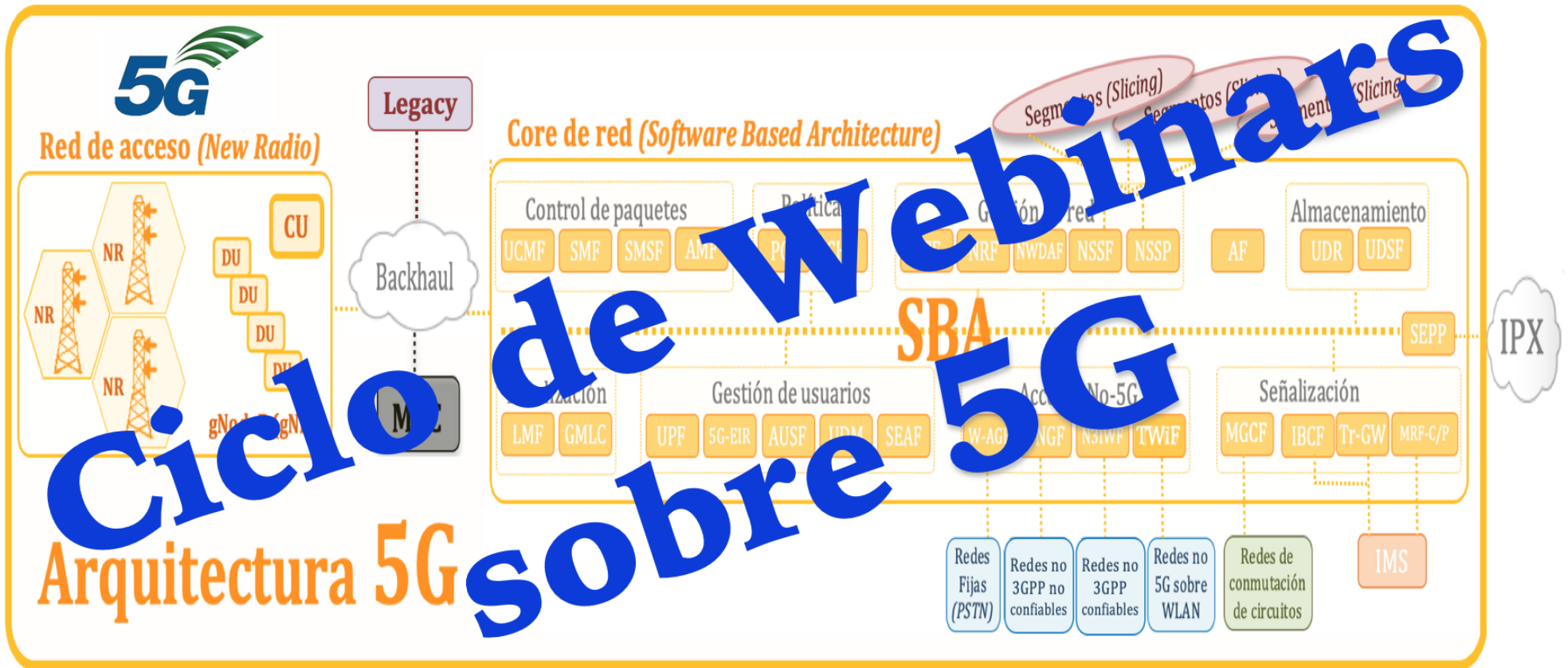


# Tema 2: New radio y gNodeB



**Alejandro Corletti Estrada**

acorletti@darFe.es



[www.darFe.es](http://www.darFe.es)

# Ciclo de Webinars sobre 5G

## Tema 2: New radio y gNodeB



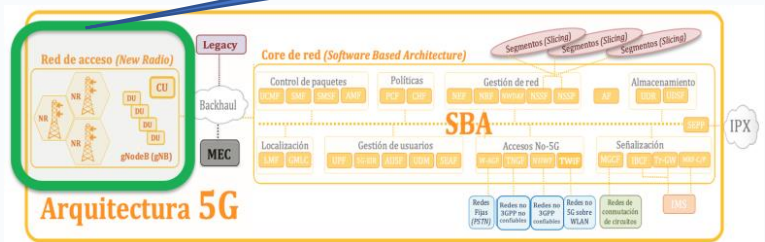
### DESARROLLO DEL CICLO DE WEBINARS

#### Webinar 1: Presentación y evolución de las tecnologías móviles

**Tema de hoy**

#### Webinar 2: New Radio y gNodeB

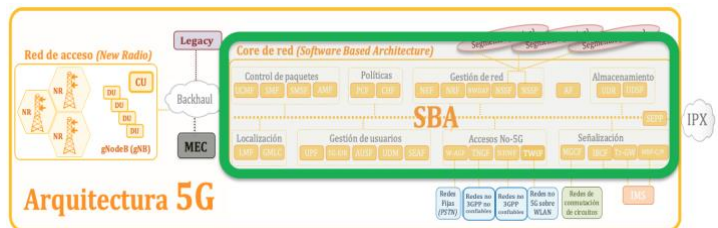
- Descripción de diseño de los gNB
- Open RAN
- Antenas compartidas (RAN Sharing)
- Frecuencias licitadas y asignadas
- Empleo de Cloud



#### Webinar 3: SBA, MEC y Slicing

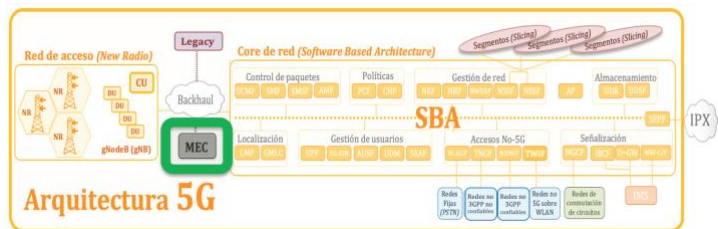
##### SBA (Core 5G) (Service Based Architecture)

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



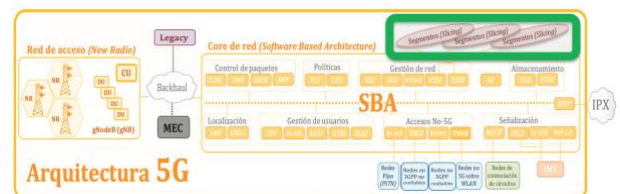
##### MEC (Multi-access Edge Computing)

- Empleo y detalle de MEC
- Análisis de contratos



##### Slicing (Segmentos)

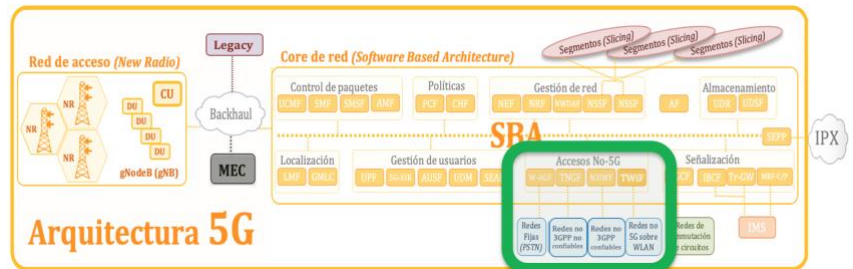
- **mMTC**: massive Machine Type Communication - *IoT*
- **eMBB**: enhanced Mobile Broadband (eMBB) - *Eventos*
- **URLLC**: Ultra-Reliable Low Latency Communications - *Salud*
- **V2X**: Vehicle to X - *Vehículos autónomos*.
- Plantillas GST (Generic network Slice Template)



