2020

Consultation Paper

Preparation of Regulatory Framework for Internet of Things (IoT) in Pakistan

Strategy & Development Division

Pakistan Telecommunications Authority

Contents

1. Preamble

Internet of Things (IoT) is the fastest growing phenomena worldwide with certain countries having implemented it with light touch regulations. With the rapid growth in demand and use cases of IoT, it is foreseen that in the coming 10-15 years, IoT will saturate into all dimensions of human lives and will have impact on the industry and the economy at large. As IoT is NOT about which protocol or which platform or which cloud is used, however it is about sharing the information among different systems, different applications, and different business sectors.

It is vital to have a regulatory framework in place, well in time, for IoT so that complete benefits of this innovation can be passed on to the citizens. The stepwise growth of this sector will demand cross sector policies and a comprehensive regulatory framework. The deployment of IoT systems in multiple sectors, and their potential impact on individuals and businesses, raises regulatory requirements such as licensing, numbering and addressing, spectrum management, network standards, QoS, data protection, privacy and security etc. Such requirements can be sector specific or cross-sector in nature.

Therefore, Government / regulator has a major role to play in shaping market rules for convenient and smooth IoT adoption, such as appropriate licensing /registration and industry / business friendly regulations etc. The focus of the Authority is to have an enabling and comprehensive regulatory framework to create sustainable IoT development and associated deployments. Moreover, regulatory guidelines are also needed to be set forth for data collection, data analysis, data sharing, use of IoT data, data privacy, data security etc. In addition, rules are required to be established about liability and ownership, for all the sectors.

Currently, the regulatory frameworks for IoT services are in their early stages worldwide, with very few countries formalizing any specific roadmap. The issues and challenges while formulating regulatory framework involve licensing, spectrum and management of licensed as well as unlicensed bands, numbering plan, permanent roaming, quality of service, security, privacy, data protection, which are dealt in this paper.

1.2 Invitation for Comments

- The Authority would like to seek comments and views of the members of the PTA-Industry Working Group on IoT, the concerned industry and the general public, on the issues and challenges of IoT for formulation of regulatory framework for the country.

- Supporting material (if any) may be attached as Annexures.

- This consultation will be opened for a period of four (04) weeks, and will close by 12 noon on **November 5, 2020.**

- All the submissions must reach PTA by 1200 noon on **November 5, 2020**. Soft copy of the submission in both Adobe PDF and Microsoft Word format positively be provided through email at iot-wg@pta.gov.pk, with a copy to Director General (Strategy and Development) PTA HQs at imad@pta.gov.pk,

- The parties other than the members of the IoT- Working Group, submitting comments should include their personal / company particulars as well as the correspondence address, contact number and email address on the cover page.

- All the comments received would be analyzed and would be duly considered while preparing the regulatory framework of IoT in Pakistan.

2. Introduction

IoT is the convergence of Information Technology (IT) and Operational Technology (OT) i.e. IT supports connections to the internet along with related data and technology systems and is focused on the secure flow of data and its organization.

Operational Technology (OT) monitors and controls devices and processes on physical o peratioalsystems (assembly lines, utility distribution networks,
production facilities, roadway systems etc.

M2M and IoT are partially over lapping concepts and, in much of the literature, both terms are used as synonyms. The difference between the IoT and M2M is not universally agreed, however at the technical level, a partial distinction between the two is possible, the distinction as per the GSMA's view is that M2M typically refers to the connection between machines or devices, while IoT refers to the whole ecosystem, which includes the application, backend connectivity etc.

M2M is recently referred to technologies that enable communication between machines without human intervention. Examples include telemetry, traffic control, robotics, and other applications involving device-to-device communications. For example, in case of connected car, M2M would typically cover the elements where machines communicate with each other with little or no human intervention. Diagnostics, telematics and software updates typically only involve machines or devices making connections to each other.

Conversely, infotainment services or remote services, such as using a wireless device to find a car's location in a car park, typically involve a whole ecosystem of different services, including GPS and payments, as well as human interaction with the solution. This would therefore be classified as IoT solutions[1].

In M2M process, automatic interconnection of the devices takes place by connection to the Internet network. For this reason, M2M is often associated with the Internet of Things (IoT). Therefore, IoT could be viewed as M2M, but acting in a wider context / larger scale.

