

Spectrum aspects of Internet of Things

Spectrum Allocations & IoT Regulations

Capacity Building Workshop

Sahar CHEAYTO



Day 2

IoT Spectrum, Licensing & Roaming

01

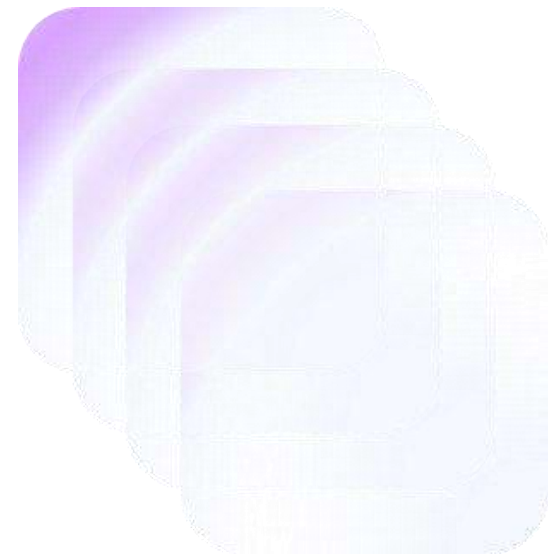
IoT Spectrum Requirement & Regulations

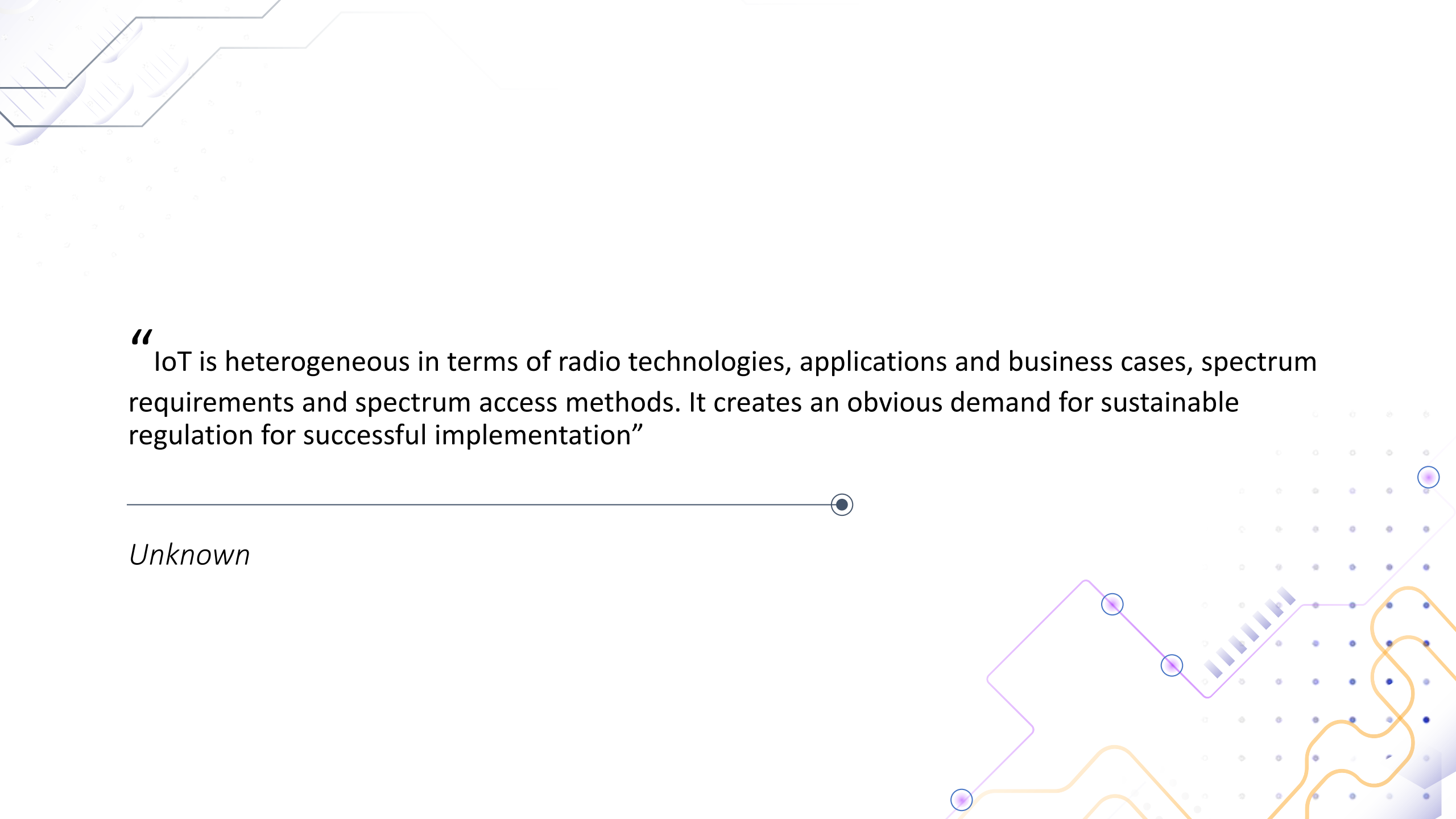
02

**IoT Spectrum Management, Licensing
& Roaming**

03

IoT Regulations





“ IoT is heterogeneous in terms of radio technologies, applications and business cases, spectrum requirements and spectrum access methods. It creates an obvious demand for sustainable regulation for successful implementation”

Unknown



01

IoT Spectrum Requirement & Regulations



IoT Spectrum Requirement

IoT spectrum Access

The spectrum requirements and standards for IoT wireless access technologies and techniques are being addressed in ITU-R, including

- ✓ Frequency Harmonization,
- ✓ Technical and operating parameters the operation of short range devices
- ✓ Spectrum to support the implementation of narrowband and broadband machine type communication (MTC) infrastructures
- ✓ Support for massive machine-type communications within the framework of the standards and spectrum for IMT-Advanced (4G) and IMT-2020 (5G)
- ✓ Use of fixed-satellite and mobile-satellite communications for IoT
- ✓ Protection of radio services from power line telecommunication system emissions

IoT Spectrum Requirement Radio Technologies for IoT

A variety of radio technologies is used to implement the Internet of things, extending from **short range devices** to **wide area sensor**, networks and **global terrestrial IMT** systems as well as **satellite systems**

➤ The ITU-R Study Groups are developing technical and operational standards to facilitate the deployment of IoT on a global basis, including **harmonized frequency** spectrum and appropriate regulatory regimes

➤ Associated aspects will also be addressed at the forthcoming World Radiocommunication Conference 2023 (WRC-23) agenda items 1.2, 1.3 and 1.4

IoT Spectrum Requirement & Regulations

ITU-R Studies

Resolution ITU-R 66

Studies related to wireless systems and applications for the development of the Internet of Things

