataformas MEC actuarán como habilitadores de nuevas fuentes de ingresos para operadores, proveedores y terceros. La diferenciación se producirá a través de las aplicaciones únicas implementadas en Edge Cloud.

Una imagen bastante clara es la que nos presenta el documento: **Mobile Edge Computing - A key technology towards 5G**, First edition – September 2015 de ETSI. (https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf).

En el mismo presenta los impulsos del mercado que genera esta tecnología.

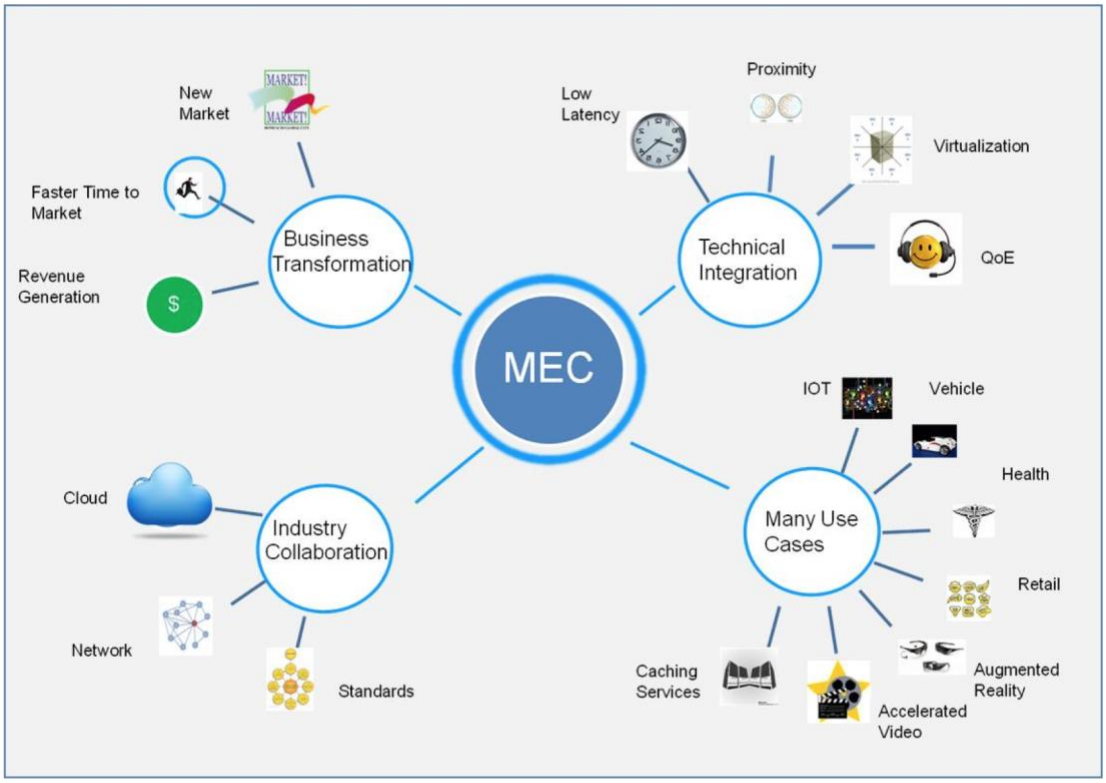


Figure 1: MEC market drivers

Imagen tomada de Mobile Edge Computing - A key technology towards 5G de ETSI

Analicemos a continuación el documento "**Multi-access Edge Computing (MEC); Framework and Reference Architecture**" de ETSI - GS MEC 003 V2.2.1 (2020-12).

MEC permite la implementación de aplicaciones como entidades únicamente de software que se ejecutan al más alto nivel de una infraestructura de virtualización, las cuáles se encuentran en, o cerca, del borde de la red. MEC está constituido por una serie de **entidades** generales involucradas que se pueden agrupar en entidades de:

MEC permite la implementación de aplicaciones como **entidades** únicamente de software

- nivel de sistema.
- nivel de host y,
- nivel de red.

Analicemos la figura que sigue:

