

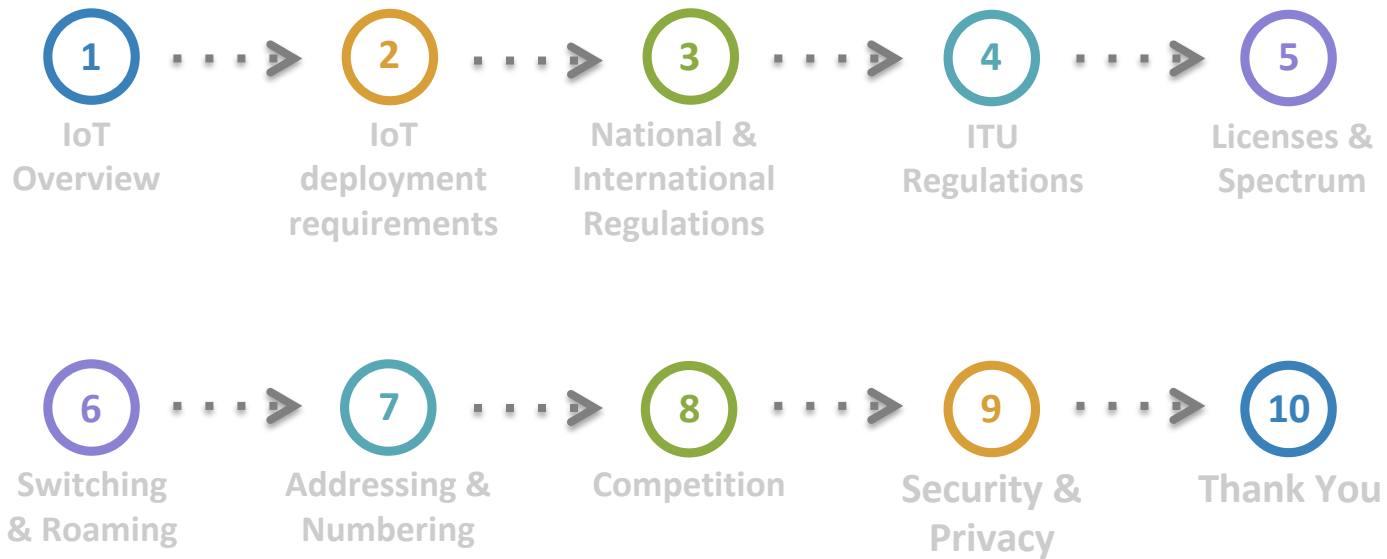
Regulations Internet Of Things (IoT)

Prepared:
Hatim Alhaqbani

Supervised:
Dr. Saud bin Saeed



Agenda





“

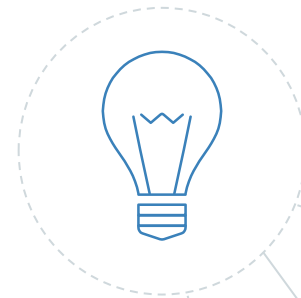
Abbreviations:

- Internet of Things (**IoT**)
- Electromagnetic compatibility and Radio spectrum Matters (**ERM**)
- Short Range Devices (**SRD**)
- Machine- to- Machine (**M2M**)
- Low Power Wide Area Networks (**LPWAN**)
- Mobile Network Operators (**MNO**).
- quality of service (**QoS**)
- Global System for Mobile Communications(**GSMA**)
- International Mobile Subscriber Identifier (**IMSI**)



What is IoT?

- It refers to the use of intelligently connected devices and systems to leverage data gathered by embedded sensors and actuators – GSMA
- It is the interconnection of multiple M2M applications often enabling the exchange of data across multiple industry sectors - Ofcom
- It is the interconnection via the internet of computing devices embedded in everyday objects enabling them to send and receive data – Oxford Dictionary
- This tremendous evolution opens up the doors for great opportunities and also poses challenges that need to be overcome if we want to benefit the most from IoT



Evaluation Of The World Wide WEB :

Web 1.0 : WWW

Characterized by separate static websites.

➤ Publication

Web 2.0 : Social web

The movement away from static webpages to dynamic + shareable content, social networking, + online collaboration.