- Different radiofrequency bands, many of which provide communication channels, infrastructure and capacity, could be used in IoT deployment with the aim of ensuring cost-effective deployment and efficient use of the radiofrequency spectrum
- IoT is a concept encompassing various platforms, applications, and technologies that are, and will continue to be, implemented under a number of radiocommunication services
- The implementation of IoT currently does not require specific regulatory provisions in the Radio Regulations
- **ITU-R is invited to conduct studies on the technical and operational aspects of radio networks and systems for IoT**
- **Development of ITU-R Recommendations, Reports and/or Handbooks as appropriate, on the basis of the studies**

IoT Spectrum Requirement & Regulations

ITU-R Studies

- Resolution 245 (WRC-19) to consider identification of the frequency bands 3 300-3 400 MHz, 3 600-3 800 MHz, 6 425-7 025 MHz, 7 025-7 125 MHz and 10.0- 10.5 GHz for International Mobile Telecommunications (IMT), including possible additional allocations to the mobile service on a primary basis
 - **Considering** that IMT systems are now being evolved to provide diverse usage scenarios such as enhanced mobile broadband, **massive machine-type communications** and ultra-reliable and low latency communications, and applications including fixed broadband;
 - That identification of frequency bands as in considering lower and higher frequency bands, the mid-band spectrum for IMT may change the sharing situation regarding applications of all services to which the frequency band is already allocated, and may require additional regulatory actions;
- Question ITU-R 262/5 addresses the study of usage of IMT systems for specific applications;
- Resolution ITU-R 54-3 Studies to achieve harmonization for **short-range devices SRDs**
- Report ITU-R M.2320 addresses **future technology trends of terrestrial IMT systems**
- Recommendation ITU-R M.2083, on the framework and objectives of the future development of IMT for 2020 and beyond;



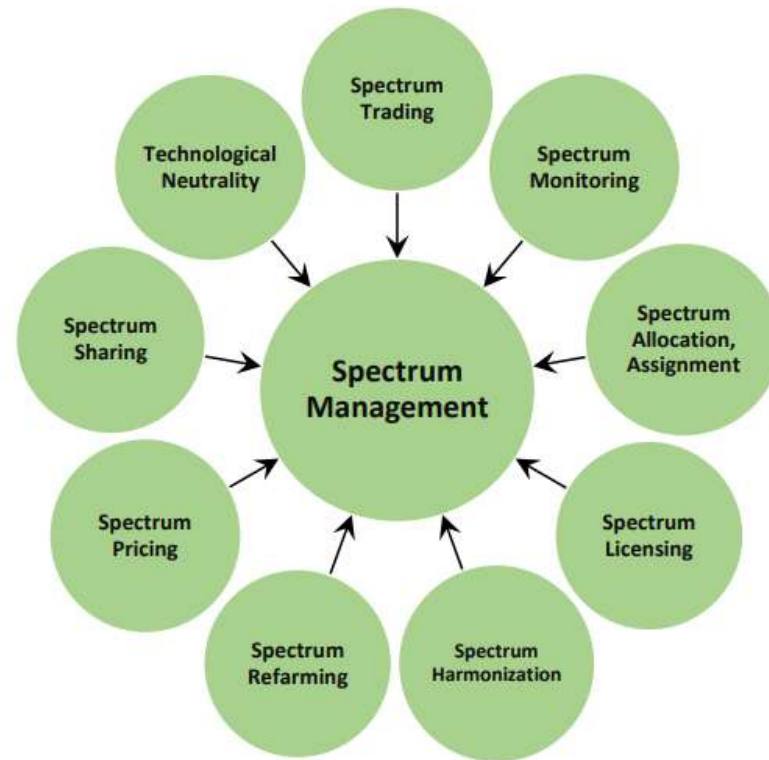
02

IoT Spectrum Management & Licensing



IoT Spectrum Management

Spectrum Management Issues for IoT Devices

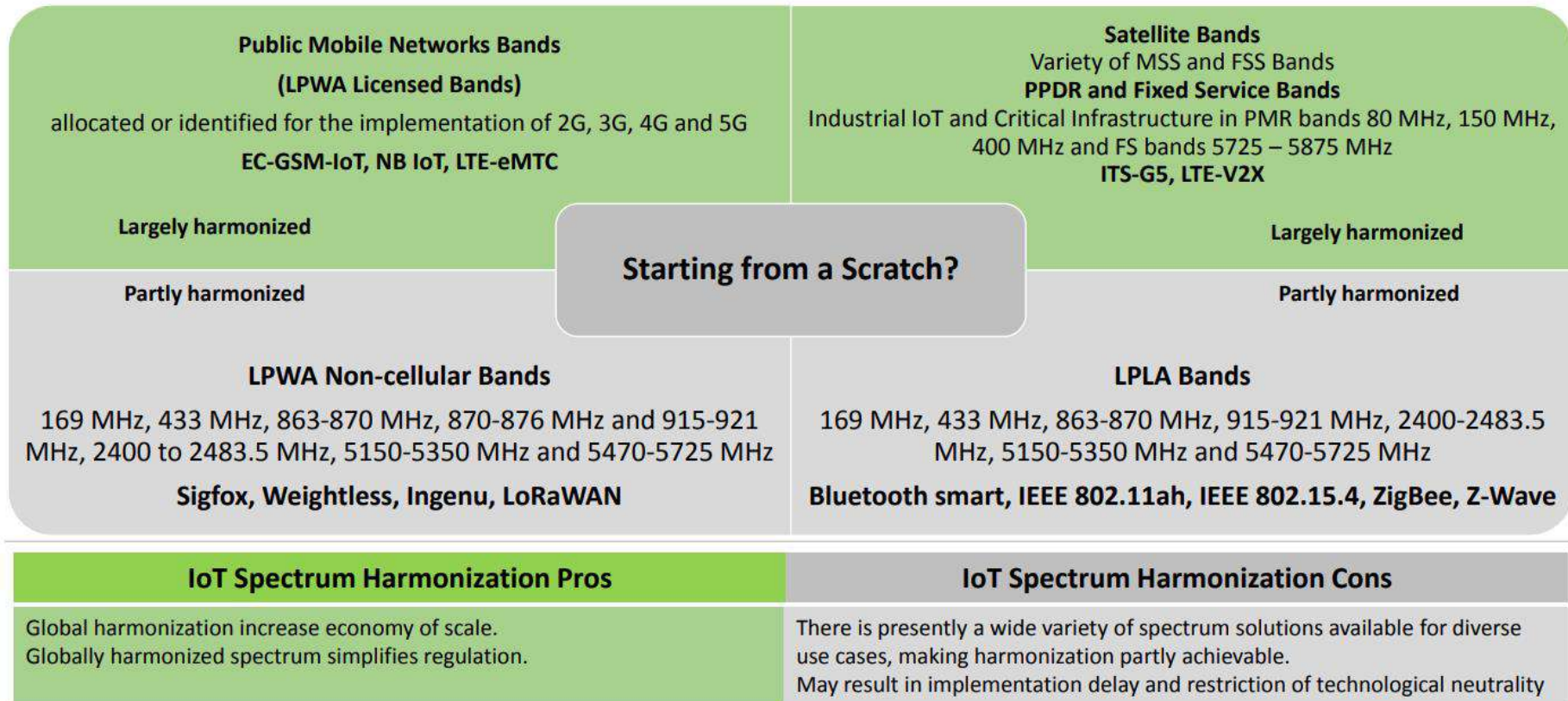


Rapidly growing IoT industry is entirely in the scope of the traditional spectrum management environment