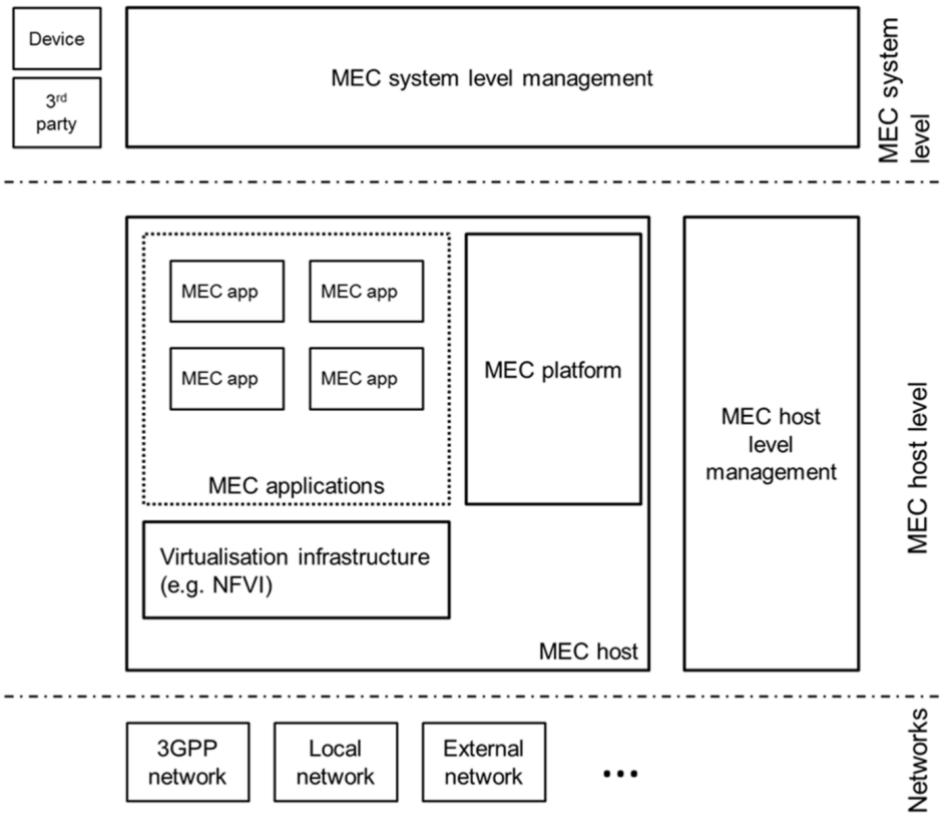


Figure 5-1: Multi-access Edge Computing framework

Imagen tomada de ETSI GS MEC 003 V2.2.1

La Figura 5-1, ilustra cómo MEC consta de las siguientes entidades o niveles:

- Nivel (entidad) de Sistemas.

  Compuesto por dispositivos propios, de 3ªs partes y su subnivel de gestión.

- Nivel (entidad) de host.

  Compuesto por:

  - Plataformas
  - Aplicaciones
  - Infraestructura de virtualización
  - Subnivel de gestión

- Nivel (entidad) de red.

  Compuesto por las redes que lo conforman. En la figura pone como ejemplo, redes 3GPP, LAN, externas, etc.

El nivel de host en MEC, es una entidad que contiene una plataforma MEC y una infraestructura de virtualización que proporciona recursos informáticos, de almacenamiento

y de red, con el fin de ejecutar aplicaciones MEC. El host MEC se describe con más detalle en la cláusula 7.1.1.

La plataforma MEC es la colección de funciones esenciales necesarias para ejecutar aplicaciones MEC en una infraestructura de virtualización particular y permitirles proporcionar y consumir servicios MEC. La plataforma MEC también puede proporcionar servicios. La plataforma MEC se describe con más detalle en la cláusula 7.1.2.

Las aplicaciones MEC se instancian en la infraestructura de virtualización del host MEC según la configuración o las solicitudes validadas por la administración de MEC. Las aplicaciones MEC se describen con más detalle en la cláusula 7.1.3.

El punto 8 "servicios MEC" de este mismo estándar de ETSI presenta lo siguiente:

8.2 Información de la red de radio.

El servicio de información de la red de radio, cuando está disponible, proporciona a las aplicaciones autorizadas información relacionada con la red de radio.

Expone información a aplicaciones, tales como:

- información apropiada y actualizada de la red de radio sobre las condiciones de la misma;
- información de medición y estadística relacionada con el plano de usuario;
- información (por ejemplo, portadores de acceso de radio y contexto de UE) relacionada con los UE servidos por el nodo o los nodos de radio asociados con el host MEC;
- cambios en la información relacionada con los UE servidos por los nodos de radio asociados con el host MEC.

La información de la red de radio se proporciona con la granularidad necesaria (por ejemplo, por equipo de usuario (UE) o por celda, por período de tiempo).

8.3 Ubicación.

El servicio de ubicación, cuando está disponible, proporciona a las aplicaciones autorizadas información relacionada con la ubicación. Expone información a aplicaciones, tales como:

- la ubicación de los UE específicos servidos actualmente por el (los) nodo (s) de radio asociados con el anfitrión MEC;
- información acerca de la ubicación de todos los UE actualmente servidos por el (los) nodo (s) de radio asociados con el host MEC;
- opcionalmente, información acerca de la ubicación de una determinada categoría de UE actualmente atendidos por los nodos de radio asociados con el anfitrión MEC;
- una lista de UE en una ubicación particular;
- información sobre la ubicación de todos los nodos de radio actualmente asociados con el host MEC.

NOTA: La ubicación puede ser geolocalización, ID de celda, etc.

8.4 Servicios de gestión de tráfico.

Se admiten los siguientes servicios de gestión de tráfico opcionales:

- Servicio de gestión de ancho de banda (**BWM**: BandWidth Management).