➤ Interaction

Web 3.0 : Semantic web

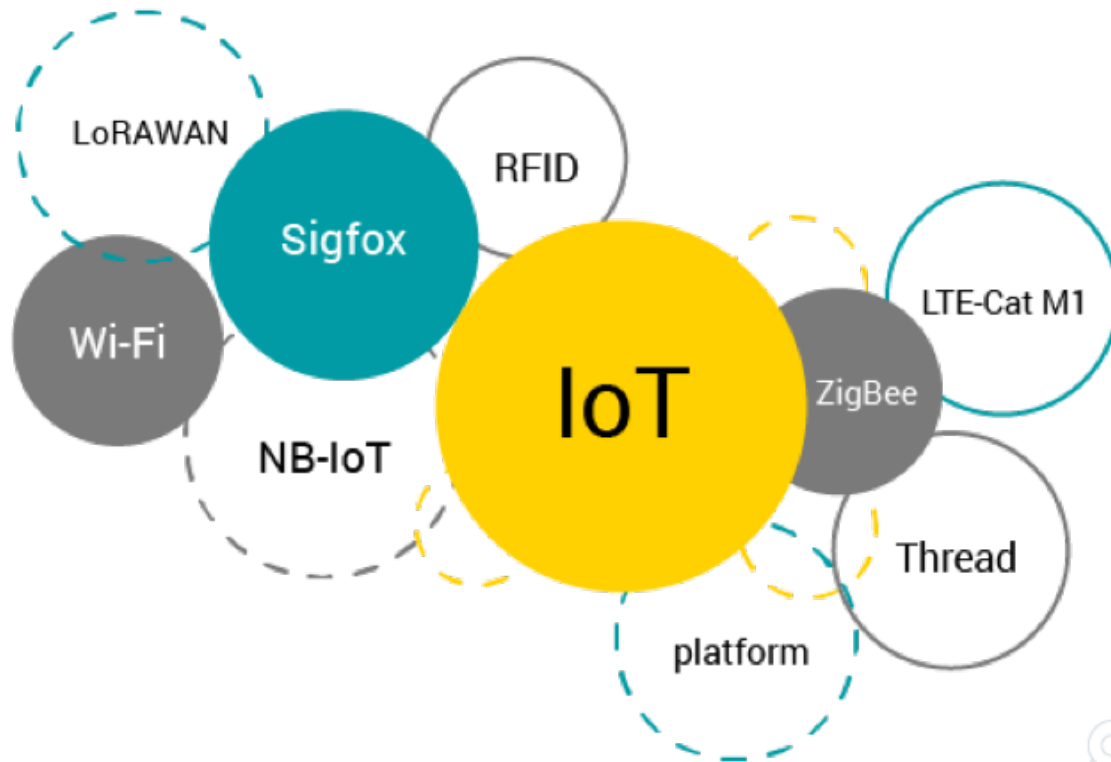
Usually conjectured to include semantic tagging of content.