IoT Spectrum Management

IoT Spectrum Harmonization

There is no single frequency band defines M2M



ITU Presentation: Spectrum Management Aspects Enabling IoT Implementation

IoT Spectrum Management

Spectrum Sharing with IoT

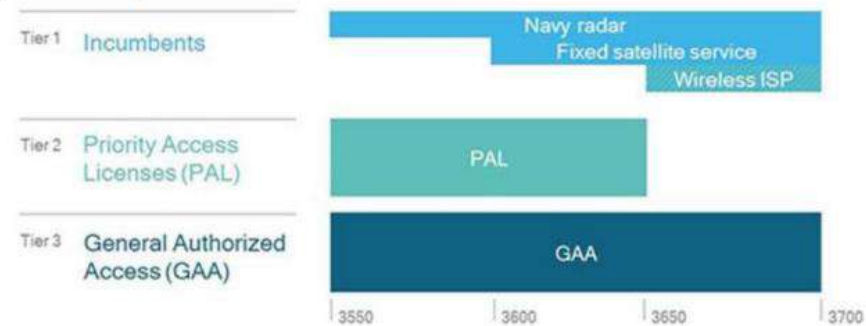
Where spectrum sharing is feasible; regulators should apply advanced engineering practices to create environment for heavy “packing” of uses in the same band while protecting superior users

New Opportunities for Spectrum Sharing

In 2016 the FCC opened up 150 MHz of spectrum in the U.S. around 3.5 GHz that it named **Citizens Broadband Radio Service (CBRS)**

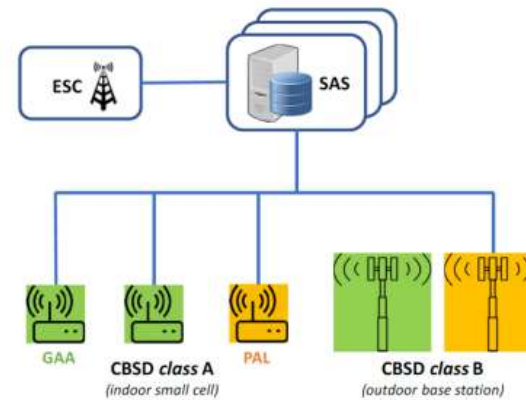


In addition to sharing with incumbents — CBRS adds a ‘third-tier’ of general usage.



CBRS adds a ‘third-tier’ of general usage where anyone can use the spectrum when it is not used by the higher tiers (the incumbents or users that paid for a license). GAA will encompass IoT uses. Source: CBRS Alliance

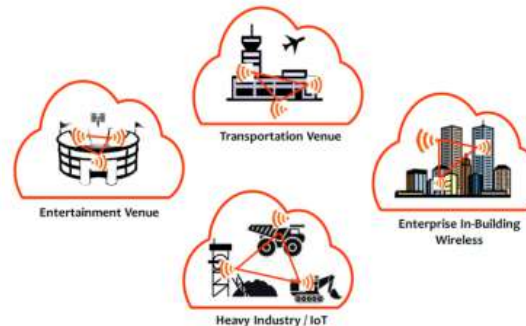
How It Works in Practice



SAS – Spectrum Access System

ESC – environmental Sensing Capabilities.

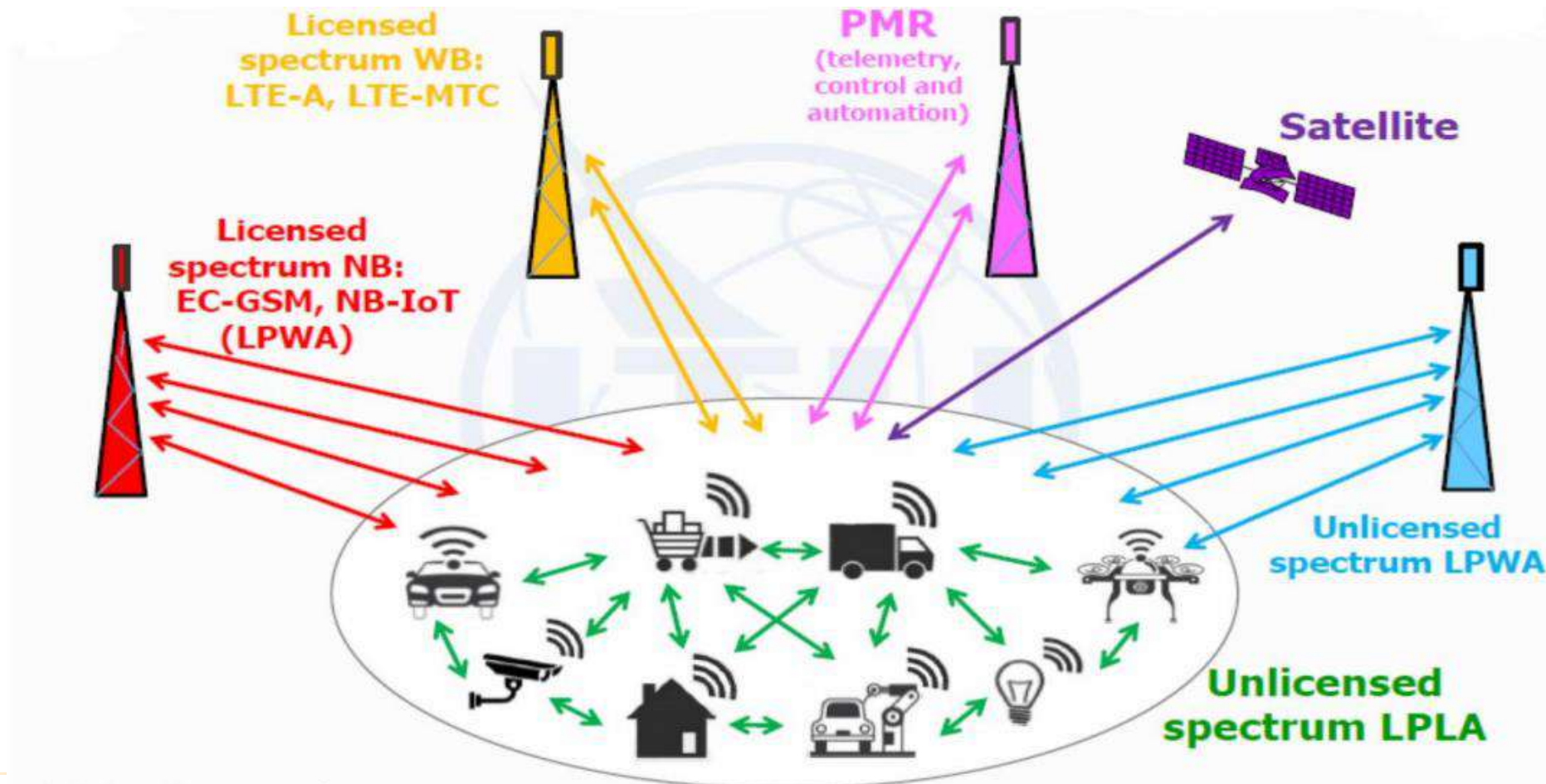
CBSD – Citizens Broadband Radio Service Devices



Heavy industry companies can set up an Enterprise Private LTE networks and run industrial IoT applications.