2.1. Definition of IoT

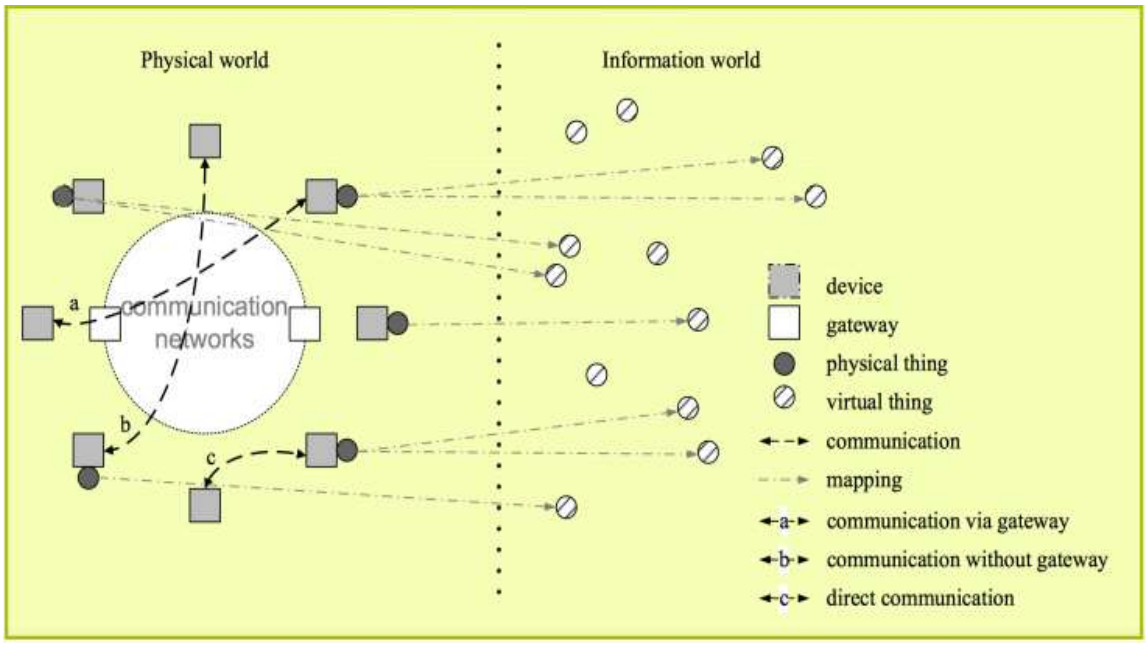
a) ITU [2] Definition of IoT

According to ITU, the IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and

[1] https: / /www.apt.int /SATRC-SAPVI
[2] Source: Recommendation ITU-T Y.2060

virtual) things based on existing and evolving interoperable information and communication technologies (ICT).

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."



Source: Recommendation ITU-T Y.2060

b) European Telecommunications Standards Institute (ETSI)

ETSI has defined M2M as 'Physical telecommunication-based interconnection for data exchange between two ETSI M2M compliant entities, like: device, gateways and network infrastructure.'

c) Organization for Economic Cooperation and Development (OECD)

According to OECD's report, the term M2M describes, "Devices that are connected to the internet, using a variety of fixed and wireless networks and communicate with each other and the wider world. They are active communication devices. The term is slightly erroneous though as it seems to assume there is no human in the equation, which quite often there is in one way or another.'

2.2. Fundamental Characteristics of IoT Networks

Few of the fundamental characteristics of IoT networks are as follows: -

a) Interconnectivity:

Anything in IoT can be interconnected with the global information and communication infrastructure.

b) Heterogeneity:

The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

c) Dynamic changes:

The state of devices change dynamically, e.g., sleeping and waking up, connected and /or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

d) Enormous scale:

The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected

to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device- triggered communication.

2.3. IoT Technical Solutions & Classification

Many short range and long-range technologies can be used to provide IoT services. The requirements, however, of a particular IoT service will determine its underlying spectrum requirements. Some of the technical standards have been highlighted below. Few new standards have also been added in the list and its is expected to be a continued process.