➤ Interoperation +
IoT

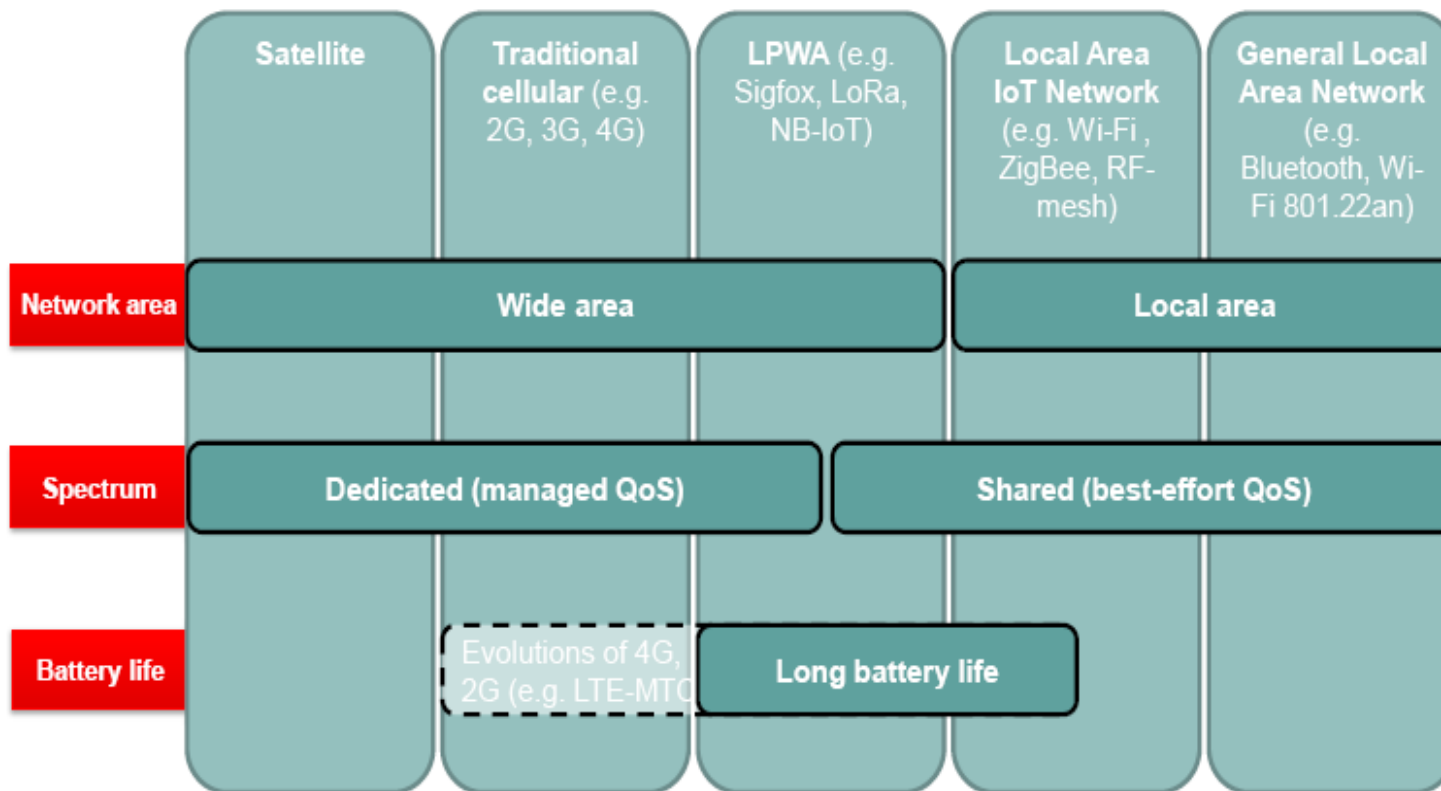
Web 4.0 : Intelligent web

It achieves a critical mass of participation in online networks

IoT communication technologies



Technology group dimensions:



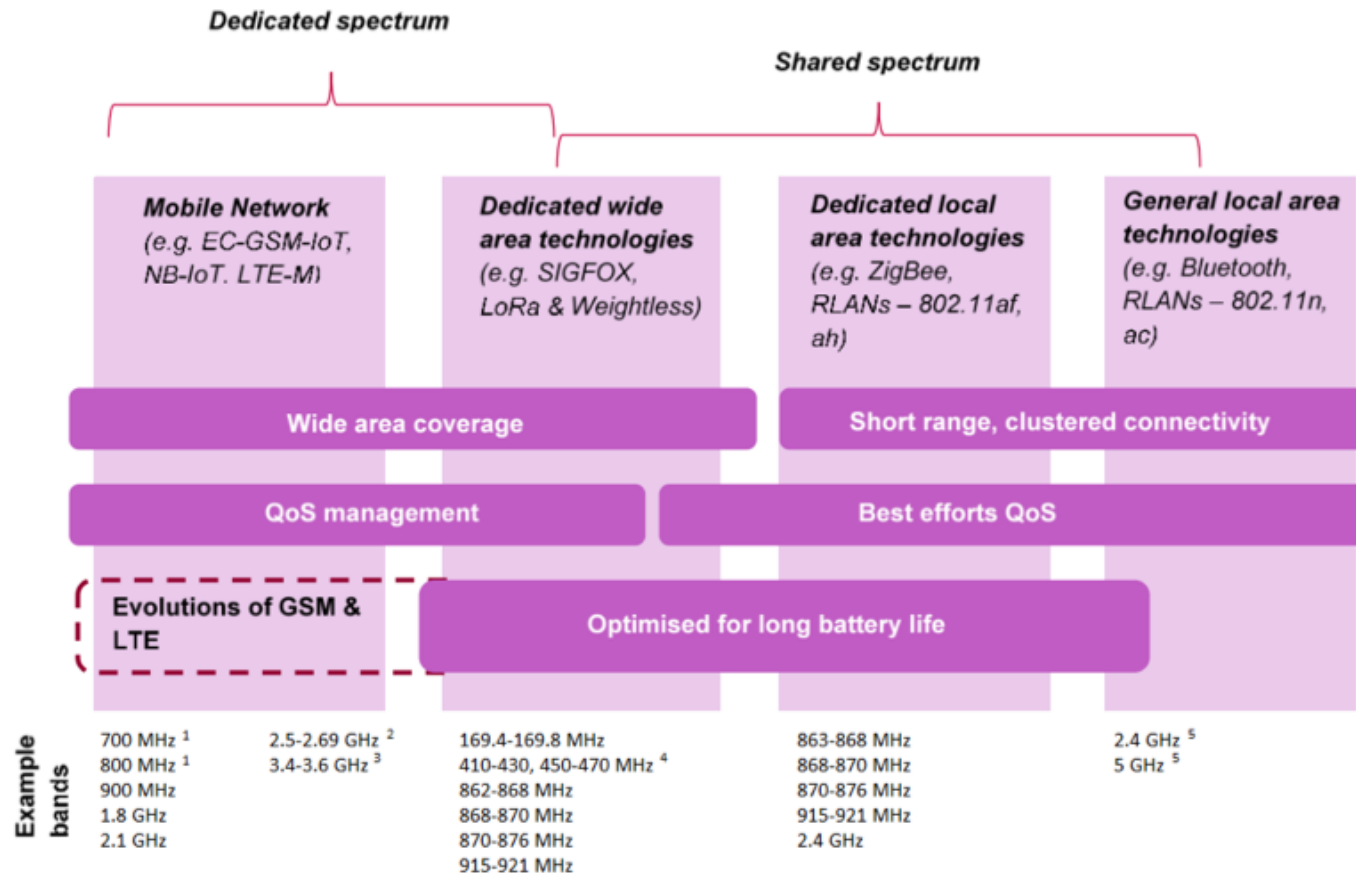
Technology group dimensions :