  El servicio BandWidth Management (**BWM**), cuando está disponible, permite la asignación de ancho de banda a cierto tráfico enrutado hacia y desde aplicaciones MEC y la priorización de cierto tráfico.

- Servicio de dirección de tráfico de acceso múltiple (**MTS**: Multi-access Traffic Steering).

  El servicio de dirección de tráfico de acceso múltiple (**MTS**), cuando está disponible, permite dirigir, dividir o duplicar sin problemas el tráfico de datos de aplicaciones a través de conexiones de red de acceso múltiple.

Otro documento sobre MEC que también debemos tener en cuenta es: **ETSI White Paper No. 28: "MEC in 5G networks**" - First edition – June 2018.

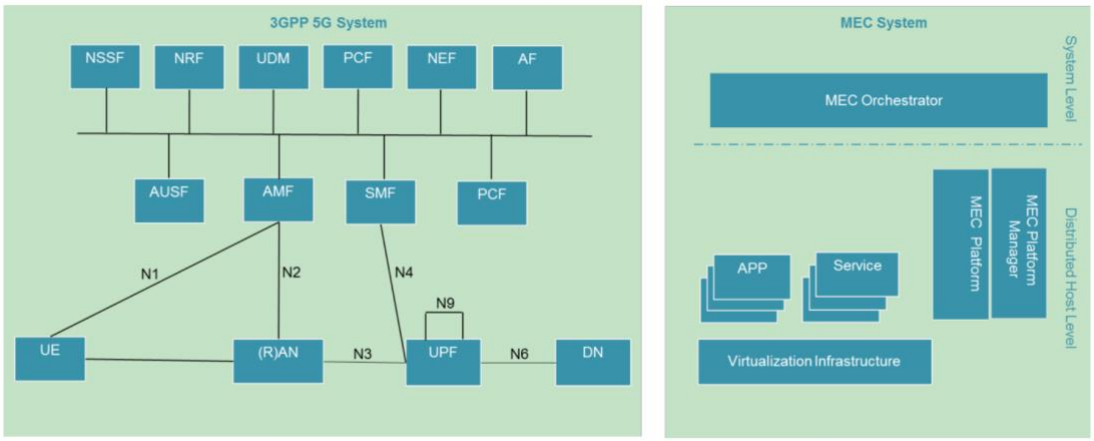


Figure 1. 5G Service-Based Architecture and a generic MEC system architecture
Imagen tomada de ETSI White Paper No. 28: "MEC in 5G network

Las funciones de red y los servicios que producen se registran en una Función de Recursos de Red (**NRF**: Network Repository Function) mientras que en MEC los servicios producidos por las aplicaciones MEC se registran en el registro de servicios de la plataforma MEC.

Además de **AF** (Application Function), NEF y NRF, hay otras funciones que vale la pena introducir. Los procedimientos relacionados con la autenticación son atendidos por la función del servidor de autenticación (**AUSF**: Authentication Server Function).

La siguiente figura muestra cómo se implementa el sistema MEC de manera integrada en la red 5G.

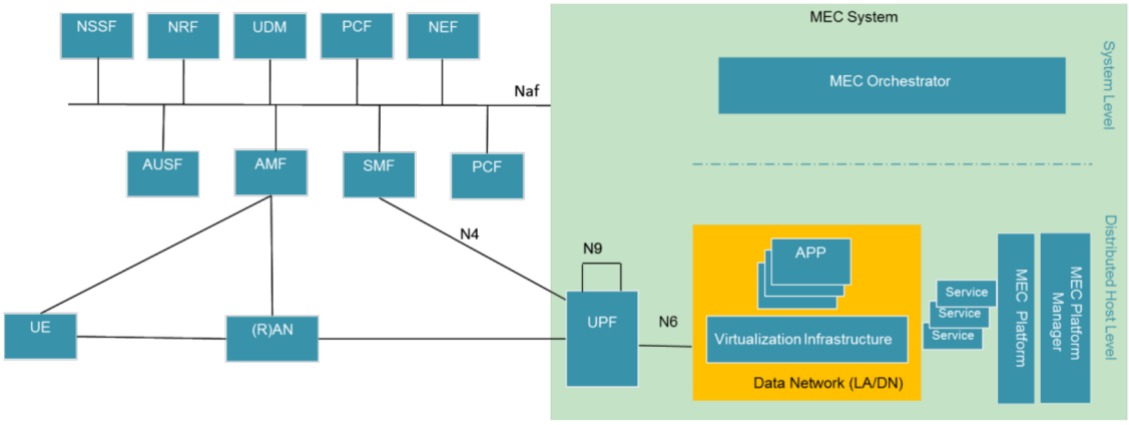


Figure 2. Integrated MEC deployment in 5G network

Imagen tomada de ETSI White Paper No. 28: "MEC in 5G network

En el sistema MEC en el lado derecho de la Figura 2, el orquestador MEC (MEC orchestrator o **MEO**) es una entidad funcional a nivel del sistema MEC que, actuando como un **AF**, puede interactuar con la función de exposición de red (**NEF**), o en algunos escenarios directamente con el 5G NF objetivo. En el nivel de host MEC, es la plataforma MEC la que puede interactuar con estos NF 5G, nuevamente en el papel de un AF. El host MEC, es decir, las entidades funcionales a nivel de host, se implementan con mayor frecuencia en una red de datos en el sistema 5G. Mientras que NEF es una función del core de 5G (SBA), también se puede implementar una instancia de NEF en el borde para permitir el acceso al servicio de baja latencia y alto rendimiento desde un host MEC.