Short Range	Long Range	
• Wi-Fi • Bluetooth (classic and LE) • 6LoWPAN • Z-wave • Zigbee • ANT/ANT+ • Thread • NFC • RFID • EnOcean	Cellular • EC-GSM • LTE-M • NB-IoT	LPWAN • LoRaWAN • Weightless-N • Sigfox • Ingenu • Neul • N-Wave

a) **Short Range, Personal and Local Area Technologies:** Short range connectivity can be provided by conventional[3], general purpose technologies such as Wi-Fi or Bluetooth. These technologies may be particularly appropriate for consumer

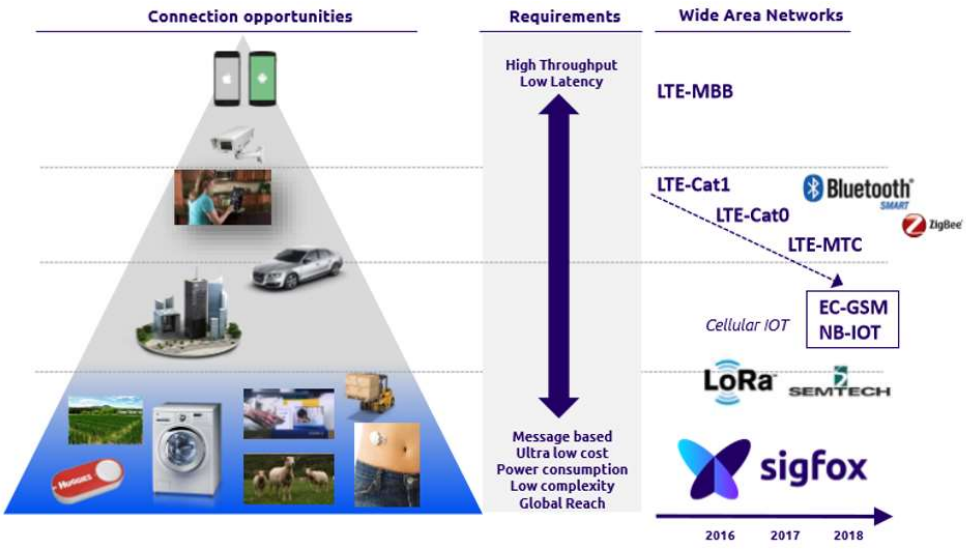
[3] https: / /berec.europa.eu /eng /document_register /subject_matter /berec /reports /5755-berec-report-on-enabling-the-internet-of-things

IoT services, such as health or fitness trackers. Optimized versions of Bluetooth and Wi-Fi are also emerging.

b) **Low Power, Wide Area Technologies**: LPWAN systems are mostly made to support massive IoT use cases with low throughput requirements. LPWAN offers a very compelling mix of long range, low power consumption and secure data transmission. When deployed using sub-1GHz spectrum, these technologies are capable of providing relatively wide area coverage. In addition, their protocols enable them to use either licensed or license exempt spectrum. LPWAN may operate under the regulations for short range devices (SRD). The LPWAN systems do not rely on a single technology, but a group of low-power, wide-area network technologies that may be proprietary or open standards. These new systems can help to address the challenges raised by the wide-ranging applications under development where numerous devices need only to transmit a few messages per day. These solutions have a number of common technical and operational characteristics that make them suitable for facilitating massive Machine Type Communications (mMTC) and Internet of Things (IoT) applications.

Some of examples / use cases of LPWAN Solutions are: Traffic and transportation system management, Water supplying system, Road lighting, Smart parking system, Pollution monitor, Waste bin management, Smart freight and inventory management etc.