	Satellite	Traditional cellular (e.g. 2G, 3G, 4G)	LPWA (e.g. Sigfox, LoRa, NB-IoT)	Local Area IoT Network (e.g. Wi-Fi, ZigBee, RF-mesh)	General Local Area Network (e.g. Bluetooth, Wi-Fi 801.22an)
Connectivity cost	High	2G: Medium 3G: Medium 4G: Medium	Low	Low	Low
Module cost	High	2G: Low 3G: Medium 4G: High	Low	Low	Low
Typical bandwidth	Low to high	2G: Low 3G: Medium 4G: High	Low	ZigBee: Low RF-mesh: Low Wi-Fi: High	Bluetooth: Low Wi-Fi 801.22an : High

Technology group dimensions :

- Spectrum used in IoT solutions can be dedicated (Licensed) or shared (unlicensed) ..

Spectrum for IoT		
Characteristic	Dedicated	Shared
QoS	Supported	Not supported
Cost	Higher	Lower
Time to market	Slower	Faster



Note 1: There are plans to open the 700 MHz and 800 MHz (Digital Dividend bands)

Note 2: The 2.500 - 2.690 GHz bands is open for IMT-2000 and other compatible technologies for the provision of Broadband Wireless Access (BWA) services.

Note 3: The 3.4 - 3.6 GHz band is open for BWA systems.

Note 4: The band 410 - 430, 450 - 470 falls within frequency band currently allocated to PMR / telemetry system.

Note 5: The 2.4 and 5 GHz frequency band already open and used for Bluetooth / WLAN systems.

Policy and regulatory enablers



IoT definition in the policy and regulatory context :

- Internet of things (IoT) [ITU-T Y.2060]: A global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable information and communication technologies
- NOTE 1 (from [ITU-T Y.2060]) – From a broad perspective, the IoT can be perceived as a vision with technological and societal implications.
- NOTE 2 (from [ITU-T Y.2060]) – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.



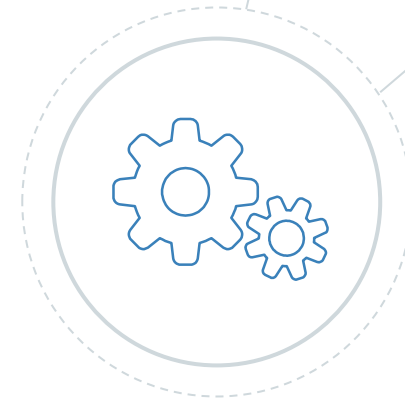
IoT deployment requirements

- Availability of appropriate spectrum ,
- communication networks with universal coverage,
- confidence in security and privacy of transactions in communication networks ,
- IoT networks that can connect sensors and devices containing smaller computer chips and requiring less power than smartphones ,
- Affordable terminal equipment ,
- Addressing requirement for IoT devices : IPv6 .