## Webinar 4: Accesos y autenticación

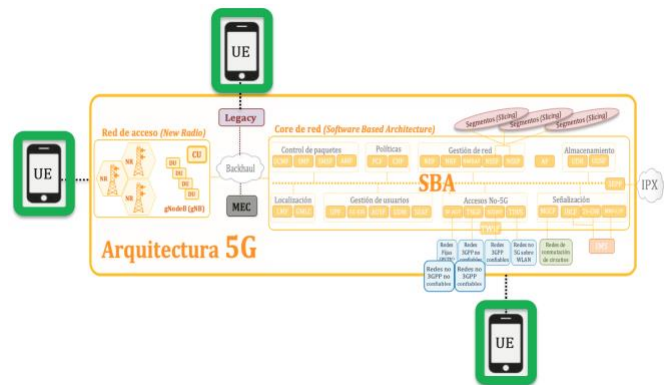
### Otros accesos

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



### Accesos UE (User Equipment)

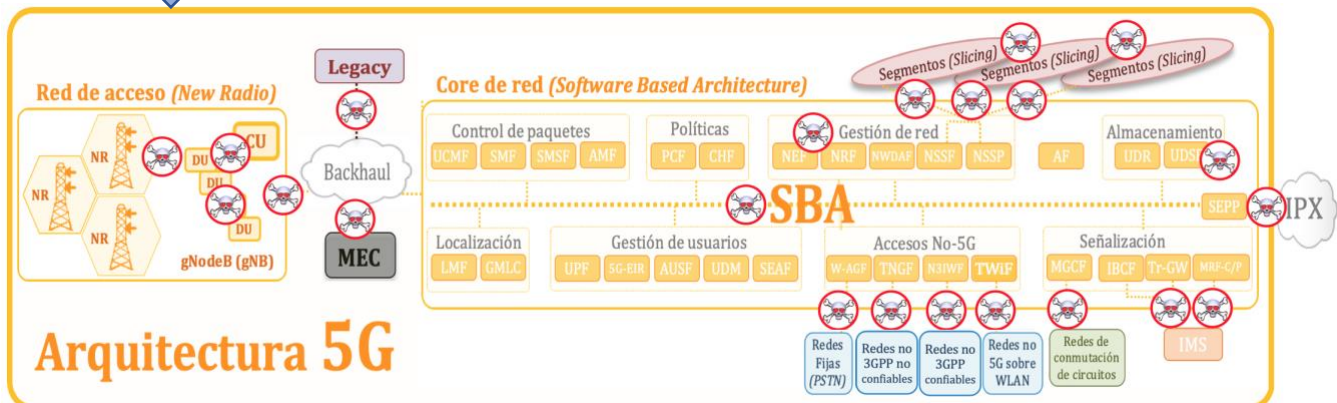
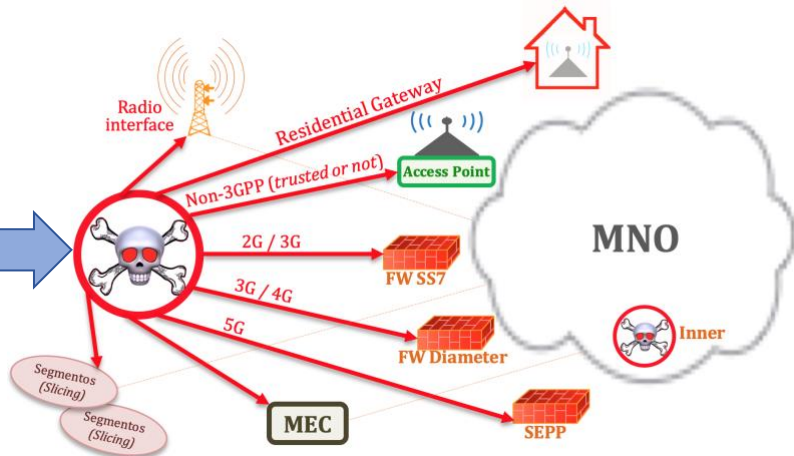
- a. UICC 4G heredado con aplicación USIM
- b. 4G UICC actualizado con la aplicación USIM
- c. 5G UICC con aplicación USIM



## Webinar 5: Seguridad en 5G

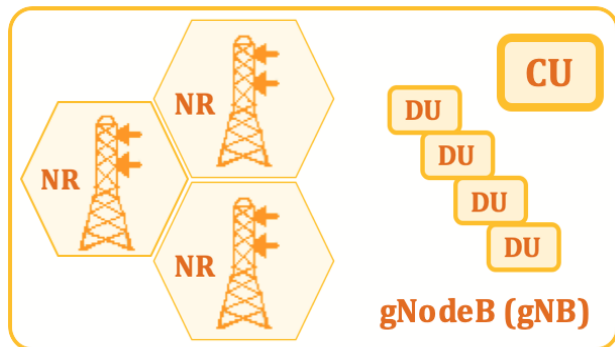
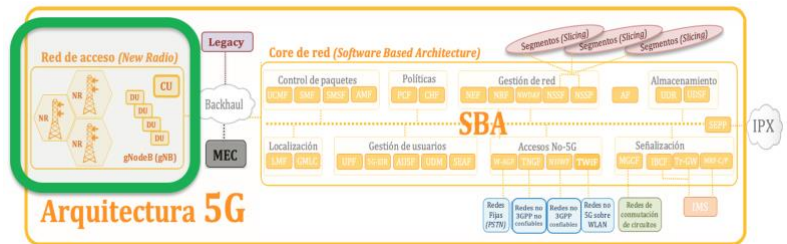
### Vectores de intrusión

### Puntos clave de seguridad en 5G



## New Radio y gNB

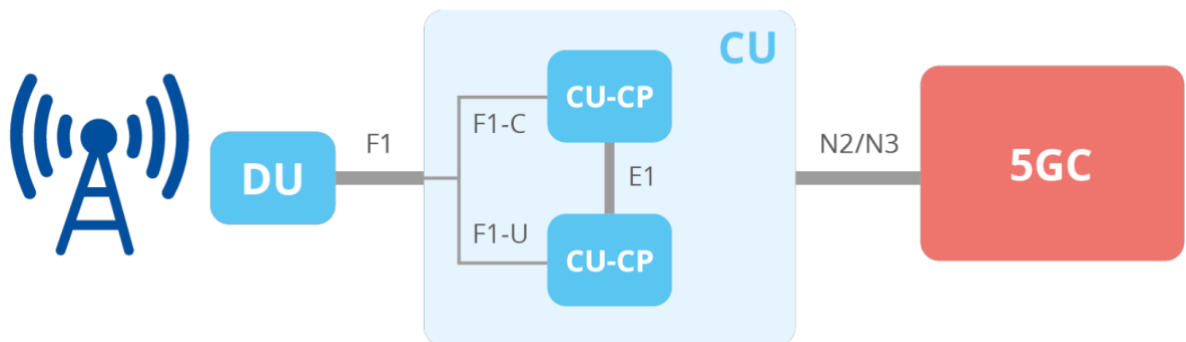
5G trae el concepto de **RAN** (Radio Access Network) dividido o desintegrado, donde el RAN se divide en: Unidades Distribuidas (**DU: Distributed Units**) y Unidades Centrales (**CU: Central Units**).



Por lo general, **DU** no tiene ningún acceso a las comunicaciones de los clientes y, por lo tanto, son adecuadas para su implementación en sitios no supervisados. **CU** realiza funciones de seguridad, finaliza la seguridad de **AS (Application Server)** y normalmente se implementa en sitios con acceso restringido al personal de mantenimiento. Juntos, DU y CU forman el gNB.

La comunicación entre DU y CU se establece mediante la interfaz **F1**. Además, las CU se comunican entre sí a través de la interfaz **E1**. El tráfico transmitido a través de estas interfaces puede transportar datos confidenciales y, por tanto, es un objetivo para los atacantes. Por lo tanto, la especificación exige confidencialidad, integridad y protección de respuesta para los datos del plano de control intercambiados a través de estas interfaces, aunque se dejan algunas opciones a los operadores, que analizaremos más adelante.

**Figure 11: Interfaces between components of the split RAN and 5G Core (simplified scheme)**



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

En las especificaciones de seguridad 3GPP (**TS 33.501: V17.1.0 "Security architecture and procedures for 5G system" (Release 17 - 2021-03)**), los requisitos para la protección de las interfaces internas de la estación base (**gNB**) que soportan la arquitectura dividida se establecen en la cláusula 5.3.9 y 5.3.10 y los mecanismos de seguridad adicionales se detallan en las Cláusulas 9.8.1 y sub-cláusula 9.8.2, para las interfaces F1 y E1. En ambos casos, el soporte de IPsec es obligatorio. Los requisitos de implementación concretos se proporcionan en la Cláusula 9.1, subcláusula 9.1.2, especificando que el protocolo IPsec ESP de acuerdo con RFC 4303 según lo perfilado por TS 33.210 (TS 33.210 V16.4.0 "Technical Specification Group Services and System Aspects; Network Domain Security (NDS); IP network layer security (Release 16 - (2020-07)) y la autenticación basada en certificados IKEv2 debe ser usado.

Con respecto a la protección de la interfaz **E1**, que se utiliza para señalar la transferencia de datos, el requisito simplemente establece que "la interfaz E1 entre CU-CP y CU-UP estará protegida por confidencialidad, integridad y anti réplica" sin enumerar explícitamente más comentarios o exclusiones.