De los documentos de ETSI, vamos a cerrar con una imagen del **GR MEC 031 V2.1.1** (2020-10) **Multi-access Edge Computing (MEC) MEC 5G Integration**.

La imagen que sigue, representa un caso de flujo entre MEC de dos operadores diferentes y se ha incorporado a este texto con la intención de poner de manifiesto las funciones y su flujo de comunicación.

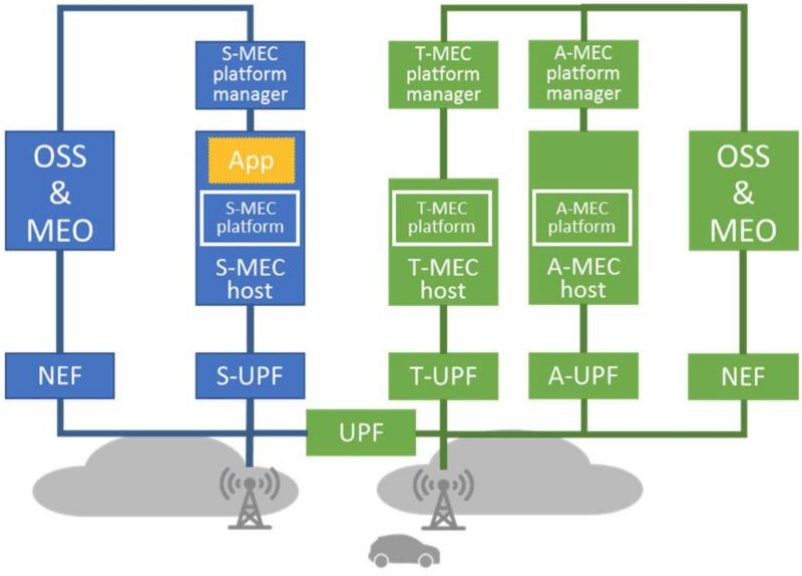


Figure 5.1.2.3-1: Function blocks in inter-operator case

Imagen tomada de ETSI GR MEC 031 V2.1.1

Otro documento que es muy representativo en cuanto a los posibles escenarios de MEC es: **Mobile Edge Computing - A key technology towards 5G** - First edition, September 2015, también de ETSI.
https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

En el mismo nos presenta los siguientes ejemplos:

Augmented Reality

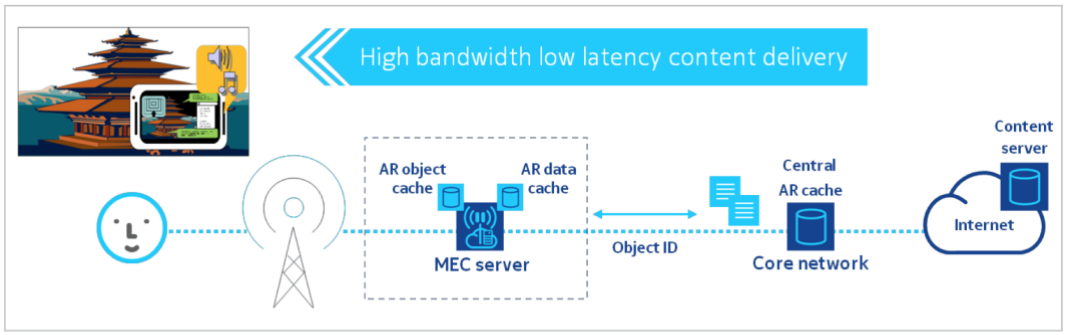


Figure 3: Augmented Reality Service Scenario
Imagen tomada de ETSI Mobile Edge Computing - A key technology towards 5G