” National Regulations

- There are many aspects of regulations that are national in nature Such as how to assign spectrum to telecommunication operators, decision to have national level licensing or region based licensing and many others
- Even national regulations have to be aligned to best practices to avoid issues such as cross border interference, technology neutrality, roaming, fee structure, etc.
- Governments generally have lots of freedom in adopting national regulations.
- It is, however, always advisable to follow best practices. ITU has published many document that can be used to have an idea about best practices



International Regulations

ITU-T Activities on IoT & Smart Sustainable Cities

ITU-T Study Group 20

Development and implementation of standards

United for Smart Sustainable Cities (U4SSC)

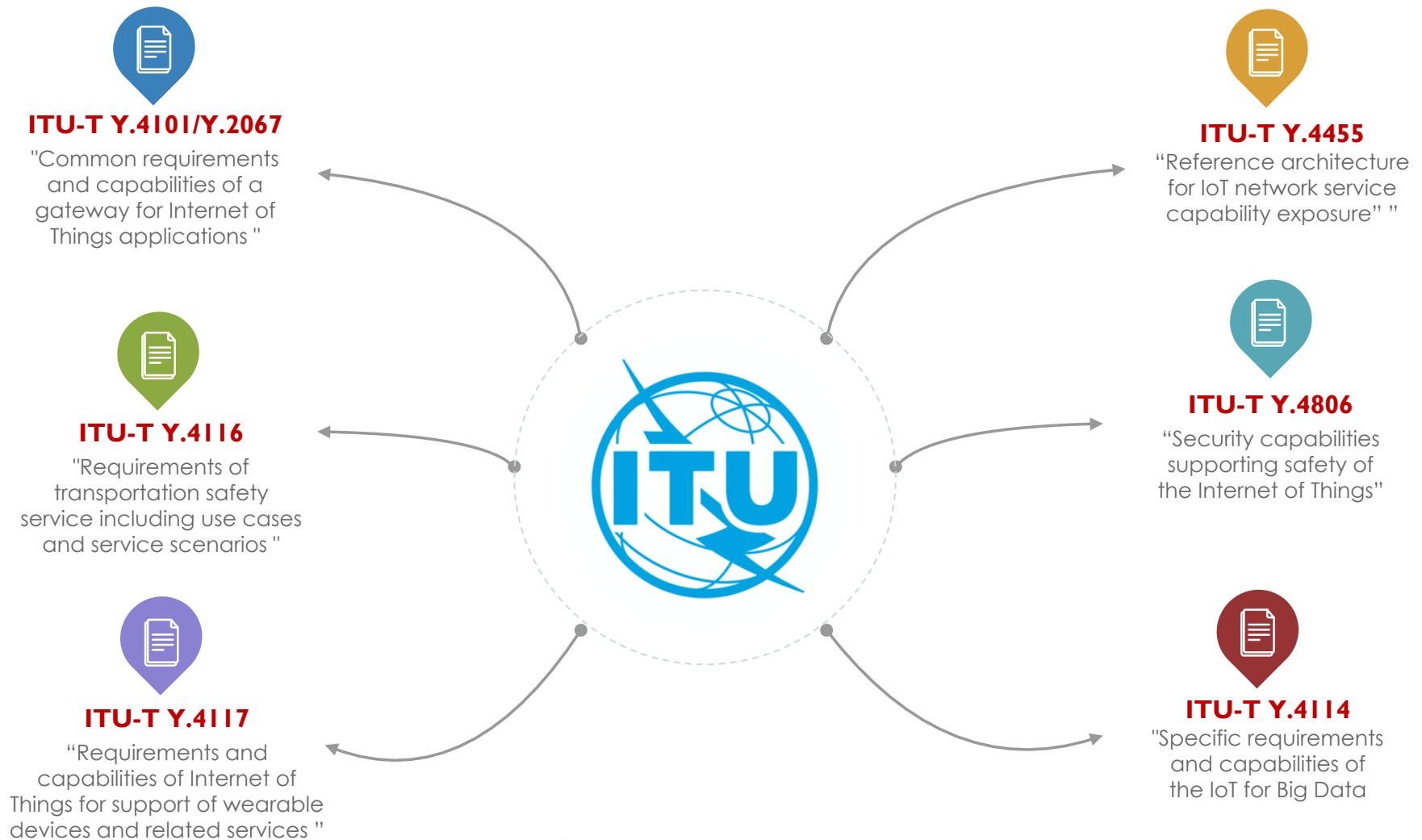
Open platform for knowledge sharing & Forward looking research

Focus Group on Data Processing Management (FG-DPM)

Research & pre standardization work.