APPLICATIONS AND NETWORKS



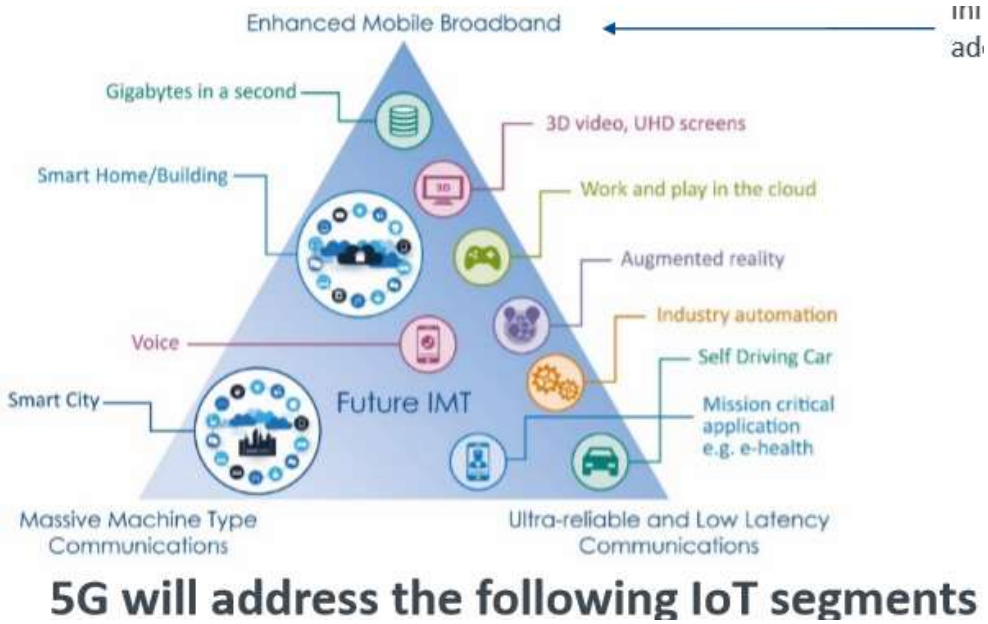
c) **Mobile technologies:** Existing mobile networks, such as GSM, have been used worldwide for several years to provide wireless point of sale applications. Various technical enhancements are being proposed which will enable mobile networks to support a wider range of IoT services more efficiently and allowing connectivity service providers to support these services using much of their existing infrastructure. These enhancements include an air interface capable of efficiently supporting IoT services within a 200kHz channel bandwidth called **NB-IoT** and IoT-optimized variants of the LTE standard used for 4G services. 5G networks will emerge to efficiently support a range of IoT services.

d) **IOT and 5G:** It's a general view around the globe that 5G has been specifically designed for IoT use (including ultra-reliable, low latency, low consumption and massive deployment). 5G will roll out much quicker than first predicted.

According to ETSI, 5G will address the following IoT segments:

- the Massive Machine Type of Communication (MTC) or Massive IoT, &
- Ultra-Reliability and Low latency Communication (URLLC) or Critical IoT.

Examples of Massive IoT include Smart Cities, Smart Homes / Buildings and Critical IoT includes, Gigabytes in Second, 3D video, UHD Scenes, Work and Play in cloud, Augmented reality, Industry Automation. Self-Driving Cars and Mission critical applications like e-health etc.