IoT Spectrum Licensing

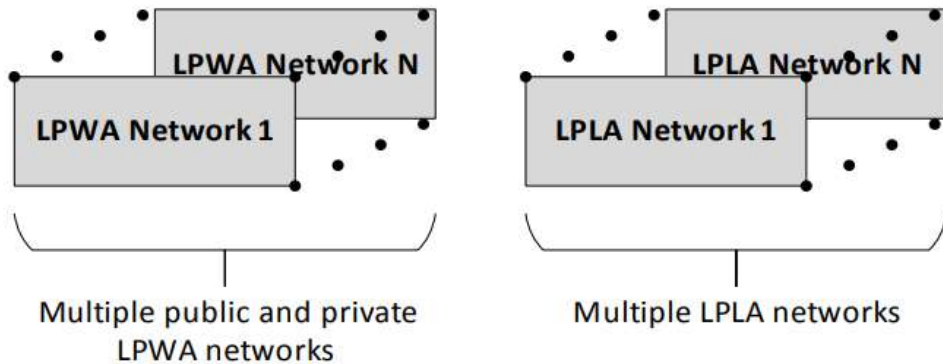
Licensed Vs Unlicensed Spectrum



IoT Spectrum Licensing

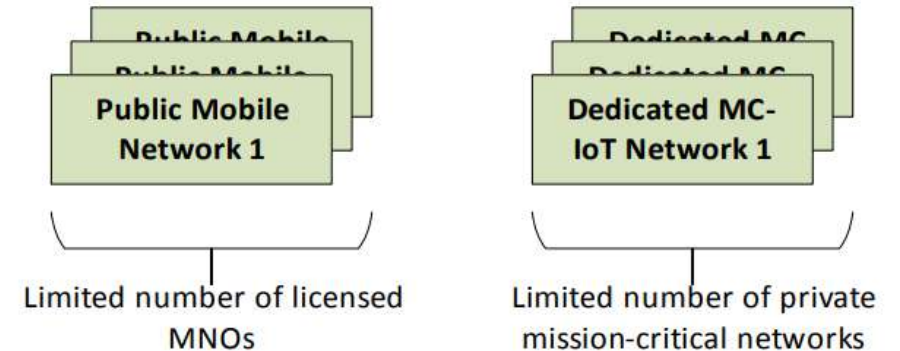
IoT regulatory use cases of licensed and unlicensed networks/spectrum

Unlicensed Spectrum



- Networks under general authorization regime (commons, class licences etc.) subject to certain regulatory conditions (EIRP limits, duty cycles etc.)
- Spectrum is used on a non-interference and un-protected basis, as a result, mainly identified for low power devices
- Applications have no strict requirements for low latency and ultra-reliable connections
- Applications are delay tolerant
- Applications with **no guarantees for sustainable QoS**

Licensed Spectrum



- Number of Public Mobile IoT networks is defined by bandwidth of licensed spectrum available for MNOs
- Dedicated Mission-Critical IoT networks are likely to utilize newly harmonized spectrum bands, e.g. 870 – 876/915 – 921 MHz, FS bands, such as 5725 – 5875 MHz etc.
- Applications requiring ultra-reliable connections in real-time communications
- Applications with high requirements for low latency
- High availability, guaranteed in-time delivery and QoS



03

IoT Spectrum Identifications & Roaming



Spectrum for IoT

Spectrum for MTC/IoT applications

Unlicensed spectrum

- *Low cost /no license fees*
Regulatory limits (EIRP restrictions)
- **Non-guaranteed QoS**

- All devices can have access to spectrum, subject to compliance with technical conditions as specified in regulations
- Short range and delay-tolerant applications are typical use cases

Licensed spectrum

- *Better Inference management*
- *Network Security*
- *Reliability*

Mobile operator Network

Reuse cellular infrastructure and device eco-system for M2M/ IoT apps

- IMT spectrum can be used for supporting NB-IoT, eMTC and LTE-V2N (eNB-to-vehicle)
- MBB spectrum can also be used for M2M/IoT

Dedicated Network

Private network customized for specific M2M/IoT apps.

Example: In **China** New bands for M2M:

- 5 905 -5 925 MHz for LTE-V2X trials
- 2 x 2.3 MHz in 800MHz can be used for NB-IoT

IoT Frequency Identification

NB-IoT and LTE-M



Parking meters



Sensors



Utility meters



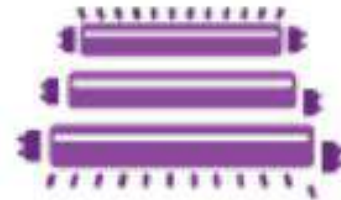
Agriculture monitors



Industrial sensors



City infrastructures



Lighting/HVAC controllers



IoT Frequency Identification

NB-IoT

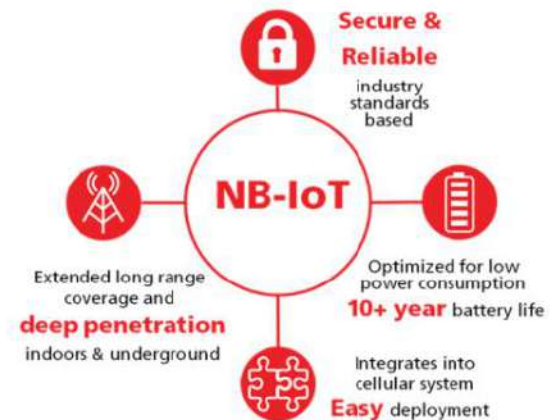
Narrowband Internet of Things NB-IoT; a new fast-growing Cellular technology standardized by **3GPP Release 13** to enable a wide range of cellular devices and services, addresses the LPWAN (Low Power Wide Area Network) **requirements of the IoT**. leverages **DSS modulation**

NB-IoT is very flexible and can operate in

- 2G, 3G and 4G bands
- can be deployed “in-band” **within a standard LTE carrier** or “standalone” **for deployments in dedicated spectrum**
- NB-IoT can also be implemented in an LTE carrier’s guard-band.