Most recent approved ITU-T Recommendations



REGULATORY ISSUES

Policy and regulatory measures taken:

01

Licensing and spectrum management

02

Switching and roaming

03

Addressing and numbering

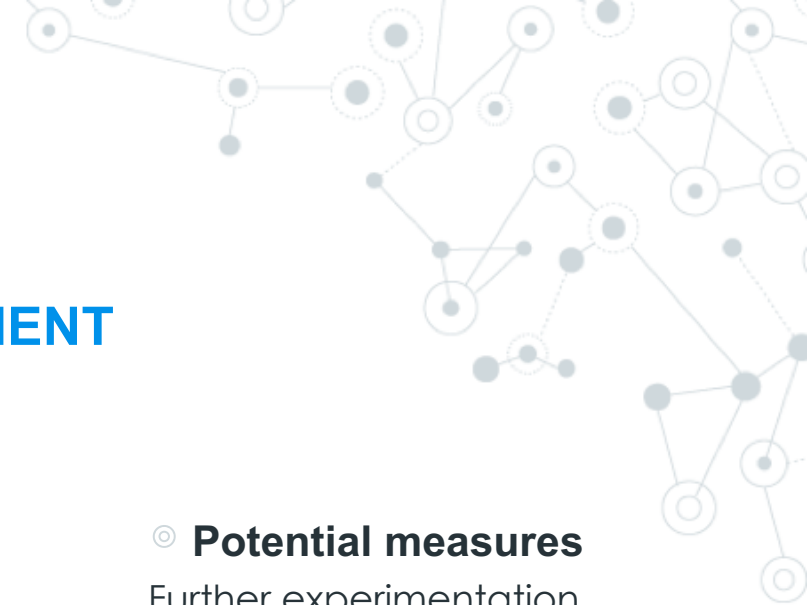
04

Competition

05

Security and privacy





LICENSING AND SPECTRUM MANAGEMENT

◎ **Goal**

Ensure spectrum is available for a wide range of IoT applications, at short and long range, in licensed and unlicensed bands. Addition, depends on Long range (NB-IOT, Sigfox, LoRA) Vs short range (RFID, Bluetooth, WiFi).