Intelligent Video Acceleration

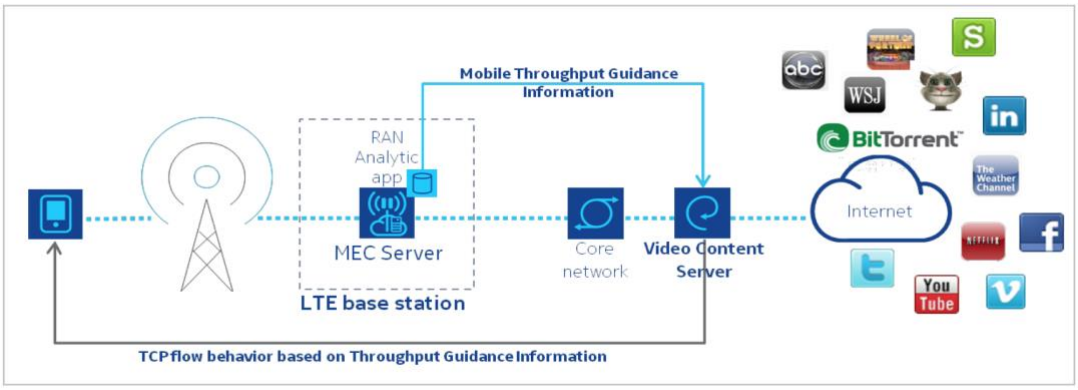


Figure 4: Intelligent Video Acceleration Service Scenario
Imagen tomada de ETSI Mobile Edge Computing - A key technology towards 5G

Connected Cars

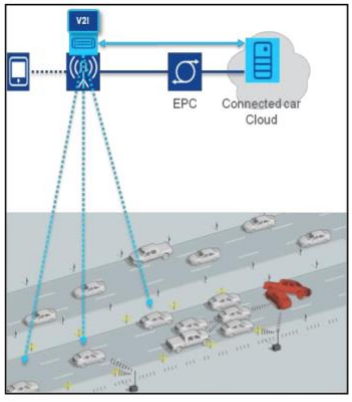


Imagen tomada de ETSI Mobile Edge Computing - A key technology towards 5G

Figure 5: Connected Vehicles Service Scenario

Internet of Things Gateway

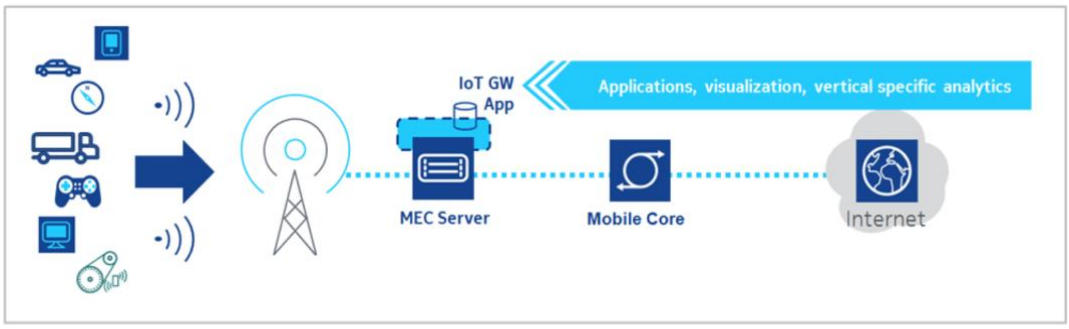
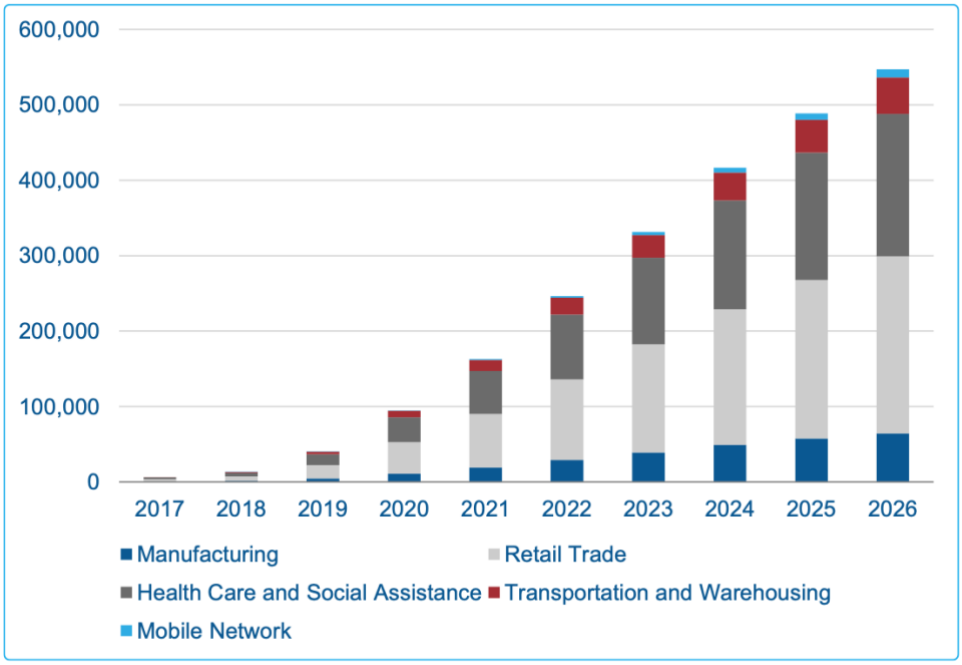


Figure 6: IoT Gateway Service Scenario

Imagen tomada de ETSI Mobile Edge Computing - A key technology towards 5G

Finalmente un dato que es de interés es la siguiente gráfica publicada en el artículo: https://www.intel.es/content/www/es/es/communications/multi-access-edge-computing-brief.html en el que se puede ver la situación actual y futura de instalaciones MEC en el Oeste de Europa.