Classified as a **5G technology** in 2016 characterized by:

- Excellent indoor coverage,
- Support of a massive number of connections,
- Cost efficiency,
- Low device power consumption,
- Optimized network architecture



NB-IoT dramatically improves **network efficiency**, increasing the capacity to support a massive number of new **connections** using only **a portion of the available spectrum**

This efficiency, in turn, **minimises power consumption** enabling battery life of more than ten years

NB-IoT **penetrates deep underground** and into enclosed spaces **providing 20+dB coverage indoors**

IoT Frequency Identification

LTE-M

LTE-M; “Long-Term Evolution (LTE) machine-type communications (MTC),” is an **LPWA** technology standard introduced by **3GPP in Release 13**, leverages **LTE spread spectrum modulation**

GSMA describe it is a **5G technology**, that supports **simplified device complexity**, massive **connection density**, **low device power consumption**, **low latency** and it **provides extended coverage**, while allowing the **reuse of the LTE installed base**

LTE-M deployment can be done

- “in-band” within a standard LTE carrier or
- “standalone” in a dedicated spectrum

It serves a broad set of use cases providing an attractive option for device manufacturers looking to **deploy on current cellular networks**

The advantage of LTE-M over NB-IoT is its comparatively **higher data rate, mobility, and voice over the network**, but it **requires more bandwidth**, is **more costly**, and **cannot be put into guard band frequency band for now**

IoT Frequency Identification

NB-IoT and LTE-M Frequency Bands

LTE-M Frequency Bands

According to recommendations by the members of the GSMA LTE-M Task Force, minimum of eleven bands: 1, 2, 3, 4, 5, 12, 13, 20, 25, 26 and 28 are required for coverage in all the countries for which the LTE-M members have provided input

Narrowband IoT (NB-IoT), also known as LTE Cat NB1

The NB-IoT specification was frozen in Release 13 of the 3GPP specification (LTE-Advanced Pro),

- In June 2016 Release 13 defined **14 frequency bands for NB-IoT**
- In **Release 14**, 4 more frequency bands were added (**11, 25, 31 and 70**)
- In **Release 15**, 7 more bands were introduced (**4, 14, 71, 72, 73, 74, 85**).

IoT Frequency Identification

LTE-M Frequency Bands

LTE Frequency Band	UL Frequency Range(MHz)	DL Frequency Range(MHz)
Band 2	1850-1910	1930-1990
Band 3	1710-1785	1805-1880
Band 4	1710-1755	2110-2155
Band 5	824-849	869-894
Band 8	880-915	925-960
Band 12	699-716	729-746
Band 13	777-787	746-756
Band 20	832-862	791-821
Band 28	703 to 748	758 to 803

IoT Frequency Identification

NB-IoT Frequency Bands

NB-IoT Band	Uplink Band	Downlink Band	Bandwidth	Duplex Mode
B1	1920 – 1980 MHz	2110 – 2170 MHz	60 MHz	HD-FDD
B2	1850 – 1910 MHz	1930 – 1990 MHz	60 MHz	HD-FDD
B3	1710 – 1785 MHz	1805 – 1880 MHz	75 MHz	HD-FDD
B4	1710 – 1755 MHz	2110 – 2155 MHz	45 MHz	HD-FDD
B5	824 – 849 MHz	869 – 894 MHz	25 MHz	HD-FDD
B8	880 – 915 MHz	925 – 960 MHz	25 MHz	HD-FDD
B11	1427.9 – 1447.9 MHz	1475.9 – 1495.9 MHz	20 MHz	HD-FDD
B12	699 – 716 MHz	729 – 746 MHz	17 MHz	HD-FDD
B13	777 – 787 MHz	746 – 756 MHz	10 MHz	HD-FDD
B14	788 – 798 MHz	758 to 768 MHz	10 MHz	HF-FDD
B17	704 – 716 MHz	734 – 746 MHz	12 MHz	HD-FDD
B18	815 – 830 MHz	860 – 875 MHz	15 MHz	HD-FDD
B19	830 – 845 MHz	875 – 890 MHz	15 MHz	HD-FDD
B20	832 – 862 MHz	791 – 821 MHz	30 MHz	HD-FDD
B25	1850 – 1915 MHz	1930 – 1995 MHz	65 MHz	HD-FDD
B26	814 – 849 MHz	859 – 894 MHz	35 MHz	HD-FDD
B28	703 – 748 MHz	758 – 803 MHz	45 MHz	HD-FDD
B31	452.5 – 457.5 MHz	462.5 – 467.5 MHz	5 MHz	HD-FDD
B66	1710 – 1780 MHz	2110 – 2200 MHz	70/90 MHz	HD-FDD
B70	1695 – 1710 MHz	1995 – 2020 MHz	25 MHz	HD-FDD
B71	633 – 698 MHz	617 – 783 MHz	65 MHz	HD-FDD
B72	451 – 456 MHz	461 – 466 MHz	5 MHz	HD-FDD
B73	450 – 455 MHz	461 – 466 MHz	5 MHz	HD-FDD
B74	1427 – 1470 MHz	1475 – 1518 MHz	43 MHz	HD-FDD
B85	698 – 716 MHz	728 – 746 MHz	10 MHz	HD-FDD

IoT Frequency Identification

NB-IoT & LTE-M Deployments

As of September 2023 GSA had identified;

254 operators that have deployed or launched NB-IoT or LTE-M networks in 81 countries

- 173 operators actively investing in NB-IoT technology, of which:
 - 128 have deployed or commercially launched NB-IoT networks
 - 25 are planning, piloting or deploying NB-IoT networks
 - 20 are evaluating or trialing NB-IoT technology

- 80 operators actively investing in LTE-M technology, of which:
 - 60 have deployed or commercially launched LTE-M networks
 - 11 are planning, piloting or deploying LTE-M networks
 - Nine are trialing LTE-M technology

IoT Frequency Identification

LTE-M deployments

LTE-M operators	LTE-M deployment Countries
AIS	Thailand
America Movil	Mexico
APTG, Chunghwa Telecom	Taiwan, Province of china
AT & T	Mexico, USA
BEll, Rogers, Telus	Canada
Dialog Axiata	Sri Lanka
Etisalat	UAE
KDDI Corporation, NTT DOCOMO, Softbank	Japan
Korea Telecom	South Korea
KPN, Verizon	The Netherlands
NTT DOCOMO	Belgium
Orange	France , Romania
SingTel	Singapore
Spark, verizon	New Zealand
Swisscom	Switzerland
Telecom Italia	Argentina
Telefonica	Brazil, Germany
Telenor	Denmark, Norway
Telstra	Australia
Turkcell	Turkey
Verizon	North America