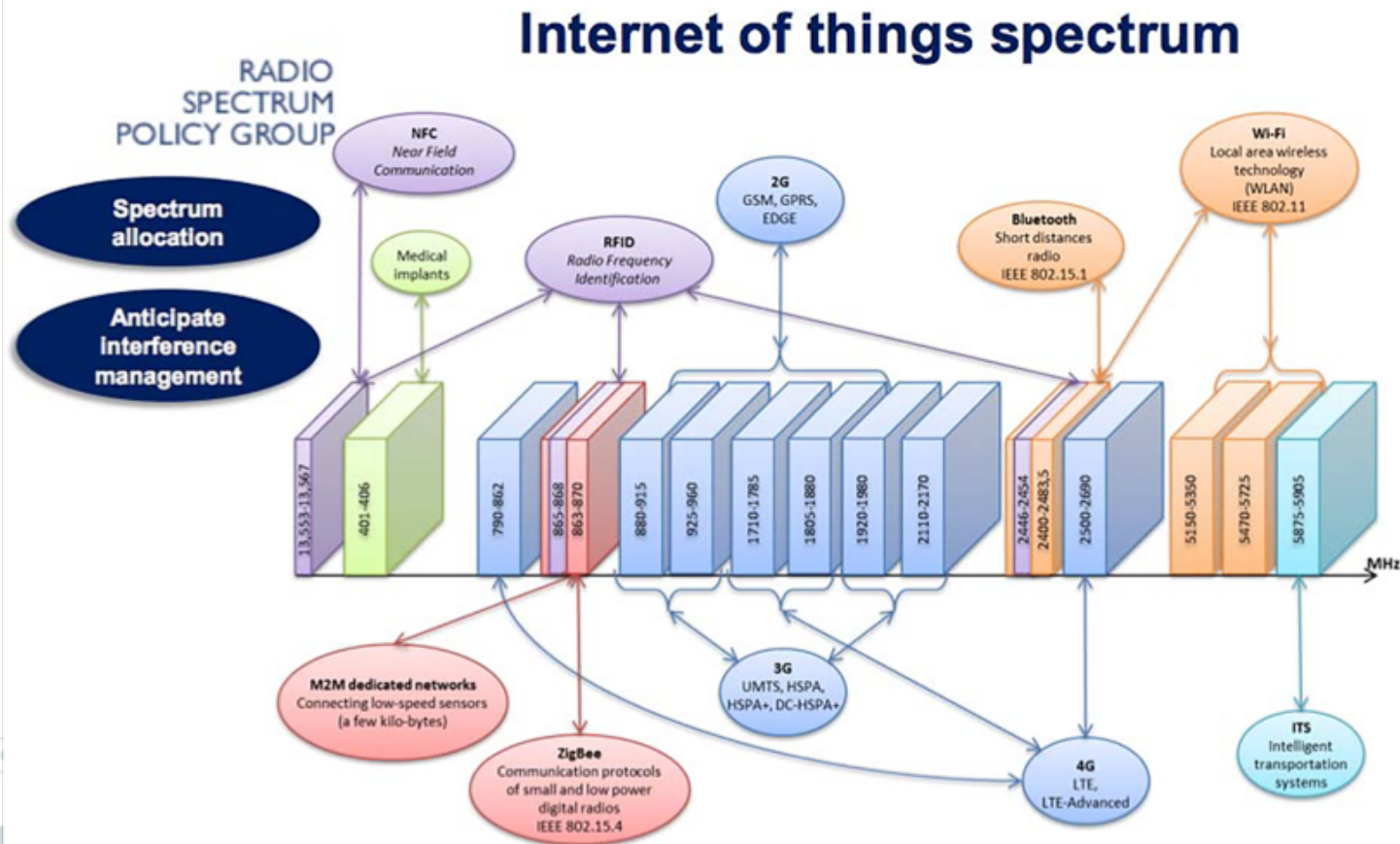
◎ **Best practice**

Monitor availability of spectrum for short and long-range IoT communications and backhaul network capacity. Encourage 4G deployment and use of small-cell technology.

◎ **Potential measures**

Further experimentation with use of white space and shared-space technology. Encourage development of LTE-A and 5G networks, and keep need for IoT-specific spectrum under review.

LICENSING AND SPECTRUM MANAGEMENT



PRACTICES

LICENSING AND SPECTRUM MANAGEMENT

❑ CITC (Saudi Arabia) :

- The license- exempt LPWANs use shared spectrum with other users, thus, there is no frequency license required from the CITC.
- The frequency bands can only be used as a secondary use, thus, the networks operating in these bands must not cause any interference to the current or future primary users. The users of these networks must not ask any protection from interference caused by the current or future primary users.

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission



PRACTICES

LICENSING AND SPECTRUM MANAGEMENT

❑ OFCOM (UK) :

- The frequency ranges are available for IoT applications on a license exempt basis except for those below 800MHz which are available through a Business Radio Internet of Things license.



PRACTICES

LICENSING AND SPECTRUM MANAGEMENT

❑ SKMN (Malaysia)

- MCMC allocated 4 MHz of spectrum in the frequency band 919-923 MHz for the use of Short Range Device (SRD) as addition to bands 433-435 MHz, 2.4 GHz and 5.8 GHz that can be used for IoT applications.



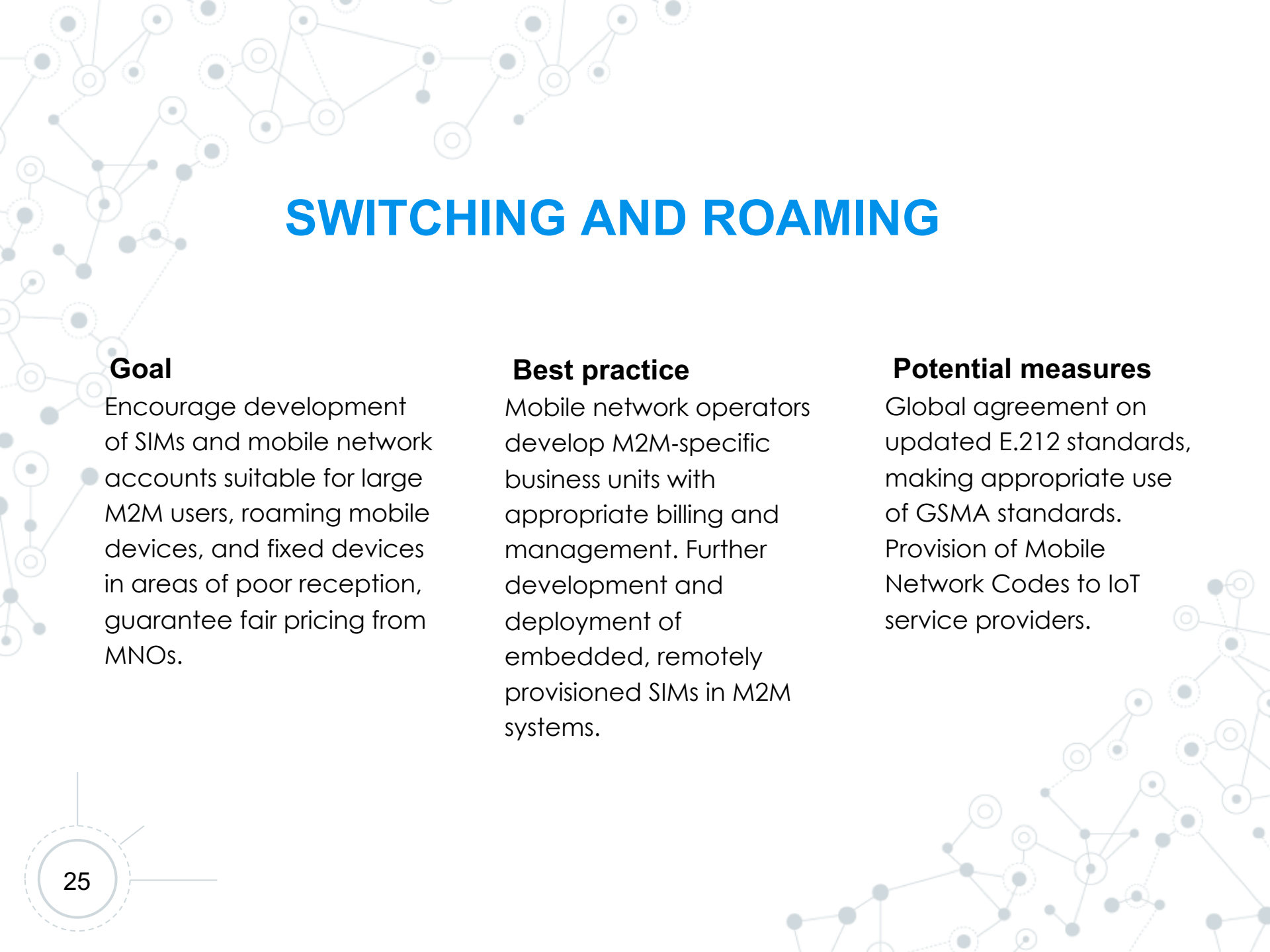
Suruhanjaya Komunikasi dan Multimedia Malaysia
Malaysian Communications and Multimedia Commission