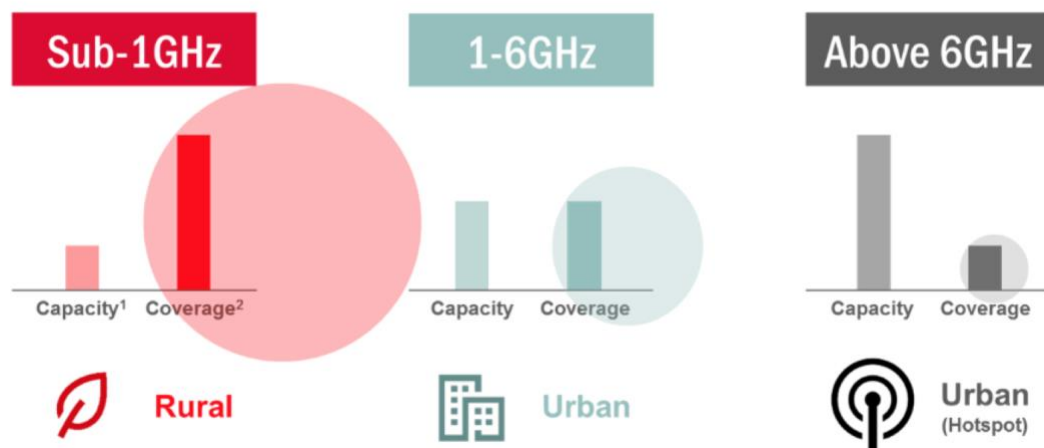
5G utiliza las frecuencias de **700 MHz, 800 MHz y 3,5 GHz**, apoyándose en las redes existentes de LTE. Progresivamente las bandas actuales se irán migrando a 5G y los despliegues se completarán con las bandas "milimétricas", **26 y 28 GHz**.

Las redes 5G operan en 3 bandas de frecuencias: **baja, media y alta**. Una red 5G estará constituida por hasta 3 tipos de celdas, cada una con un tipo de antena diferente. Estas antenas, proveerán diferentes relaciones entre velocidad de descarga vs distancias y área de servicio.

- La banda baja de 5G usa el mismo rango de frecuencia que un terminal 4G, es decir 600-850 MHz, garantizando una velocidad superior a la de 4G: 30-250 megabits por segundo(Mbit/s).
- La banda media de 5G (**Sub-6**), el nivel de servicio más utilizado, usa ondas de radio comprendidas entre los 2.5 y 3.7 GHz, permitiendo velocidades de 100-900 Mbits/s, en donde cada torre celular provee servicio a varios kilómetros de su radio.
- La banda alta de 5G (**mmWave**: millimeter wave), que es la que se espera utilizar en un futuro cercano, funciona con frecuencias comprendidas entre los **25** y los **39 GHz**, para así alcanzar velocidades de descarga en el rango de los gigabit por segundo (Gbit/s), que es una cantidad comparable a la que alcanza el Internet por cable.

El inconveniente de esta banda, es su límite, rango que hace que se requieran muchas más celdas para garantizar calidad de servicio. Las ondas de alta frecuencia, es que experimentan problemas en atravesar algunos materiales como paredes o ventanas. Por motivos de costos, se planea utilizar estas celdas en sitios concurridos como estadios o coliseos, así como también en entornos urbanos densamente poblados.

Figure 2: Capacity and coverage considerations of spectrum categories

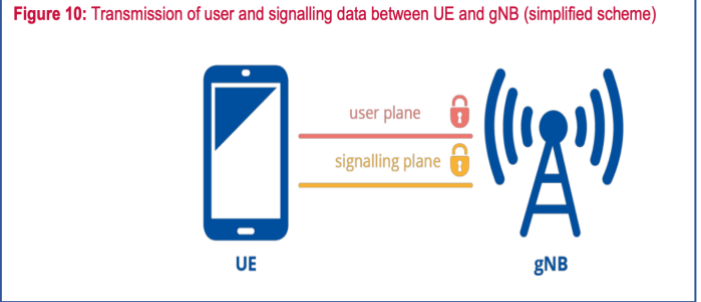


*(imagen tomada del documento Road to 5G: Introduction and Migration de GSMA)*

**5G** separa desde la misma interfaz radio, el plano de control y el de usuario y ambos deben estar securizados.

El uso de un cifrado fuerte para la protección entre el UE y la estación base no es nuevo. En las redes **4G** actuales, el cifrado del tráfico entre la estación móvil y eNodeB se puede implementar para la protección de la confidencialidad y la integridad de los datos intercambiados entre **UE** y **MME** (MME: Mobility Management Entity). En las redes 5G se aplican requisitos similares. Al igual que en el caso de 4G, algunos de estos requisitos son opcionales. La novedad que viene con 5G es la protección de la integridad de los datos del plano del usuario, pero esto también es opcional.

La protección de la integridad es **obligatoria** solo para el plano de señalización (señalización RRC y señalización NAS), mientras que es opcional para el plano de usuario.

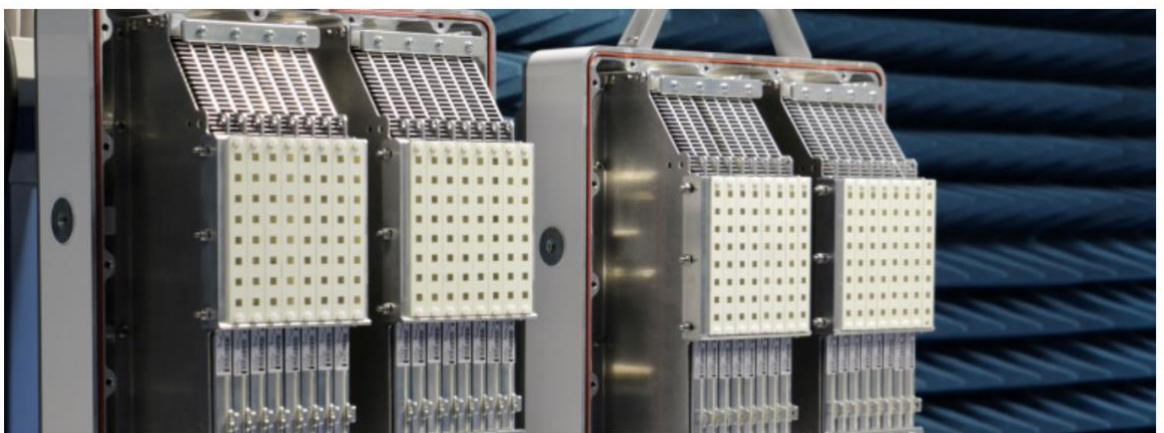


*Imagen tomada de: ENISA Report - Security in 5G Specifications.pdf*

### Otra novedad: mMIMO

MIMO masivo (**mMIMO: massive Multiple Input, Multiple Output**) significa tener al menos 8 antenas en cada extremo. El empleo de múltiples antenas en 5G está enfocado a dos objetivos.

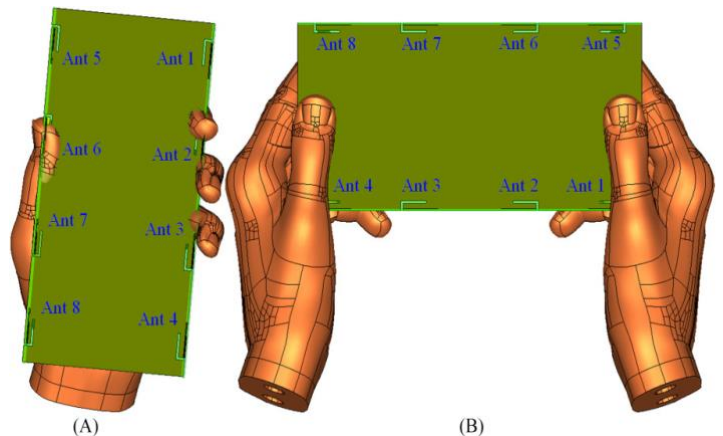
- El primero es compensar la pérdida de cobertura ocasionada por el uso de bandas milimétricas.
- El segundo es mejorar la eficiencia espectral, lo cual es importante sobre todo en el rango de sub6 donde 5G tiene que competir con LTE, esto se logra con el empleo de un indicador llamado **CSI** (Channel Status Information) que ayuda a la estación base a separar las señales transmitidas hacia o desde varios UEs.



64 TX + 64 RX 5G MU-MIMO antenna suitable for Massive MIMO (Credit: [Ericsson](#))

Aquí se presenta un problema físico del lado de usuario, pues como bien sabemos las frecuencias determinan la longitud de las antenas, por lo tanto si se desean emplear

simultáneamente diferentes señales, será necesario **contar en el teléfono móvil con más de una antena** (tema ya existente en LTE, pero ahora en mayor medida). En la actualidad, se presentan en el orden de ocho antenas diferenciadas dentro de un mismo UE (en la estación base son más aún). Cada una de estas antenas debe ser diseñada en detalle, para no interferir con el resto y responder adecuadamente a un amplio rango de frecuencias.



La potencia de emisión, tanto de las estaciones de radiofrecuencia, como la de los dispositivos móviles, son una de las mayores preocupaciones y fuentes de conflicto para las entidades gubernamentales, como así también para las empresas, organismos de control medioambiental y movimientos de defensa social. En Europa están bastante regulados y controlados y España se ajusta a estas decisiones, no es así con las empresas asiáticas por lo que es cierto que no se tiene garantía de cumplimiento cuando se adquieren teléfonos móviles que no han pasado por los organismos de control Europeos.