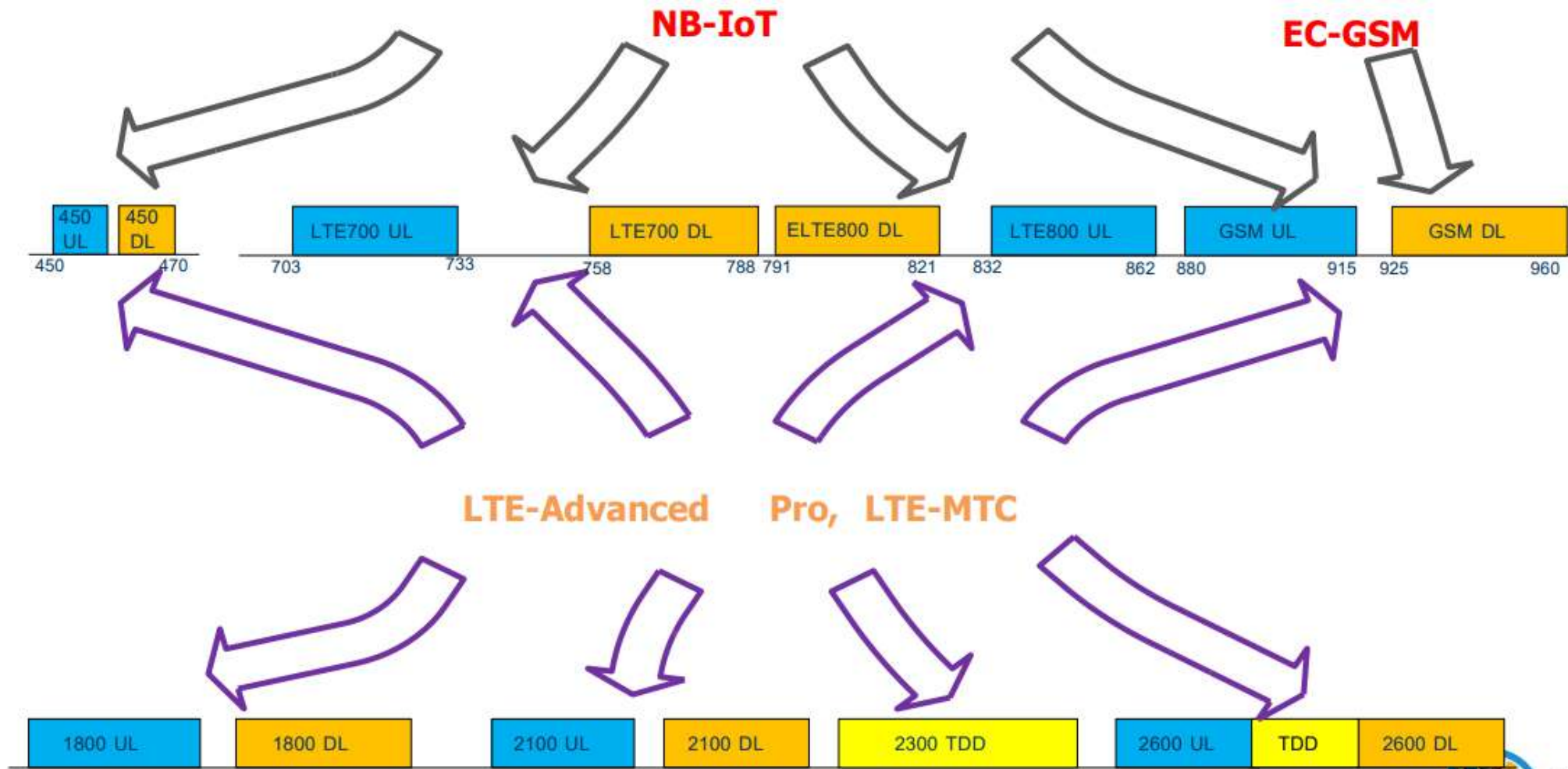
IoT Spectrum Identifications

Short Range IoT Applications frequency

Technology	Frequency	IoT Applications
Zigbee	915 MHz, 2.4 GHz	General (Smart Home/Commercial buildings)
Z-Wave	2.4 GHz	
Bluetooth	2.4 GHz	
Wifi	2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz and 5.9 GHz	
Wireless HART	2.4 GHz	IIoT
ISA 100.11a	2.4 GHz	
MBAN	2360–2400 MHz	Medical
WBAN	2.4 GHz	
WAIC	4200–4400 MHz	Avionics

IoT Spectrum Identifications

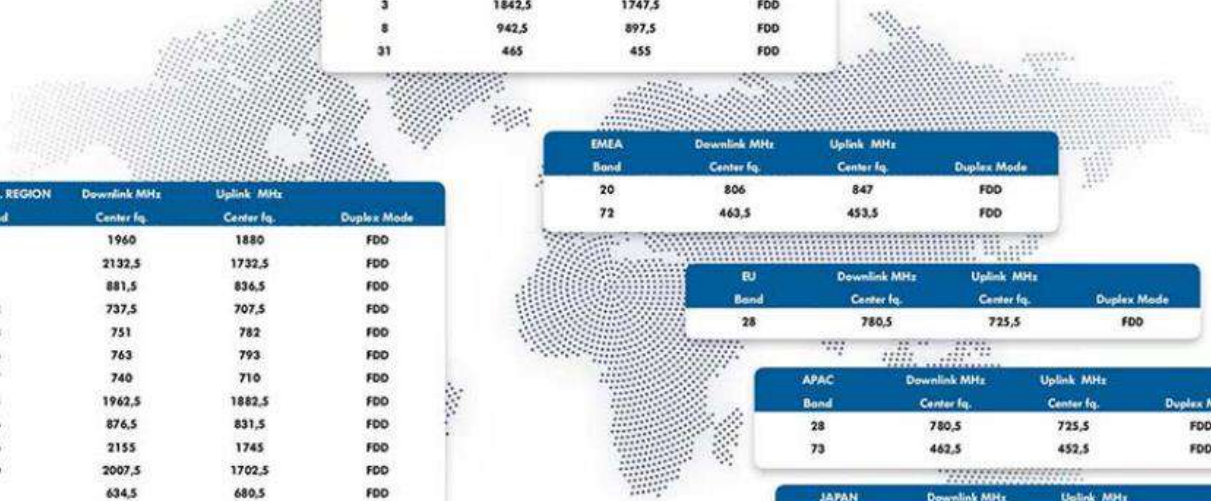
IoT deployments in Licensed Spectrum - IMT



IoT Spectrum Identifications

NB-IoT Frequency Bands

NB-IOT FREQUENCY BANDS



GLOBAL				
Band	Downlink MHz Center fq.	Uplink MHz Center fq.	Duplex Mode	
1	2140	1950	FDD	
3	1842,5	1747,5	FDD	
8	942,5	897,5	FDD	
31	465	455	FDD	

NORTH AM. REGION				
Band	Downlink MHz Center fq.	Uplink MHz Center fq.	Duplex Mode	
2	1960	1880	FDD	
4	2132,5	1732,5	FDD	
5	881,5	836,5	FDD	
12	737,5	707,5	FDD	
13	751	782	FDD	
14	763	793	FDD	
17	740	710	FDD	
25	1962,5	1882,5	FDD	
26	876,5	831,5	FDD	
66	2155	1745	FDD	
70	2007,5	1702,5	FDD	
71	634,5	680,5	FDD	
74	1496,5	1448,5	FDD	
85	737	707	FDD	

EMEA				
Band	Downlink MHz Center fq.	Uplink MHz Center fq.	Duplex Mode	
20	806	847	FDD	
72	463,5	453,5	FDD	