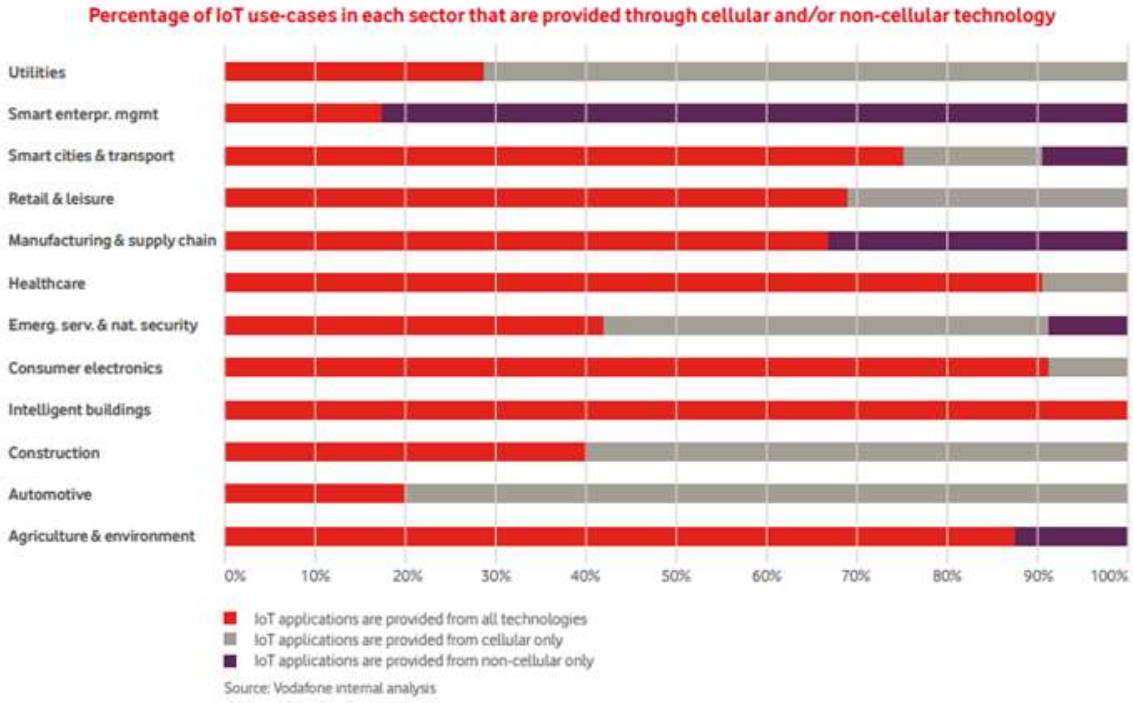


5G will address the following IoT segments

General Services Administration (GSA), US has identified[4] (217) operators (and operators-to-be), in (86) countries, investing in 5G mobile and 5G FWA networks, in the form of tests, trials, planned and pilot deployments, and launches. The numbers at the end of April 2018 were (154) operators in (66) countries. At least (94) projects had involved testing Massive MIMO in the context of 5G (i.e., MIMO trials involving (64) or more transmitters, or lower order MIMO used on new high frequency spectrum bands, or involving some other 5G aspect such as New Radio characteristics). At least (26) projects have been planned, explicitly featuring Network Slicing.

2.4. Cellular & Non-cellular Use Cases

Analysis of IoT connectivity technologies in Vodafone's analysis figure below shows, the percentage of IoT use-cases provided via cellular technology, via non-cellular technology or via both forms of technology, in to different sectors of life. The analysis shows that IoT has penetrated into almost all the sectors associated with life and interestingly in the majority of sectors, almost most all IoT use-cases can be implemented through the cellular as well as non-cellular connectivity technologies, in parallel.



[4] https: / /docbox.etsi.org /Workshop /2019 /201910_ETSIIoTWEEK /ETSIIoTWORKSHOP /S01_ETSIIoTWEEK /ETSI_WELCOME_KEYNOTE_SCRASE.pdf

3. IoT in Pakistan

In Pakistan, international & national ICT firms are in early stages of developing innovative services using IoT technology. Some of IoT use cases include advanced metering infrastructure with automated meter reading on real-time or near-time two-way communication, smart devices /sensors / actuators, smart farming, health care solutions, smart grids and connected agriculture. Most of such applications are currently being provided through cellular networks. However, there is a need to formulate a comprehensive regulatory framework elaborating requirements for developments of IoT ecosystem in licensed as well as unlicensed bands. Some of the frequency bands for unlicensed IoT have been proposed by Frequency Allocation Board (FAB).

3.1. Government Initiatives

The Ministry of Information Technology & Telecommunications (MoIT&T) in Section 3(iii) of Telecom Policy-2015 has emphasized on forward looking to provision of the new services using latest technologies.

Later the Policy Directive of Ministry of IT on test and development of 5G dated October 16, 2017 had identified few bands for 5G and also required, to recommend, in consultation with industry / stakeholders, the suitable frequency bands in view of future technologies.

a) Industry Working Group on IoT (WG-IoT)

In view of the above, and also keeping into consideration the latest trends of IoT and 5G, PTA has created an industry working group. The aim of this working group is primarily to:

a) Foresee the IoT future developments in Pakistan, and
b) To evaluate and recommend the possible regulatory options (requirements in terms of spectrum, data protection /privacy, roaming, numbering /addressing, device standardization / type approval, etc.), that PTA and Government of Pakistan may adopt to tackle the challenges and avail the opportunities offered by IoT services /applications.

3.2. Regulatory Framework

a) Global Practices

IoT communication is in its evolution. Certain countries have regulated it in a modest way while others are figuring out a balanced approach to identify requisite parameters to regulate it. As the impact of this phenomena is cross sectoral, therefore, regulation of this communication technology is vital, so that a balanced

eco system can be created for the IoT value chain. The telecom regulators, globally, are focusing on establishing a balanced regulatory regime as the growth in IoT sector progresses exponentially.