En la actualidad ya se cuenta con una amplia gama de teléfonos 5G, algunos de ellos se presentan a continuación.

### 5G smartphones

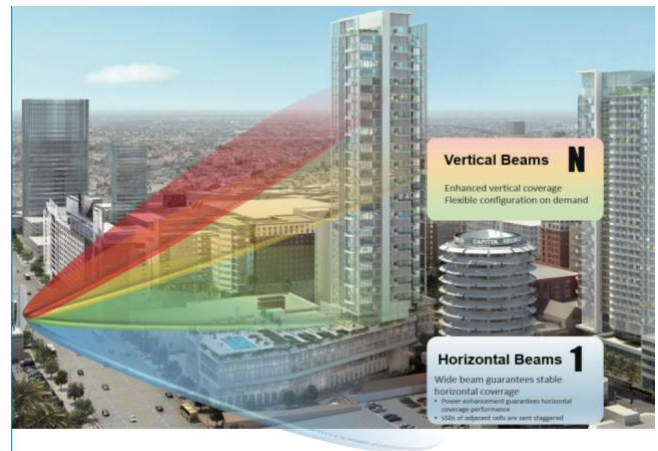


*Oriqende la imagen: Future of 5G (Qualcomm)*

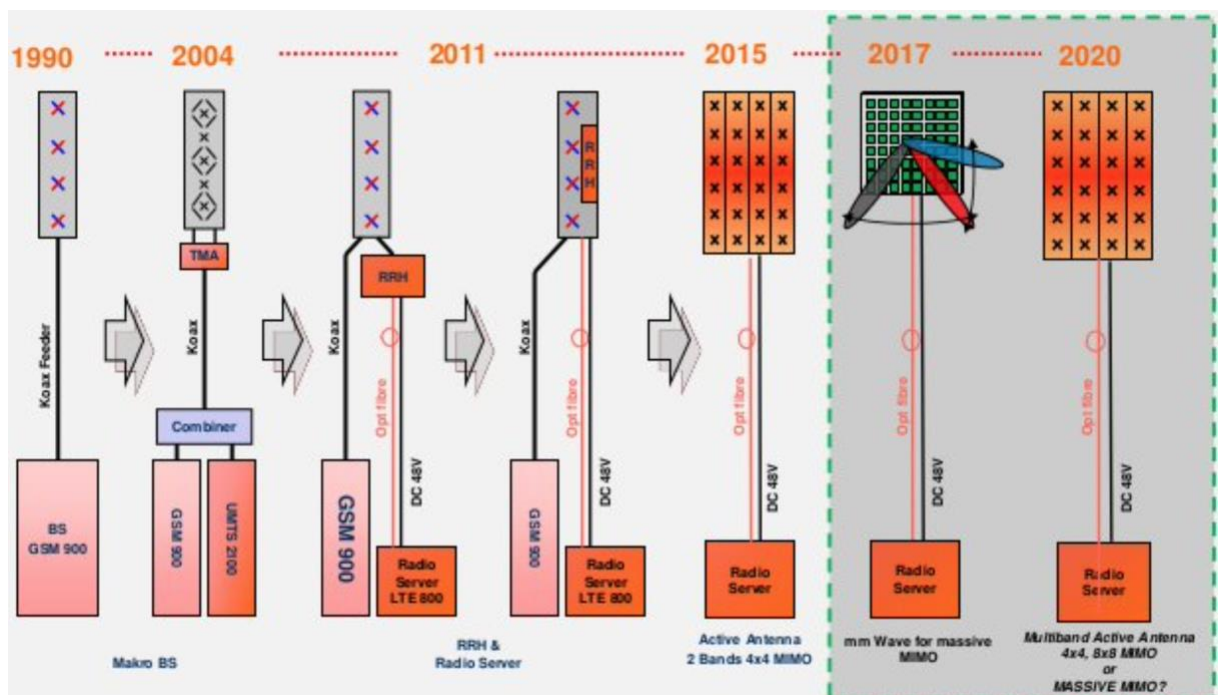
<https://www.qualcomm.com/media/documents/files/making-5g-nr-a-commercial-reality.pdf>

Otro concepto novedoso de 5G es la capacidad de empleo de **MuMIMO (Multi User MIMO)** que se basa en antenas con haces (beams) muy direccionables permitiendo a las estaciones base tener un alto número de antenas que dirigen sus haces usuarios más individualizados.

El concepto más novedoso trata ya de Full Dimension MIMO (**FD-MIMO**) que permiten una precodificación dinámica conjunta en todas las antenas de una matriz con la finalidad de conseguir haces más direccionales que eviten interferencias entre sí, en general estas matrices de antenas toman como base **128x128 elementos o más**.



Con todas estas características, las antenas de telefonía móvil a lo largo de su historia han sufrido muchos cambios, a continuación se puede ver una imagen de una presentación de Kathrein (<https://www.slideshare.net/KarvaCarbi/antenna-evolution-from-4g-to-5g-70581361>) donde se ponen de manifiesto estos cambios.



*Imagen tomada de la presentación citada en el párrafo anterior*

Las antenas de los años 90 eran mono banda, con 3G se comenzó con antenas multi banda. La necesidad de ampliar espectros, llevó al concepto de **RRH (Remote Radio Head)** inaugurando la tecnología de estación base distribuida, donde se comienza a separar esta RRH de la función digital o Unidad de Banda Base (BBU: Base Band Unit) conectándose ambas por fibra óptica (FO).

Las altas frecuencias que proponen las mmWave ocasionan también otro inconveniente que afecta a los cables coaxiales, pues su atenuación en relación con la frecuencia aumenta considerablemente. La solución a este problema nace con las **Antenas Activas (AA)** donde



los elementos de RF se colocan pegados a la antena. Es decir, se integra la RRH con la antena en un mismo elemento físico.

Por último aparece la capacidad de sumar múltiples frecuencias y con la incorporación de las ondas milimétricas (mmWave) que permite una gran direccionabilidad de las señales entrando en juego el concepto de "haces" de frecuencias. Hoy en día es normal encontrar antenas con funciones que se conocen con RET (Remote Electrical Tilt) que permiten dirigir el Haz de forma vertical u horizontal hacia el destino deseado.

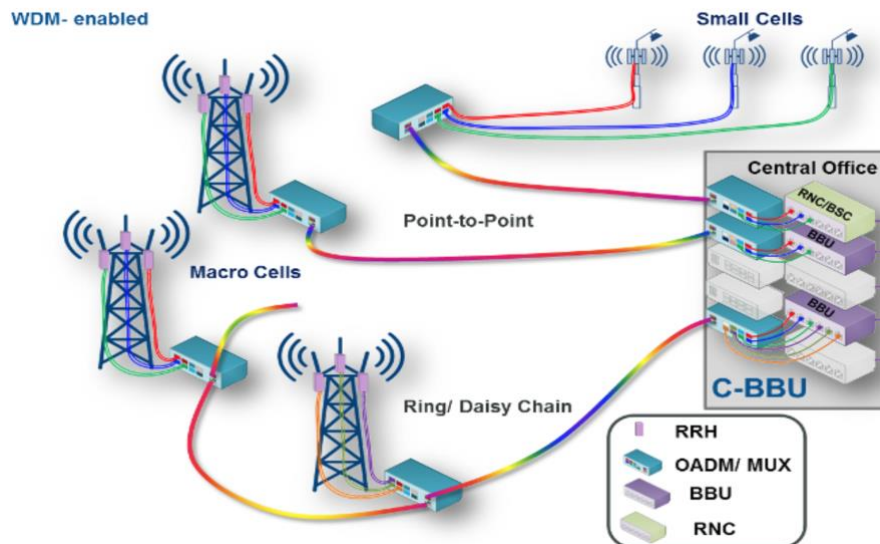
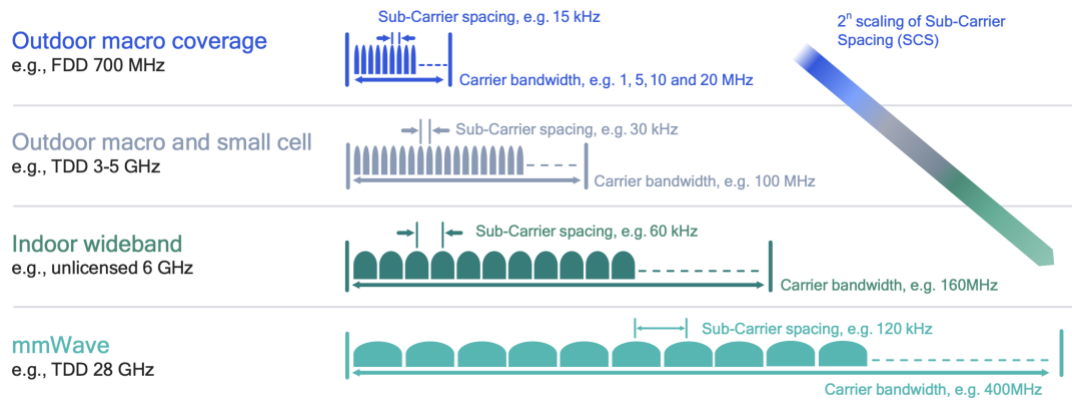


imagen tomada de: <https://www.conectronica.com/wireless/redes-wireless/fronthaul-backhaul-movil>

Esta nueva arquitectura se conoce como "**Cloud RAN**" o **C-RAN**. Este nuevo diseño representa enormes ahorros de instalaciones, espacio, energía y refrigeración a las teleoperadoras, aparece el concepto de "**Front Haul**" que trata de la conexión mediante FO de varias RRH a un único BBU, si a esto sumamos las capacidades actuales de multiplexación por división de onda (**WDM**: Wavelength Division Multiplexing) que ofrece la FO, la situación se convierte en imprescindible.