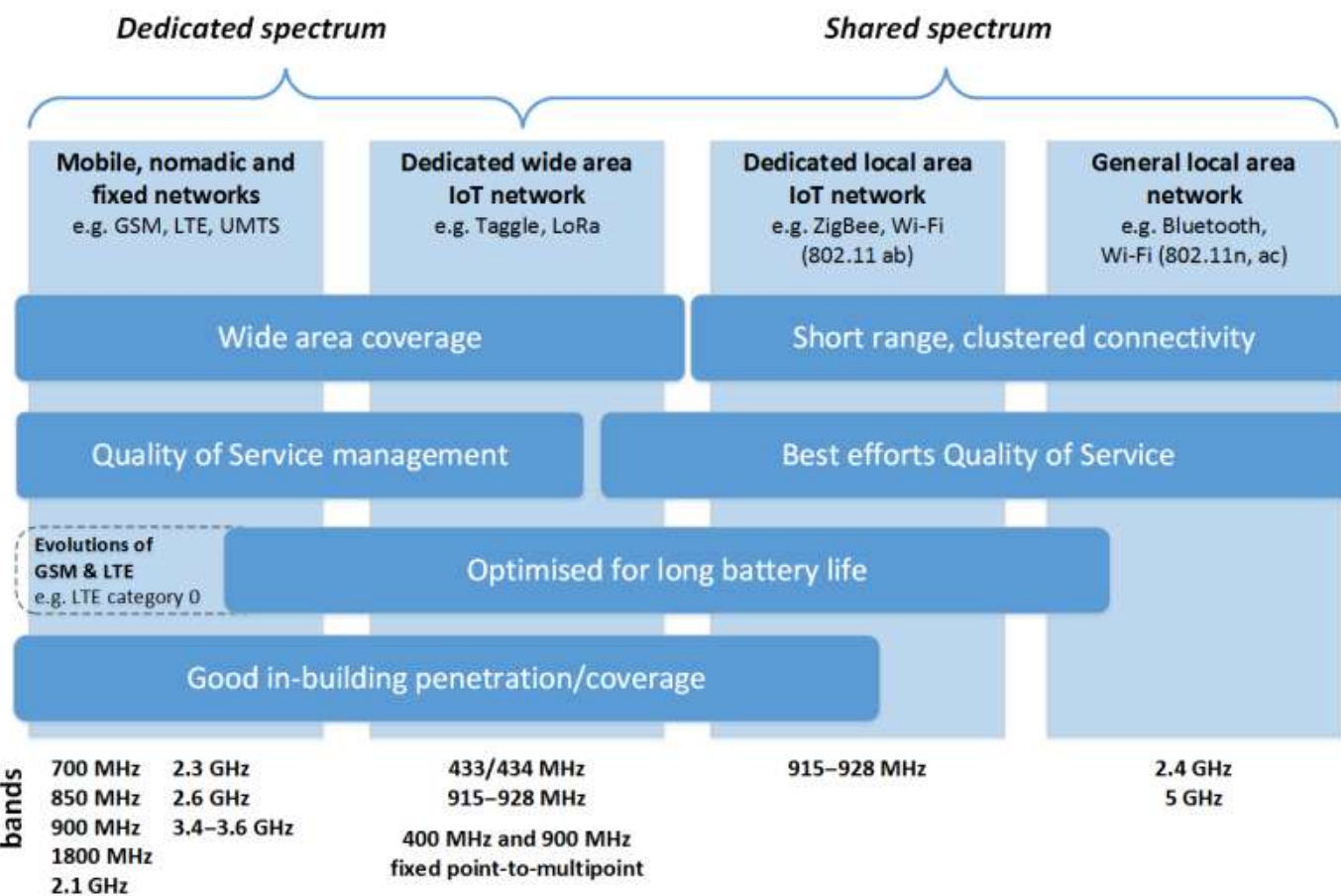
EU				
Band	Downlink MHz Center fq.	Uplink MHz Center fq.	Duplex Mode	
28	780,5	725,5	FDD	

APAC				
Band	Downlink MHz Center fq.	Uplink MHz Center fq.	Duplex Mode	
28	780,5	725,5	FDD	
73	462,5	452,5	FDD	

JAPAN				
Band	Downlink MHz Center fq.	Uplink MHz Center fq.	Duplex Mode	
11	1485,9	1437,9	FDD	
18	867,5	822,5	FDD	
19	882,5	837,5	FDD	
21	1503,4	1455,4	FDD	

IoT Spectrum Identifications

Available Spectrum for IoT applications



Note*. Example bands marked with * are available on a national basis.

Source: Radio Spectrum Policy Group. A Spectrum Roadmap for IoT

Dedicated spectrum

There is a regulation of which devices and device types can access and use the spectrum

It is well suited to wide area IoT applications with a required high quality of services

Shared spectrum

No regulation related to which devices and device types are sharing access to the same spectrum band based on approved access protocols from industry

It is well suited to low power, short range IoT uses with a required local clustered connectivity around an individual, office, premises, vehicles, vessels etc.

IoT Spectrum Identifications

Mobile IoT

Mobile IoT is the only standard for LPWAN defined in 3GPP

- It is not proprietary and only operates in licensed spectrum
- unlicensed spectrum can be used in other countries for other purposes without notice

IoT Spectrum Identifications

Technology innovations driving new spectrum demand

IMT applications using 5G now compete with incumbent services in low-, mid-, and high-band spectrum

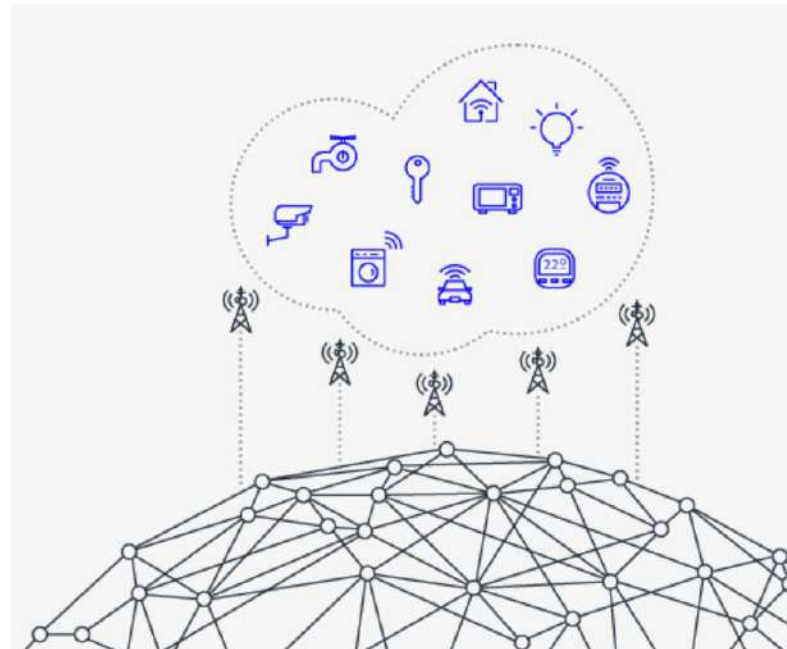
- The most common frequency bands for mobile networks to date have been focused on low- and mid-band spectrum, interest in the use of the high-bands for 5G, such as millimetre wave (mmWave) **between 24 GHz and 86 GHz**, has put them in focus as well
- Interconnected devices operating through applications like Bluetooth and Wi-Fi have proliferated, further increasing competition for valuable and finite spectrum
- Applications such as HAPS and NGSO satellites have also increased the pressure to access spectrum in different bands

This increased demand makes efficient spectrum use even more important

IoT Roaming

Roaming for IoT Devices

- Roaming enables IoT devices to connect to networks outside their home network's coverage
- IoT Roaming agreements between network operators facilitate this.