Figure 6: Western Europe MEC Installations

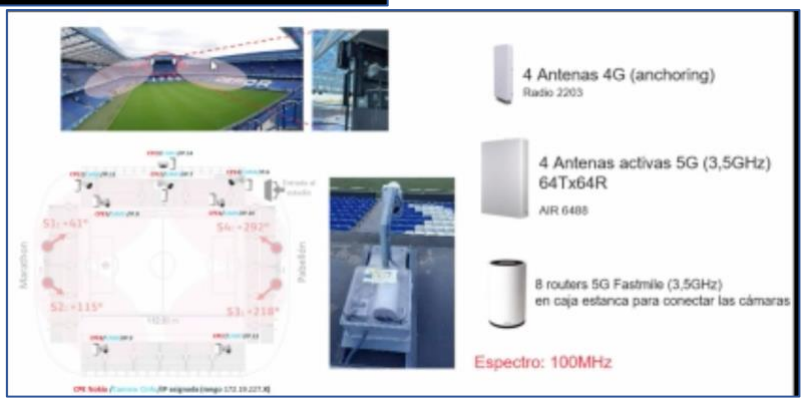


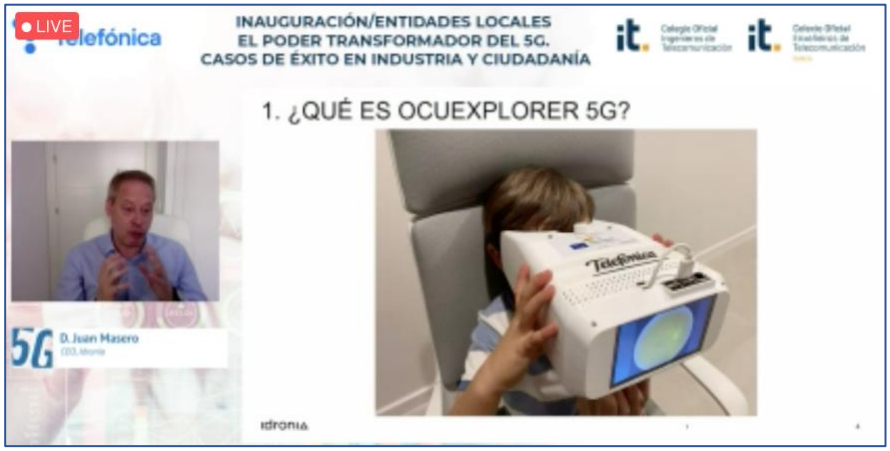
Source: iGR, 2017

Imagen tomada de https://www.intel.es/content/www/es/es/communications/multi-access-edge-computing-brief.html

El día 15 de junio de 2021, el **COIT** (Colegio Oficial de Ingenieros en Telecomunicaciones) realizó un Webinar con el título: "**EL PODER TRANSFORMADOR DEL 5G. CASOS DE ÉXITO EN INDUSTRIA Y CIUDADANÍA**", en el mismo participaron varias empresas y organizaciones y se presentaron casos de implantación de MEC con la participación de **Telefónica de España**, algunos de ellos fueron:

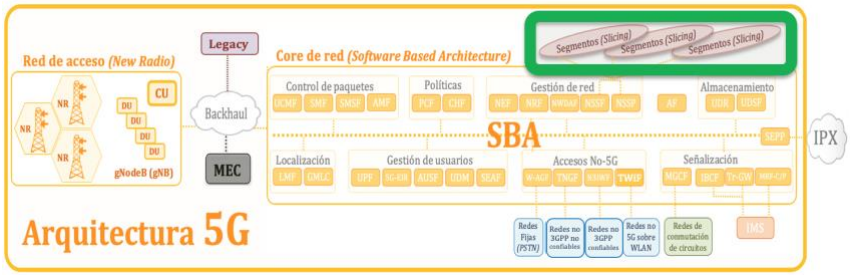

tiivii
New life for live Sports
cinfo
Despliegue de cámaras: 8 HD/4K
Cubierta: 1 cámara panorámica semiesférica para toma "beauty": planos superiores de los jugadores, marcadores, ...
Nivel 2:
2 cámaras 4K "bullet" en los extremos para predecir el juego.
1 cámara PTZ 4K para zoom y coordenadas del juego.
Nivel 1:
4 cámaras PTZ 4K ubicadas en las esquinas del estadio, capaces de enfocar a cualquier butaca del graderío.