There are few major parameters that are observed to have been considered by majority of the administrations for addressing with certain regulatory conditions for harmonized implementation and adoption of the evolving new technology. The major parameters involve:

a. Licensing regime / regulatory framework for the industry.
b. Spectrum allocation for use of such devices and networks.
c. Harmonized numbering plan, for use at national and international level.
d. Global and National Roaming.
e. QoS Standards.
f. Privacy and Protection of huge volume of data generated by IoT system.

These parameters have been catered for, by different countries in different ways. The same has been considered in the document for feedback, in order to shape up a regulatory instrument for Pakistan, in the light of international best practices.

A brief overview of regulatory practices of global regulatory bodies, on the important aspects are discussed hereunder with set of questions at the end of each section for consultation purpose.

b) IoT Licensing

Licensing is an important pillar of regulatory regime for ensuring level playing field for service providers and requisite provision of services to consumers. In order to formulate a balanced eco system for IoT, some countries have opted to have separate category of license for such services under certain conditions of provisions. Few of the country cases are discussed here under:

Table 3.1 Licensing / Regulatory Practices for IoT

Countries / Regulator	**Practices**
European Union	**BEREC (The Body of European Regulators for Electronic Communications.** No special treatment is necessary or appropriate for M2M communication, except for the following areas: • Roaming • Switching • Number portability

	Some European countries have issued Mobile Virtual Network Operator (MVNO) licenses for M2M players.
United Kingdom	Ofcom observed that the industry is best placed to drive the development, standardization and commercialization of new technologies such as M2M. Ofcom has therefore, launched the following licenses for M2M: 1. **Business Radio licenses** for M2M communication, covering the use of radio for mostly short range localized radio networks for factories, shopping centers. 2. **Other licenses** cover communication requirements for courier firms, bus companies, taxis and utility firms. 3. **Radio Supplier's License:** There is also a radio supplier's license covering demonstration and short term hire of equipment. 4. **Existing Licenses:** The current telecom licensees would continue to operate under the existing framework; however, specific changes to particular licenses on a case-by case basis would be made.
Singapore	**License for M2M:** Operators are required to have a license to offer M2M services under the framework of the regulator, Info-communications Media Development Authority (IMDA). Licensees have to ensure that SIM cards used for M2M services are only used for automated communication. Licensees shall list out the following: 1. The range of International Mobile Subscriber Identity (IMSI) numbers and Mobile Station International Subscriber Directory Number (MSISDN) to be used 2. Working with any local operator partner in relation to the provision of M2M services 3. Identification of M2M equipment importer 4. Registration of all SIM cards used to provide M2M services in Singapore 5. The records to be maintained in Singapore for a minimum of 12 months from the date of termination of the service 6. The M2M license enables the licensee to provide M2M services using equipment with embedded SIM cards.

Brazil	The M2M players are registered in the **MVNO category** and brought under the regulatory framework.
USA	In January 2017, the US Department of Commerce published guiding principles and outlined an approach to support the advancement of M2M. The key highlights are as follows: 1 Enabling infrastructure availability and access: Physical and spectrum related assets; IPv6 adoption 2 Crafting balanced policy and building coalitions: Cyber security, privacy, intellectual property and free flow of cross-border data 3 Promoting standards and technology advancement 4 Encouraging markets: Public private partnerships, Government procurement and workforce issues (education, training and civil liberties)
Saudi Arabia / CITC	IoT services can be provided using wired and wireless networks. They can be classified according to the networks used into: a) IoT services provided through mobile networks. b) IoT services provided through fixed networks c) IoT services provided using license-exempt frequencies. a) IoT services through mobile networks can be provided by licensed service providers from the CITC, such as Facilities Based Unified Licensees, MVNOs, IoT- VNOs, or any other licenses defined by CITC. b) IoT services through fixed networks can be provided by Fixed Facilities Based Licensees provided that the offered services comply with the licenses scope. c) IoT services using license- exempt frequencies can be provided commercially by service providers who have "providing IoT services using license- exempt frequencies" license from CITC. Service providers having the Facilities Based Unified License and Fixed Facility Based license from the CITC can provide this type of services without the condition of having "providing IoT services using license- exempt frequencies" license from CITC, provided the compliance with the technical security requirements. IoT networks that use license- exempt frequencies can be built and used indoor for non-commercial purposes without the condition of having "providing IoT services using license-

	exempt frequencies" license from CITC provided the compliance with the following conditions: i. Comply with the data security, privacy and protection requirements. ii. Comply with the Technical Specification numbered (RI114), which is available through CITC website (www.citc.gov.sa). iii. The importation of the equipment and implementation of the IoT networks must be done by the owners of those buildings and properties. IoT networks that use license- exempt frequencies can only be built outdoor by licensees having "providing IoT services using license-exempt frequencies" license from CITC, or service providers that have the Facilities Based Unified License from the CITC, or licensed fixed facility based service providers.