Como se acaba de presentar en las imágenes anteriores, ahora sí se puede volver a los conceptos sobre los tres tipos de frecuencias que se han planteado al principio (bajas, sub6 y mmwave).

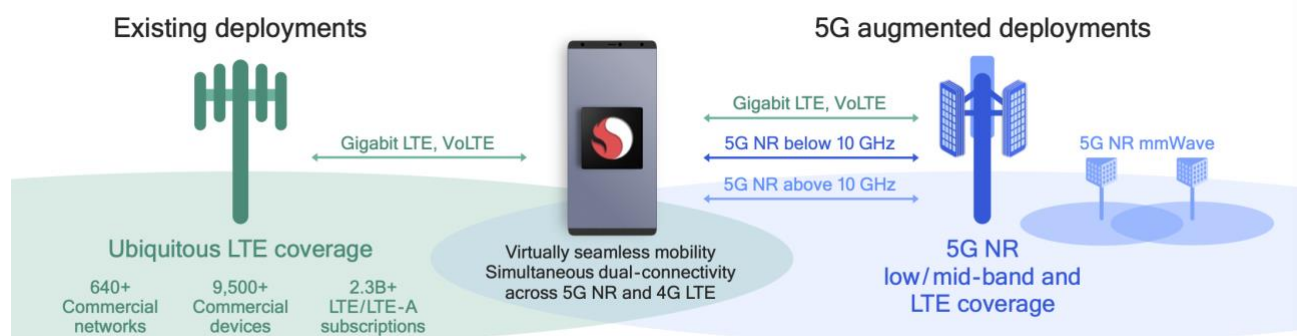
- Los **SCSs (Subcarrier Spacing)** menores se emplearán en los entornos "macro" tradicionales ya existentes con anchos de banda de 1, 5, 10 y 20 MHz, cuyo objetivo principal es lograr la total cobertura con 5G. En estos rangos es muy difícil encontrar rangos vacíos de frecuencias del orden de los 100MHz.
- Las bandas por encima de los **3 GHz**, donde ya se pueden encontrar rangos de frecuencias vacías de 100 MHz, y estas frecuencias ya nos permiten dar mayor capacidad o velocidad de transmisión.
- Para **entornos cercanos** ya se pueden emplear las frecuencias más altas logrando las mayores capacidades de 5G en detrimento de la distancia. Aquí se emplean SCSs de 30, 60, 120 y 240 KHz



Origen de la imagen: Future of 5G (Qualcomm)

<https://www.qualcomm.com/media/documents/files/making-5g-nr-a-commercial-reality.pdf>

Otra idea que plantea 5G es la "**Dual Connectivity**" (**DC**) en el modo NSA, el usuario accede a la red LTE y luego es configurado para operar en NR, conectándose simultáneamente a LTE y NR, pudiendo a su vez ser cada una de ellas en un plano diferente, por ejemplo una para plano de control y otra para el de usuario.



Origen de la imagen: Future of 5G (Qualcomm)

<https://www.qualcomm.com/media/documents/files/making-5g-nr-a-commercial-reality.pdf>

Cuando se habla de "Dual connectivity", no podemos dejar de lado dos conceptos más:

- **Refarming:** que reparte el espectro entre dos tecnologías.
- **DSS (Dynamic Spectrum Sharing)** Reparte el espectro de manera simultánea. Cada un milisegundo la interfaz radio analiza la demanda y asigna los recursos disponibles, en nuestro ejemplo a 4G y/o 5G, de manera que todos los usuarios tienen acceso a todo el espectro en todo momento. En estos momentos con pocos usuarios activos en 5G, es muy eficiente porque no resta ancho de banda a 4G.

**Dato Interesante:** Los **sensores SAR (Specific Absorption Rate)**, en español sería tasa de absorción específica, se implementan para medir la potencia que absorbe nuestro cuerpo y se expresa en Vatios sobre kilogramo. El cuerpo humano es un emisor de señales electromagnéticas denominadas generalmente como bioelectricidad, aunque son muy débiles, estos sensores SAR tienen la capacidad de detectarla y en el caso de los smartphone poseen circuitos integrados que tienen más de uno de ellos para incrementar su capacidad de detección, y hasta son capaces de diferenciar un ser humano de un objeto inanimado que

genere una señal similar. Cabe mencionar que estos sensores SAR hoy también suelen encontrarse en tablet, relojes inteligentes y ordenadores.

La lógica que acompaña a los sensores SAR, le permite también, en primer lugar detectar la emisión electromagnética del móvil en sí mismo, y luego la potencia con la que está irradiando para poder reaccionar rápidamente en caso que supere el umbral que tiene definido legalmente y reducirla de forma automática.

### Empleo de Open RAN.

El objetivo de **Open RAN** es ampliar la arquitectura de radio hacia una red abierta e inteligente cumpliendo con los estándares de 3GPP, que incluyen:

- **Estandarización de interfaces abiertas**
  - Radio y banda base
  - **EMS**: Element Management System
  - **CU y DU** (Centralized unit y Distributed unit))
- **Desagregación de Software del hardware**
- **Hardware abierto:**
  - procesadores estándar.
  - Empleo de racks, chasis, distribuidores de potencia y cableado tal cual lo define OCP: Open Compute Project
  - interfaz estándar de acelerador de procesos
- **Software abierto:**
  - Soluciones de comunidades como **ONAP (Open Networking Automation Platform)**  
Un ejemplo es **OSC (O-RAN Software Community)**, que es una alianza entre Linux foundation y O-RAN para el desarrollo de una solución Open RAN.

NOTA: Para profundizar en estos conceptos, se recomienda analizar la alianza O-RAN y sus grupos de trabajo.

La tecnología Open RAN ya está ganando impulso. La transición está siendo ayudada por los trabajos en asociaciones industriales como la **O-RAN Alliance**, la **Open RAN Policy Coalition**, el **Telecom Infra Project (TIP)**, la **GSMA**, el **Broadband Forum** o el **Open RAN G4**, por nombrar algunos. Open RAN también forma parte de la agenda de la Comisión Europea de asociaciones público-privadas para fomentar la investigación en la red. Todas las partes interesadas públicas y privadas reconocen la importancia estratégica de agilizar la adopción de Open RAN en los mercados relevantes.

Las funciones **CP** (Control Plane) y **UP** (User Plane) se complementan con una arquitectura de gestión de alto nivel también ilustrada en la figura de abajo. Esto muestra las cuatro interfaces de gestión clave que especifica O-RAN Alliance, a saber:

- **A1**: Definido entre el No-RT RIC (Real Time, RAN Intelligent Controller) en el marco de gestión y orquestación de servicios y el RIC en tiempo "casi" (near) real en la RAN

- **E2**: una interfaz lógica definida entre el RIC near-RT y un nodo E2, que para **NR** (New Radio) puede ser cualquier combinación de **O-CU-CP**, O-CU-UP u **O-DU** (open central unit - open Distributed unit) **O-RU** (open radio unit).
- **O1**: definido entre el marco de gestión y orquestación de servicios y las funciones de red O-RAN.
- **Open Fronthaul Management Plane (M-Plane)**: definido entre el marco de gestión y orquestación de servicios y el O-RU definido por O-RAN.
- **O2**: definido entre el marco de gestión y orquestación de servicios y O-Cloud para proporcionar recursos de plataforma y gestión de carga de trabajo virtualizada.