SWITCHING AND ROAMING

❑ Challenge:

- It's difficult operating large networks of M2M devices via mobile telephony networks, with a fixed SIM in each device, may not find it easy to switch network at the end of a contract, or if a device roams into a different network area or for some time period could get better service from a different provider.
- The MNOs don't make distinction between traditional roaming traffic and IoT roaming traffic, that caused a challenge in implementing IoT roaming lays in deciding on the appropriate pricing for the service.

❑ Roaming service enables users to continue using their existing mobile services while travelling abroad.



SWITCHING AND ROAMING

Goal

Encourage development of SIMs and mobile network accounts suitable for large M2M users, roaming mobile devices, and fixed devices in areas of poor reception, guarantee fair pricing from MNOs.

Best practice

Mobile network operators develop M2M-specific business units with appropriate billing and management. Further development and deployment of embedded, remotely provisioned SIMs in M2M systems.

Potential measures

Global agreement on updated E.212 standards, making appropriate use of GSMA standards. Provision of Mobile Network Codes to IoT service providers.

ADDRESSING AND NUMBERING

Challenges:

The increased volume of IoT devices will drive up demand for numbering resources
Enabling peer-to-peer connections between devices required a large address space to individually identify each one.

The number of unallocated addresses for the current version of the Internet Protocol (IPv4) is extremely limited.

Goal

Large address space needed for globally addressable things (although many IoT devices only need local connectivity).

Best practice

- Deployment of IPv6 by ISPs, public and private sector organizations.
- Use of IMSI for M2M applications, which it has the advantage of a well-developed authentication, payment and global roaming framework, operated by mobile telephony providers, with hardware security based on SIMs.

Potential measures

Universal IPv6 adoption by governments in their own services and procurements, and other incentives for private sector adoption.



COMPETITION

Goal

Avoid IoT user lock-in and new barriers to entry.

Best practice

Ensure competition regulators have capability to monitor IoT markets for abuses of dominant positions. Provide institutional mechanism for ongoing review of laws and regulations for impact on IoT competitiveness.

Potential measures

Consider measures to increase interoperability through competition and consumer law. Give users a right to easy access to raw data. Support global standardization and deployment of remotely provisioned SIMs for greater M2M competition.

SECURITY AND PRIVACY

Challenges:

Without adequate security, intruders can break into IoT systems and networks, accessing potentially sensitive personal information about users, and using vulnerable devices to attack local networks and devices.

Goal

- Significantly reduce security vulnerabilities in IoT systems let attackers access private data and cause physical harm in cases such as medical devices and connected vehicles.
- Encourage security and vulnerability patching of devices.
- Reduce potential for discrimination in employment, financial and healthcare services.

Best practice

Ensuring security and privacy from outset of IoT system design process. Development of co-regulation by all stakeholders to protect security and privacy. Further development of privacy and consumer protection rules to ensure security testing of IoT systems that process sensitive personal data.



THANK You ..