Source:[5]

Most of the countries have adopted to issue a separate category of licenses / registration. The same approach might be suitable for Pakistan.

[5] "BEREC Report on Enabling the Internet of Things," BEREC IoT Workshop, 1 February 2017; "Fostering the advancement of the IoT," The Department of Commerce Internet Policy Task Force & Digital Economy Leadership team January 2017; "Guidelines for submission of application for services based operations license," IMDA, December 2016; VHF radio spectrum for the Internet of Things," Ofcom, March 2016; ," Ofcom, July 2014. around: "VHF radio spectrum for the Internet of Things," Ofcom, March 2016 and "Promoting investment and innovation in the Internet of Things," Ofcom, July 2014.

The following questions, in this regard are raised for your comments /feedback:

Table Q-1: Questions -Licensing / Regulatory Framework

1. Should there be a separate category of Class Value Added license / registration for IoT service provisioning? What should be the scope of IoT Service Providers license / registration? Please, recommended terms and conditions and other regulatory requirements for the IoT service providers' license / registration?
2. Should there be a regional IoT license (14 telecom regions) or provincial or nationwide?
3. Should all of the existing telecom licensees be allowed to offer IoT services? If so, what should be the recommended method to regulate them? Should such licensees be allowed to offer IoT services under their respective licenses with necessary /required amendments in their existing licenses on case to case basis?
4. Should IoT in licensed frequency bands be allowed under MVNO's regime?
5. Should there be a requirement to register IoT base stations with Frequency Allocation Board (FAB)?
6. Should there be a regulatory categorization of critical and non-critical IoT services? And should there be specific permissions /authorizations for critical and non-critical IoT? Which services should fall under critical IoT category?
7. Should the Critical IoT services be allowed under cellular services only or also for or individual licenses for IoT?
8. Should other domain regulators and authorities (like, oil & gas, power, agriculture, transportation, highways, climate control, etc.) have their own policies and regulations regarding IoT applications, or they may be governed under the telecommunication license? Is it recommended to develop collaborative regulations for IoT in consultation with other domain regulators & authorities?
9. If embedded SIMs (e-SIMs) are to be used for IoT devices, what should be the mechanism for their registration?
10. Any other aspect not mentioned here should be shared with details and justifications.

c) IoT Spectrum for Unlicensed Frequency Bands

Many IoT use cases appears to be served by radio technologies that operate in unlicensed spectrum e.g. ZigBee, Bluetooth and Wi-Fi, and they are designed for short-range connectivity with limited QoS and security requirements.

The Long Range technology, i.e., LPWAN on the other hand has operational capabilities to enable a massive number of connections, with relatively low output power levels to provide connectivity on average over several kilometres, while maintaining longer battery life.

a)Transceiver Parameters:

As per ITU6 report, LPWAN systems connect objects and devices through gateways and access stations. All systems are not always balanced and the equivalent isotropic radiated powers vary according to the technologies and the role of each transmitter in the systems. Typical values range (EIRP) between 200 mW to 4W for the access stations and 5 mW to 500 mW for the end-points.

b) Antenna characteristics:

Most of the transmitters use omnidirectional antenna. Typical value ranges between 0 dBi to 6 dBi. These typical values come from standards and regulations under which LPWAN systems operate worldwide (i.e. ETSI EN 300 220, 47 CFR 15.247, etc.).

LPWAN systems are currently deployed in spectrum bands harmonized regionally for SRD as follows:

ITU Region 1[7]

In CEPT countries, most of LPWAN infrastructures are operated in the 865-870 MHz SRD band. In particular, they rely on the bands 865-868.6 MHz at 25 mW ERP and 869.4-869.65 MHz at 500 mW ERP by using mitigation techniques like duty cycle restriction. Equipment should comply with the ETSI EN 300 220.