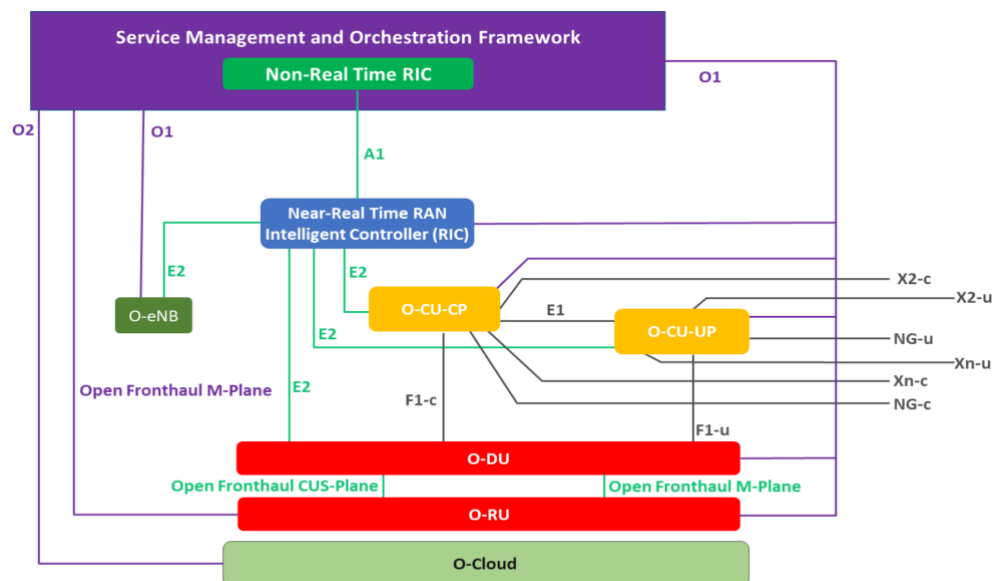


Figure 2-1: Logical O-RAN Architecture

Figura tomada de: [InDesign-Transition-Toward-Open-Interoperable-Networks-2020.pdf](https://www.in-design.com/transition-toward-open-interoperable-networks-2020.pdf)

### Solución virtualizada Open RAN.

La solución Open RAN sigue un diseño de red completamente en la nube. La **CU (Centralized unit)** y la **DU (Distributed unit)**, así como el **Sistema de Gestión de Elementos (EMS)** que gestiona los elementos de la red RAN, se benefician de una arquitectura definida por software. Las instancias virtuales adecuadas de **vCU**, **vDU** y **vEMS** se pueden implementar en una plataforma escalable basada en la nube administrada por un marco de gestión y orquestación de servicios.

### vCU y vEMS.

Los dos principales elementos virtualizados de la arquitectura Telco Cloud en la tecnología Open RAN son la **vCU** y la **vEMS**.

La **vCU** realiza las funciones de CU de las subcapas **PDCP** (Packet Data Convergence Protocol) y **RRC** (Radio Resource Control) en una plataforma servidor.

La función de **vEMS** es recopilar información con la granularidad adecuada de los diferentes módulos de software para controlarlos y operarlos de forma automatizada según lo ordena el **OSS** (Operation Support System). Incluye un conjunto de aplicaciones para ofrecer soluciones de sistemas de gestión de elementos como **FCAPS** (fallas, configuración, contabilidad, rendimiento y seguridad), **3GPP IRP** (Integration Reference Point) para la integración de **OSS** y compatibilidad con scripts. vCU y vEMS también se pueden implementar de manera flexible como un conjunto de funciones de red en contenedores para cumplir con los escenarios de implementación de 5G.

### RAN Sharing.

El concepto de RAN Sharing es algo que ya viene de tecnologías anteriores, pero en el caso de 5G cobra aún mayor importancia, pues en esta nueva interfaz radio (**NR**: New Radio) se debe desplegar nuevamente una costosa infraestructura para dar cobertura 5G en todo el territorio con tecnologías cada vez más sofisticadas y por ende más caras.

La idea de RAN Sharing ofrece a su vez beneficios medio ambientales, pues evita la saturación de antenas minimizando el impacto visual y la interferencia electrónica, cuestiones que también están siendo muy atacadas en argumentos de salud pública. Reduce también el consumo eléctrico natural que tiene cada una de estas instalaciones al compartir recursos.

Existen dos formas o tipos para implementar RAN Sharing:

- **Pasiva.**

Comparte elementos pasivos como pueden ser: edificios, espacios físicos, mástiles (Mast sharing), torres, etc. Se suele llamar también "Site Sharing".

Este tipo suele ser el más beneficioso para las operadoras, pues en la actualidad, el espacio físico, como así también el despliegue de nuevas antenas es uno de los mayores costes.

- **Activa.**

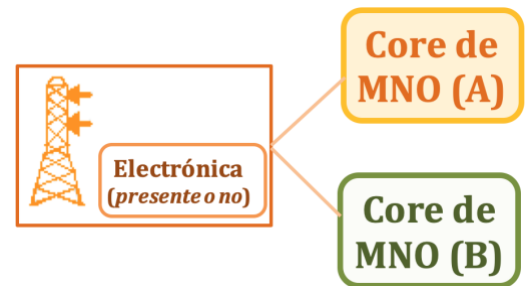
Comparte electrónica, accesos radio, antenas, licencias y hasta inclusive interconexiones con el resto de la red.

Existen varios tipos de compartición activa:

- **MORAN** (Multi Operator Radio Access Network)
- **MOCN** (Multi Operator Core Network)
- **Roaming**
- **MVNO** (Mobil Virtual Network Operator)

**MORAN** (Multi Operator Radio Access Network)

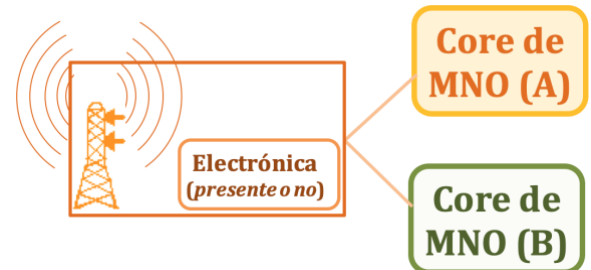
Tal vez sea la compartición activa más frecuente e importante. Los **MNO** (Mobile Network Operator) comparten una misma **RAN** (Radio Access Network) y, en general compartiendo también la **BTS** (Base Transceiver Station), **BSC** (Base Station Controller), **RNC** (Radio Network Controller), **NB** (nodeB), eNB o gNB, aunque esta electrónica no es condición mandatoria.



### MOCN (Multi Operator Core Network)

Es muy similar a la anterior, pero además de MORAN, aquí también se comparte el espectro de frecuencias y, en este espectro compartido tenemos nuevas opciones:

- Spectrum pooling: Comparten el ancho de banda de los espectros que cada uno tiene asignado.
- Spectrum Sharing: Si un operador no tiene espectro asignado, comparte el del otro u otros.



### Roaming

En este caso se trata del "Roaming Nacional", es decir, los acuerdos que tienen entre operadoras de un mismo país para dar cobertura a sus suscriptores aunque en esa zona no tenga despliegue de RAN.

Es el modelo más sencillo y económico para compartir recursos de red, ofreciendo a su vez importante flexibilidad a nuevos operadores pues permite el uso de toda una infraestructura desplegada de forma temporal o permanente por parte de otra empresa.

### MVNO (Mobil Virtual Network Operator)

Son Operadoras (o no) que comercializan servicios de voz y datos pero no tienen una infraestructura de red completa. En algunos casos hasta no tienen ninguna infraestructura de red, pero cuentan por ejemplo con una enorme base de datos de clientes (grandes centros comerciales, importantes marcas o empresas que poseen carteras de clientes por millones, etc.). Ejemplos de ello son Simyo, Jazztel, Yoigo, Carrefour, Pepephone, etc. Este caso aplica a varios segmentos e infraestructuras, pero en el caso que estamos tratando aquí, específicamente se trata de que no poseen desde frecuencias hasta la infraestructura de RAN.

Un factor clave de RAN sharing es la competencia que se genera en cualquiera de los casos. Este hecho, impacta menos en el tipo pasivo pues la operadora suele tener mucho más control de los recursos, en el caso activo el tema es más preocupante, y las regulaciones de cada país establecen en general, marcos de referencia y medidas concretas a cumplir.

En el año 2008 ITU convocó al 8th Global Symposium for Regulators, una de las charlas fue “**MOBILE SHARING**” (por: C. Borba), de la misma presentaremos algunas imágenes que presentan de forma más detallada los aspectos técnicos y componentes de RAN Sharing.

La Figura 1 (a continuación) nos describe los recursos que pueden compartirse en “passive sharing”.