IoT Roaming

- Roaming enables IoT devices to maintain connectivity and functionality across different networks and geographical areas
- The term Roaming is usually used in cellular communication
- IoTs are based on several different technologies
- IoT based on cellular technologies would be a small portion of the total IoT market

IoT Roaming are critical for the successful operation of IoT devices in various applications, including logistics, asset tracking, smart cities, and more

IoT Roaming Requirement

Roaming Agreements between operators in order to define the terms, conditions, and pricing for IoT roaming allow devices from other networks to access their services

Involves

- **Data Billing and Pricing;** different pricing models, such as flat rates, volume-based, or event-based billing IoT devices need to be configured to handle the billing and pricing structures of the visited network
- **Regulatory Compliance** with international regulations and standards when crossing national borders.

Consider

- **Security and Authentication**
IoT devices must authenticate themselves to the visited network securely, and encryption should be used to protect data

Specify

- **Quality of Service (QoS)** levels provided to roaming IoT devices for the data transfer rates and latency factors

Mobile IoT (LPWA) Roaming

Mobile IoT (LTE-M & NB-IoT) are the only true LPWA Roaming networks

- As part of the Global Cellular Network family it offers the same benefits of security, billing and control through a SIM that you get with 2G/3G/4G/5G
- Enables a mobile subscriber to LTE-M or NB-IoT networks to seamlessly connect their IoT devices, and access associated IoT services, across several countries and/or mobile networks, using the SIM from the same service provider,
- Enables Connections also when the IoT devices move outside the geographical coverage area of their home network

Mobile IoT (LPWA) Roaming is technically enabled by inter-operator mobility management, authentication and billing procedures

Establishing roaming between network operators is based on the commercial terms contained in dedicated roaming agreements

IoT Roaming

Cellular Networks

Many National Regulatory Authority are working on or have regulations related to cellular technology based IoTs

- These IoTs may have a regular SIM card or may have an embedded SIM
 - Embedded SIM cards (eSIM) offer flexibility for IoT devices to switch between different networks without the need to physically replace SIM cards (This simplifies roaming for IoT devices)
- There is a need to look at the issue of roaming in a more comprehensive manner in general context of regulations related to IoTs

IoT Roaming

Other Technologies

LoRa, Sigfox networks may also require similar roaming agreements

- This may require agreements between Sigfox or LoRa network operators
- Such time of roaming for the time being has not caught the attention of regulators but with may require handling in the future.

IoT Roaming in Africa

Mobile connectivity in Africa continues to be the fastest-growing consumer market in the world. However, **IoT roaming is still emerging**

For companies opting for IoT roaming in Africa, controlling mobile data connectivity packages is critical

Global roaming data Sims also don't always perform as well in Africa

The dream of a global Sim that performs well in every country, with every type of hardware and at low data costs is not real

IoT Regulations

NB-IoT & LTE-M Equipment

In terms of IoT equipment, GSA has identified a significant rise in both the number and range of devices supporting 3GPP IoT standards since September 2022:

➤ 1,366 devices supporting either Cat M1, Cat NB1 (NB-IoT) or Cat NB2

Within that total:

- 534 devices support Cat NB1
- 156 identified device models support Cat-NB2
- 676 devices support Cat-M1

IoT Regulations

Regulating the Internet of Things

Self-regulatory regimes inspired (or not) by safety standards are gradually being replaced by country-specific regulations imposing security implementation requirements

Based only on the current legal requirements, the minimum level of requested cybersecurity for vendors and manufacturers is attainable

But regulatory compliance on basic security for individual IoT devices is just the first step

Network operators need to take additional actions. They can implement more high-level cyber-security and solutions that go beyond the performance of individual devices to address the IoT more holistically and comprehensively

Compliance with technical regulations is, by nature, mandatory. Conformity with standards is voluntary

IoT Regulations

Understanding the IoT regulations

The rapid growth of IoT adoption and the persistent insecurity of many devices set the stage for regulatory actions

- In 2019, lawmakers started regulating the Internet of Things, especially network and device security

Today, the challenge lies more in understanding which regulations apply or will apply and whether or not IoT regulatory compliance is enough to provide adequate security

There's a misconception that the IoT is a largely unregulated, While it's true that legislators have struggled to keep up with innovation in the past, today, **the IoT regulatory environment has matured**. But here is the tricky part.

- Lawmakers regulating the IoT industry are facing two distinct challenges:
 - Make connected devices more resilient to cyber threats and attacks (IoT cybersecurity)
 - Protect the privacy of personal information (IoT privacy)

Aspects of an IoT deployment may then be subject to many different forms of oversight

- In Europe, for example, **data created and transmitted via IoT devices** may be subject to the [General Data Privacy Regulation \(GDPR - effective May 25 2018\)](#).

The **infrastructure** may be covered by the [Network and Information Security Directive \(NIS – effective May 24 2018\)](#) and the **business** by the [EU's Cybersecurity Act](#) (effective June 27 2019)

Most recent regulation frameworks impacting the IoT in Europe and the United States (June 2021)

Region	Consumer Data Privacy	Cybersecurity
EU	<p>The General Data Protection Regulation (EU GDPR Directive 95/46/EC) effective May 25 2018, became law in the EU and the UK.</p>	<p>The EU Cybersecurity Act Effective June 27 2019, and became law in the European Union and the UK. The NIS Directive (IoT infrastructure) became effective May 24 2018, in the EU and the UK. Each country will have to pass a law.</p>
USA	<p>No comprehensive federal law regulating the collection and use of personal information yet. Specific laws:</p> <ul style="list-style-type: none">•Healthcare: Health Insurance Portability and Accountability Act•Finance: Gramm-Leach-Bliley Act•Government agencies: US Privacy Act of 1974•Children’s Online Privacy Protection Act	<p>The IoT Cybersecurity Improvement Act of 2020, signed by President Trump on December 4 2020 The bill gives NIST, the National Institute of Standards and Technology, the authority to manage IoT cybersecurity risks for devices acquired by the federal government.</p>
California	<p>The California Consumer Privacy Act The California Privacy Rights Act SB-1121 became effective on January 1 2020 CPRA will be enforced on July 1 2023</p>	<p>The California IoT cybersecurity law SB-327 became effective on January 1 2020</p>

IoT Regulations

More resources on cybersecurity IoT standards and recommendations

“Most regulations stay focused on the privacy aspects of IoT. This is changing, and, as it takes 18-24 months to design a new IoT device, it would be a blunder to design now without having future regulations in mind.”

- Australia’s [Draft Code of Practice for Securing the Internet of Things for Consumers](#)
- The UK [Code of practice for Consumer IoT Security](#)
- The UAE IoT framework from the [PWC](#) website
- The UK government [press release](#) on requirements for IoT device manufacturers (January 2020)
- GSMA IoT [Security Guidelines](#)
- October 2020: Data privacy [predictions for 2021](#)
- December 2020: [CPRA explained](#)
- Center for Internet Security: [Cybersecurity best practices](#)
- [FCC regulations](#) (Federal Communications Commission)
- The [CE marking and IoT products](#)
- [The Federal Financial Institutions Examination Council](#) (FFIEC)
- Thales’ [IoT security solutions](#)