4 Antenas 4G (anchoring)
Radio 2203
4 Antenas activas 5G (3,5GHz) 64Tx64R
AIR 6488
8 routers 5G Fastmile (3,5GHz) en caja estanca para conectar las cámaras
Espectro: 100MHz


LIVE
Telefónica
INAUGURACIÓN/ENTIDADES LOCALES
EL PODER TRANSFORMADOR DEL 5G.
CASOS DE ÉXITO EN INDUSTRIA Y CIUDADANÍA
1. ¿QUÉ ES OCUEXPLORER 5G?
D. Juan Masero
5G
idrona


Drones y 5G
5G, palanca para vuelos BVLOS
Baja latencia. Nos permite controlar el dron de forma instantánea desde cientos de kilómetros de distancia así como ver las imágenes de la cámara de pilotaje con retardo mínimo.
Alto ancho de banda. Especialmente en UpLink. Necesario para transmitir gran cantidad de datos en tiempo real, como por ejemplo, vídeo de alta calidad.
Conectividad. Las redes celulares permiten hacer vuelos de decenas de km sin perder la conexión habilitando los vuelo BVLOS
Edge computing. Procesado de datos en la red de Telefónica, sin pasar por Internet y con baja latencia. Descargar parte de la inteligencia del dron en la red por restricciones de consumo y peso. Analítica y servicios
Seguridad y fiabilidad. Redes cifradas y libres de interferencias gracias al uso de la SIM y del espectro licenciado de la tecnología 5G.
D. Ángel Alves
Innovación
Telefónica España
5G

3. Slicing (Segmentos)



En el presente documento, traduciremos "**Slice**" como "**Segmento**", pero también se interpreta como: rodaja, rebanada, corte, etc.

Temas a desarrollar en esta sección.

- **mMTC**: massive Machine Type Communication - *IoT*
- **eMBB**: enhanced Mobile Broadband (eMBB) - *Eventos*
- **URLLC:** Ultra-Reliable Low Latency Communications - *Salud*
- **V2X:** Vehicle to X - *Vehículos autónomos*.
- Empleo e implantación de plantillas **GST** (Generic network Slice Template)

Una de las características de la tecnología 5G es la posibilidad de "segregar" la red en varias sub-redes que pueden ser administradas de forma independiente, lo cual es conocido como "**network slicing**", en este texto lo denominaremos como "Segmentos" pero es posible que en otras publicaciones lo encontremos como "cortes, rodajas, tajadas, niveles, etc.".

Teniendo como base la modularidad de las funciones de red y su virtualización, es posible dividir y aislar la red en distintas instancias o funciones lógicas, con distintas prestaciones y rendimiento, compartiendo la misma infraestructura física. Esto permitirá adaptarse a los distintos requisitos de servicios de una forma muy rápida y eficiente, reduciendo riesgos y costes. Por ejemplo, para habilitar el coche conectado es necesaria una latencia muy baja y requiere alta redundancia; sin embargo, para ofrecer banda ancha de alta velocidad a ordenadores portátiles, el ancho de banda es un aspecto más importante.

Gracias a "network slicing", 5GC permite ofrecer una gran variedad de aplicaciones IoT, tanto por parte del operador, como por sus socios industriales (empresas de seguridad, energéticas, logísticas, salud, industrias, etc.). Los "partners" son responsables de la aplicación, los dispositivos y la gestión de identidad, y la operadora es la responsable de la infraestructura física, incluyendo generalmente centros de datos, transporte y funciones de red. La gestión del segmento (slide) puede ser compartida entre los dos, permitiendo al socio (dentro de un acuerdo de SLA) manejar las capacidades de las funciones de red que soportan la aplicación, tal y como la gestión de la movilidad local.

Las nuevas funcionalidades técnicas inherentes a las redes 5G (enrutamiento y direccionamiento del tráfico a las aplicaciones en la red de datos local en el **UPF**; la posibilidad de un **AF** de influenciar en el enrutamiento del tráfico directamente mediante el **PCF** o indirectamente mediante el **NEF** dependiendo de las políticas del operador; etc.), facilitarán también el despliegue de **MEC** (Multi-access Edge Computing) que se verá en el siguiente punto.

3GPP actualmente define en el **TS 23.501** los siguientes cuatro tipos de tipos de segmentos de red, según sus características de calidad de servicio:

1) Comunicación masiva de tipo de máquina (**mMTC**: massive Machine Type Communication) - **TR_22.861.**

2) banda ancha móvil mejorada (**eMBB**: enhanced Mobile Broadband) – **TR_22.863**.

3) Comunicaciones de baja latencia ultra fiables (**URLLC**: Ultra-Reliable Low Latency Communications) - **TR_22.862.**

4) Vehículo a X (**V2X**: Vehicle to X)

Escenarios de caso de uso específico:

- mMTC está diseñado para cubrir segmentos que dan servicio a grandes cantidades de dispositivos de Internet de las cosas (IoT).
- eMBB tiene la intención de servir casos de uso de entretenimiento. Un ejemplo típico sería la transmisión de eventos.
- URLLC puede proporcionar redes de misión crítica o aplicaciones de salud con un segmento adecuado.
- V2X se enfoca en autos conectados y autónomos.