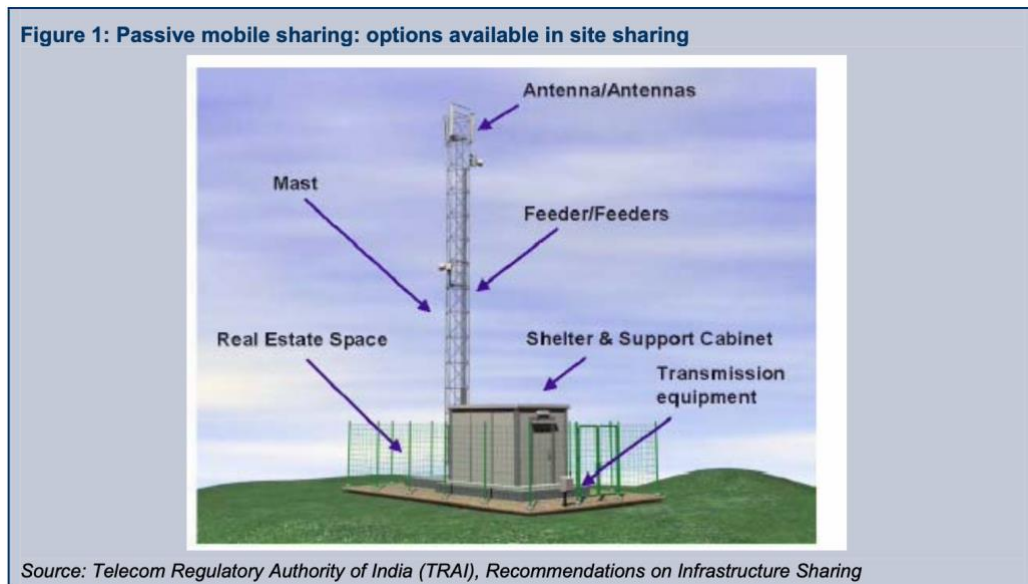


Figura tomada de: “MOBILE SHARING” (por: C. Borba).

En las dos imágenes que siguen, se presenta de forma más detallada y desglosada en dos formas, el concepto de “active sharing”, y se considera importante esta subdivisión para que podamos observar el nivel del problema que representa a un operador, desde el punto de vista de la seguridad, tener que dar acceso a la competencia a componentes clave de su infraestructura.

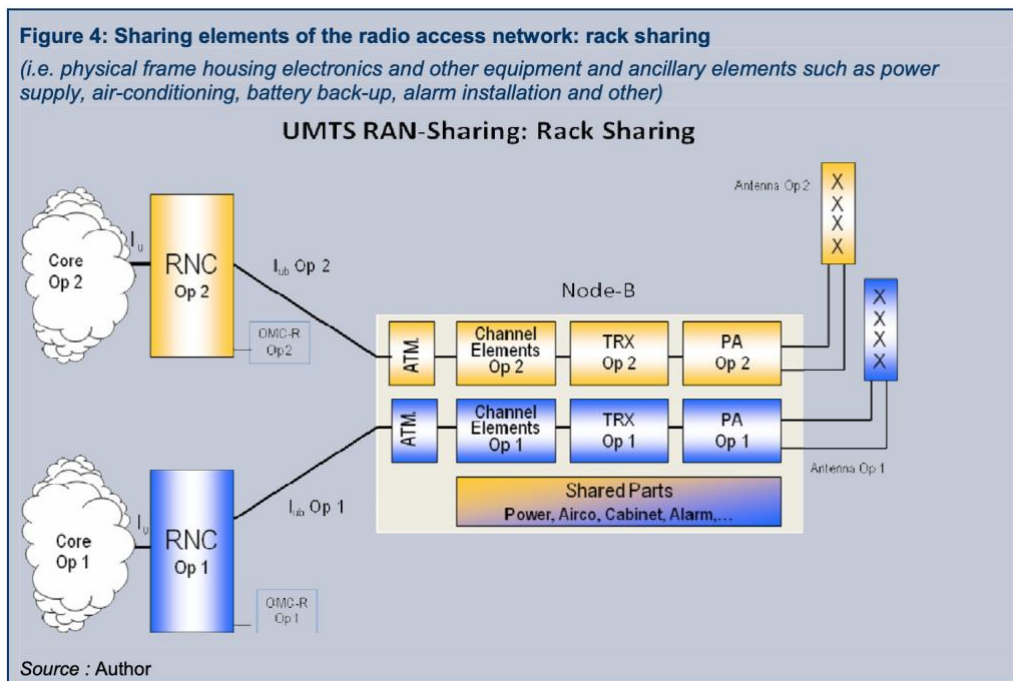


Figura tomada de: “MOBILE SHARING” (por: C. Borba).

- TRX: Transmisor/Receptor
- PA: Amplificador de potencia
- ATM: Switch de transmisión ATM (puede ser otro protocolo, ej: Ethernet)
- OMC-R: Operación y mantenimiento RNC
- Channel Elements: procesadores de datos para diferentes servicios
- RNC: Radio Network Controller
- Iub: Interfaz entre RNC y nodeB

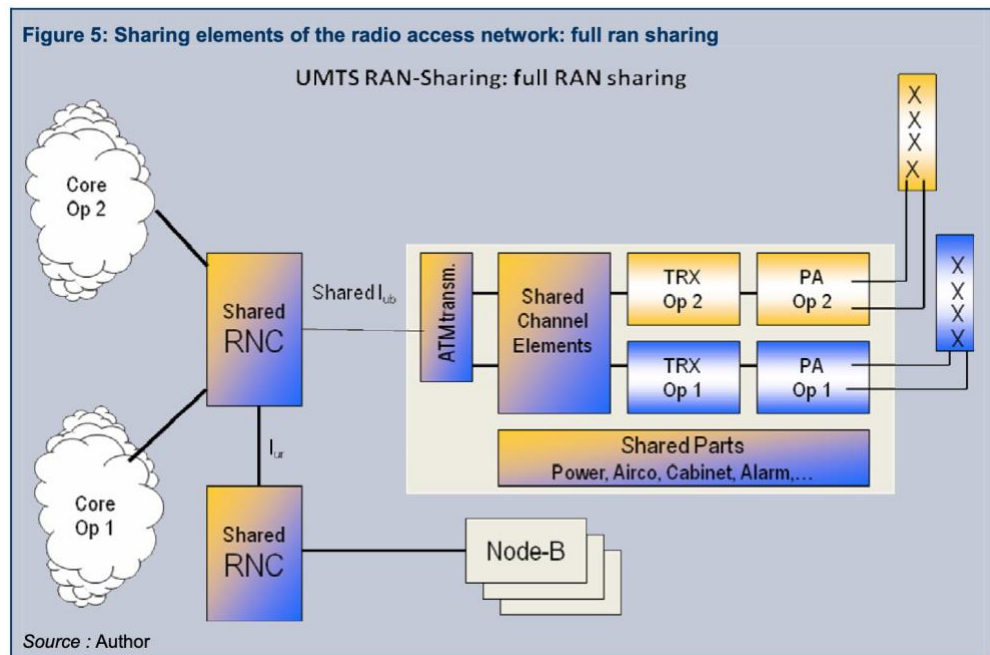


Figura tomada de: "MOBILE SHARING" (por: C. Borba).

### Seguridad en RAN Sharing.

Este es uno de los temas más importantes de compartir. Tanto en el tipo pasivo, como activo es necesario contemplar un conjunto de medidas que no pueden ser dejadas de lado.

En RAN Sharing pasivo, el principal control es en la parte física, donde se deberá tener en cuenta un riguroso procedimiento de control de acceso y de ser posible de segmentación física de los recursos de la otra operadora. Es un tema muy frecuente, encontrar en centrales y gabinetes de comunicaciones, el empleo de jaulas, pasillos y hasta accesos diferentes a las instalaciones de personal externo. Por otro lado, también se debe gestionar adecuadamente la supervisión y monitorización de estos accesos y medidas para evitar anomalías o fallos en momentos críticos, y en caso de producirse, contar con las alarmas y mecanismos adecuados de respuesta.

En RAN Sharing activo, el tema es más complicado pues se está abriendo el acceso lógico (y seguramente también físico) a personal que es externo a la operadora, y en la mayoría de los casos competencia.

Los controles a considerar deberían ser al menos:



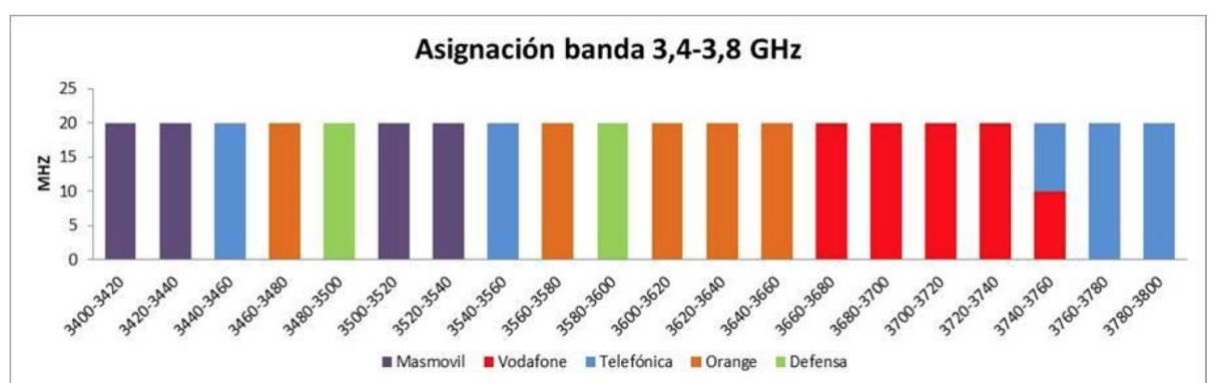
- Robustos procedimientos de gestión de accesos y gestión de usuarios.
- Adecuada segmentación de entornos.
- Supervisión, control y monitorización de actividad.
- Estricto empleo de roles y perfiles en las herramientas de Operación y mantenimiento. Control sobre escalado de privilegios y empleo de cuentas con atributos especiales.
- Empleo de un buen sistema de gestión y correlación de Logs.
- Desarrollo y prácticas sobre técnicas forenses.

### Frecuencias licitadas y asignadas

Para tratar este tema, pongamos como ejemplo a España. Actualmente estas frecuencias se encuentran asignadas de acuerdo a las imágenes que siguen. Se finalizó la subasta de la banda de **3,4 a 3,8 GHz** con resultados bastante insatisfactorios pues solo Vodafone logró ganar 90 MHz contiguos, el resto de las operadoras los tienen divididos, lo cual complica alcanzar máximas velocidades, también hay intermedios rangos que son del Ministerio de Defensa.

El “ACUERDO POR EL QUE SE EMITE INFORME AL PROYECTO DE ORDEN, POR LA QUE SE APRUEBA EL PLIEGO DE CLÁUSULAS ADMINISTRATIVAS PARTICULARES Y DE PRESCRIPCIONES TÉCNICAS PARA EL OTORGAMIENTO POR SUBASTA DE CONCESIONES DE USO PRIVATIVO DE DOMINIO PÚBLICO RADIOELÉCTRICO EN LA BANDA DE 3400-3600 MHz Y SE CONVOCA LA CORRESPONDIENTE SUBASTA IPN/CNMC/045/20 SUBASTA 20 MHz BANDA 3,5 GHz “

(<https://www.cnmc.es/sites/default/files/3309398.pdf>), presenta cómo ha quedado esta subasta en España.



*Imagen tomada de: <https://www.cnmc.es/sites/default/files/3309398.pdf>*

La televisión analógica en España ha utilizado históricamente para su emisión parte de la banda de frecuencias **VHF: 47-230 MHz** y parte de la banda **UHF: 470-862 MHz** (VHF: Very High Frequency - UHF: Ultra High Frequency). Con la tecnología de digitalización de la señal analógica el mundo ha cambiado, y no hay duda de los inmensos beneficios que este nuevo

tipo de señales ofrecen, si a ello sumamos la capacidad de compresión que ofrece la electrónica actual no queda lugar para señales analógicas. Por ejemplo, en el caso de la televisión, en el ancho de banda de un canal analógico se pueden transmitir hoy en día seis canales digitales. Esta evolución tecnológica, ha llevado a todos los países a reorganizar sus asignaciones de frecuencias. Volviendo al caso de España, siguiendo las directivas de la Unión Europea, generó los llamados dividendos digitales para esta reorganización de frecuencias. Entre el 2011 y 2015 se produjo el primero de ellos, liberando para 4G las frecuencias de **790 a 862 MHz**, que se correspondían a los canales 61 a 69 de la Televisión Digital Terrestre (**TDT**), esta banda es la que se denominó banda de 800 MHz y cuenta con un ancho de banda de 72 MHz. Esta licitación tuvo como resultados la tabla que se presenta a continuación.

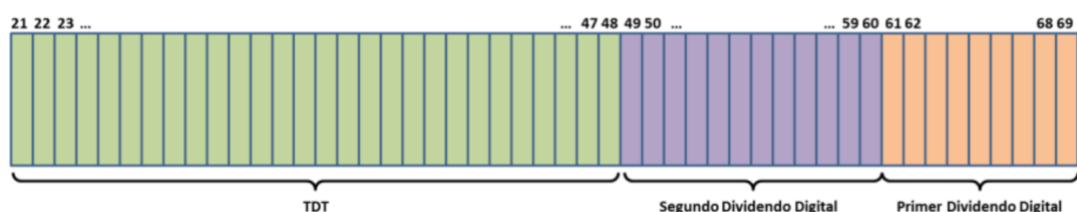
Bloque	Subida	Bajada	Operador	Concesión	Caducidad
2x5 MHz	832-837MHz	791-796MHz	Orange	01/04/2015	25/04/2031
2x5 MHz	837-842MHz	796-801MHz	Orange	01/04/2015	25/04/2031
2x5 MHz	842-847MHz	801-806MHz	Vodafone	01/04/2015	25/04/2031
2x5 MHz	847-852MHz	806-811MHz	Vodafone	01/04/2015	25/04/2031
2x5 MHz	852-857MHz	811-816MHz	Movistar	01/04/2015	25/04/2031
2x5 MHz	857-862MHz	816-821MHz	Movistar	01/04/2015	25/04/2031

Imagen tomada de: [https://wiki.bandaancha.st/Frecuencias telefonía móvil](https://wiki.bandaancha.st/Frecuencias_telefonía_móvil)

En el enlace de la imagen anterior puede encontrarse información de detalle sobre toda la distribución de frecuencias para la telefonía móvil.

Ya pensando en **5G**, la "*DECISIÓN (UE) 2017/899 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de mayo de 2017 sobre el uso de la banda de frecuencia de 470-790 MHz en la Unión*" reguló un nuevo rango. En el año 2020 siguiendo estas directivas, entró en vigor en España el llamado segundo dividendo digital, liberando ahora las frecuencias comprendidas entre los **694 y 790 MHz**, lo que se denominó banda de 700 MHz.

En la imagen que sigue, se presentan los canales que han sido liberados. Como hemos dicho, en el primer dividendo se liberaron los canales 61 a 69 correspondientes a las frecuencias 790 a 862, denominada banda de 800 MHz, y con este segundo dividendo se liberan los canales 49 a 60 correspondientes a las frecuencias de 694 a 790 MHz, denominada banda de 700 MHz. En el mes de julio de 2021 comienza la subasta de la banda de 700 MHz que quedó libre con este último dividendo digital.



El espectro de telefonía móvil en España en la actualidad, quedaría de acuerdo a la imagen que se presenta a continuación.

700 MHz (Banda 12) 5G	-	-	-	-	-
800 MHz (Banda 20) 4G	20 MHz FDD	20 MHz FDD	20 MHz FDD	-	-
900 MHz (Banda 8) 2G y 3G	30 MHz FDD	20 MHz FDD	20 MHz FDD	-	-
1.800 MHz (Banda 3) 2G y 4G	40 MHz FDD	40 MHz FDD	40 MHz FDD	30 MHz FDD	-
2.100 MHz (Banda 1) 3G	30 MHz FDD 5 MHz TDD	30 MHz FDD 5 MHz TDD	30 MHz FDD 5 MHz TDD	30 MHz FDD 5 MHz TDD	30 MHz FDD 5 MHz TDD
2.6 GHz (Banda 7) 4G y 5G	40 MHz FDD 10 MHz FDD Madrid y Melilla	40 MHz FDD 20 MHz TDD	40 MHz FDD 10 MHz TDD 10 MHz FDD España excepto Castilla La Mancha, País Vasco, Asturias, Galicia, Madrid Melilla	10 MHz TDD Madrid, Cataluña, Castilla-La Mancha y Andalucía	-
3.4/3.8 GHz (Banda 42-43) 5G	90 MHz TDD (40 MHz válidos hasta 2030) (50 MHz válidos hasta 2038)	90 MHz TDD (válidos hasta 2038)	100 MHz TDD (40 MHz válidos hasta 2030) (60 MHz válidos hasta 2038)	80 MHz TDD (válidos hasta 2030)	-

El día 21 de julio de 2021 se finalizó con la licitación de las frecuencias de 700 MHz, producto del segundo dividendo digital terrestre que hemos mencionado. En este caso Telefónica de España obtuvo 20 MHz en el bloque 1, a continuación se presenta cómo ha quedado esta nueva distribución de frecuencias:

Banda de frecuencias	Número de la concesión	Rango de frecuencias	Ancho de banda por concesión	Cobertura geográfica	Precio de adjudicación (€)	Adjudicatario
Banda pareada 703-733 y 758-788 MHz	1	Bloque abstracto	2x10 MHz	Estatal	310.089.000	TELEFÓNICA
	2	Bloque abstracto	2x10 MHz	Estatal	350.000.000	VODAFONE
	3	Bloque abstracto	2x5 MHz	Estatal	175.000.000	ORANGE
	4	Bloque abstracto	2x5 MHz	Estatal	175.000.000	ORANGE
Banda 738-753 MHz	5	Bloque abstracto	5 MHz (solo descendente)	Estatal	Desierta	
	6	Bloque abstracto	5 MHz (solo descendente)	Estatal	Desierta	
	7	Bloque abstracto	5 MHz (solo descendente)	Estatal	Desierta	
Total					1.010.089.000	