Cada instancia de segmento se identifica en el núcleo (core) 5G, el 5G RAN y en el equipo de usuario (**UE**) mediante una identidad de segmento que se denomina Información de asistencia para la selección de segmento de red única (**S-NSSAI**: Single-Network Slice Selection Assistance Information) en TS 23.501. Este identificador tiene dos partes:

- Slice Service Type (**SST**) es un valor predefinido para eMBB o mMTC, etc. (8bits)
- Slice Differentiator (**SD**) es un valor específico de MNO opcional para diferenciar entre segmentos del mismo tipo (24 bits)

Un MNO puede ofrecer el mismo tipo de segmento a diferentes verticales, por ejemplo, eMBB para diferentes proveedores de transmisión o mMTC para diferentes proveedores de servicios de IoT. El MNO puede elegir, si quiere, poblar el SD y qué valor poner allí. Tenga en cuenta que el MNO también puede usar S-NSSAI no estándar si así lo desea, como usar su propio valor de SST no definido por 3GPP, o un SST y SD autodefinidos y específicos de MNO.

Dentro de la red central, el **S-NSSAI** se utiliza para la diferenciación del tráfico y los aspectos de QoS, pero también para la autorización, la aplicación de políticas y potencialmente para el enrutamiento. Como un UE puede pertenecer a varios segmentos, se introdujo el concepto de grupo o lista de segmentos, y esto se denomina (algo confuso) Información de asistencia para la selección de segmentos de red (NSSAI). Hay diferentes categorías de NSSAI. Las categorías típicas que se utilizan son NSSAI permitida, NSSAI rechazada, NSSAI configurada o una NSSAI solicitada.

Empleo e implantación de plantillas **GST** (Generic network Slice Template):

El Grupo de Red de GSMA (NG) especificó la Plantilla de Segmento Genérica (**GST**: Generic Slice Template) en su especificación NG.116. El GST es un conjunto de características para un tipo de segmento o servicio. Es un conjunto genérico de atributos obligatorios y

opcionales. Esos atributos están relacionados con el rendimiento, la tolerancia al retardo, el espectro de radio, etc. NG.116 v2.0 también contiene los siguientes atributos relacionados con la seguridad, que se centran principalmente en el aislamiento físico y lógico/virtual. NG.116 divide el aislamiento en los siguientes 2 tipos principales:

Aislamiento físico

- Aislamiento de procesos y subprocesos
- Aislamiento de la memoria física
- Aislamiento de la red física

Aislamiento lógico

- Aislamiento de recursos virtuales: un segmento de red tiene acceso a un rango específico de recursos que no se superpongan con otros segmentos de la red (por ejemplo, aislamiento de la máquina virtual)
- Aislamiento de red: la función de red está dedicada al segmento y al cliente vertical, pero los recursos virtuales son compartidos.
- Aislamiento de inquilinos/servicios: los datos verticales del cliente están aislados de otros verticales, pero son virtuales los recursos y las funciones de la red son compartidos.

GST (Generic network Slice Template): conjunto de atributos que pueden caracterizar un tipo de segmento/ servicio de red, genérico y no vinculado a ninguna implementación de red específica.

NEST (NEtwork Slice Type): **GST** lleno de valores (es decir una plantilla ya completada y específica de un segmento en particular).

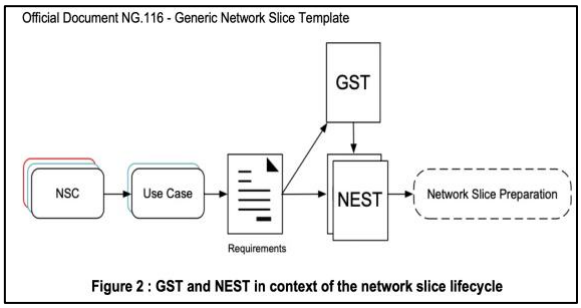


Figure 2 : GST and NEST in context of the network slice lifecycle

NOTA: Especial atención a cómo la MNO trata el nivel de aislamiento. El documento NG.116 propone las siguientes gráficas:

Official Document NG.116 - Generic Network Slice Template

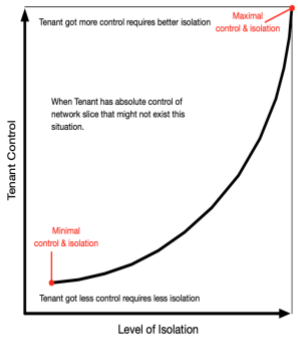


Figure 3 Relation between Tenant Control and Isolation

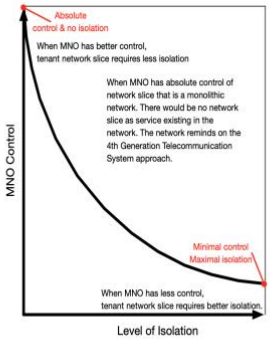


Figure 4 Relation between MNO Control and Isolation