Similarly, LPWAN systems are operated under those conditions in some African and Middle Eastern countries that have implemented SRD regulations in the 865-870 MHz range.

---

6 REPORT ITU-R SM.2423-0, https: / /www.itu.int /md /R15-SG01-C-0135 /_page.print

7 Source: ITU Report Report ITU-R SM.2423-0

ITU Region 2

In the 902-928 MHz ranges, unlicensed usage with a transmit power up to 4W EIRP is generally enabled. An example may be found in 47 CFR 15.247.

ITU Region 3

LPWAN deployments are done on a country specific basis. Recently, several administrations in Asia-Pacific have authorised LPWAN services in 915-925 MHz range on the basis of different spectrum access techniques and standards, such as ARIB STD-T-108 in Japan.

Furthermore, according to an APT survey report on IoT in Asia Pacific countries in edition September, 2020, 433 MHz has been identified mostly for LPWAN / non-cellular IoT by Iran (433.05 – 434.79 MHz), Bangladesh (433.05 – 434.79 MHz), Vietnam (433.05 - 434.79 MHz), Malaysia (433 MHz - 435 MHz). Thailand has identified 433 MHz for RFID.

The following frequency bands have been proposed by Frequency Allocation Board (FAB) for unlicensed IoT.

Table 4.2 Proposed Spectrum for IoT

Proposed Spectrum for IoT		
S. No	**Frequency Bands**	**Max Radiated Field Strength / Output**
1	433.05-434.79MHz	100 mW ERP
2	920-925MHz*	≤ 200 mW ERP

(*) protection of primary services operational in adjacent frequency bands shall be ensured

Industry point of view is sought on the following spectrum related queries.

Table Q-2: Questions - Spectrum requirements for IoT
11. Are there any other frequency bands which may be considered for LPWAN besides those recommended by Frequency Allocation Board (FAB)? How to ensure interference mitigation for incumbent services being offered in adjacent bands (e.g., Mobile (GSM) in 900 MHz, PPDR (LTE) in 865 MHz). 12. What is the recommended transmit power (EIRP) requirement in 433 MHz and 920 MHz bands for popular LPWAN technologies like LoRA and Sigfox for both end terminal and base stations?

13. Does the allocated spectrum seem to meet the future demand of IoT devices or additional spectrum (licensed or unlicensed) may be required?
14. Are there any other comments or suggestions related to the topic?

d) IoT Numbering and Addressing

The international practices of addressing or numbering resource allocation for IoT services are listed below:

i. **Electronic Communications Committee (ECC) Reports**

ECC has carried out comprehensive analysis of numbering requirement and various solutions which are available in its various reports which are detailed as Appendix-1:

ii. ITU's Allocation of MNC (Mobile Network Code) for M2M

The ITU held a consultation on the "Possibility of parallel usage of 2 and 3 digits E.212 Mobile Network Codes (MNCs) under one geographic Mobile Country Code (MCC)" in 2013, However, its formal position is yet to be finalized. Opening up access to MNCs for M2M service providers could stimulate competition by enabling balanced negotiations that promote the growth of M2M. A large M2M service provider holding its own MNC could have more leverage when entering negotiations with a potential partner MNO over its roaming (and other) rates.

As it would no longer be dependent on the specific package that a mobile operator is prepared to offer, but could change SIM and other settings over the air, competition in the marketplace for M2M would be enhanced. Furthermore, switching to a new MNO at any stage would be much simpler and less costly for a M2M service provider because the SIM cards which are installed in the M2M devices would not need to replacement. If the ITU recommend the issuance of MNCs to such M2M service providers and change the criteria as currently stipulated in Annex B of the ITU-T Rec. E.212, some countries may directly allocate MNC to big M2M service providers.

iii. AT&T comments on Ofcom consultation document

AT&T had commented on the Office of Communications, U.K. (Ofcom) consultation document, promoting investment and innovation in IoT, during October 2014[8], detailed at Appendix-2.

[8] AT&T Comments on Ofcom Consultation Document, Promoting Investment and Innovation in the Internet of Things, 1 October 2014.

AT&T had advised Ofcom to consider the approach of several European countries (for example, Belgium, Bulgaria, Croatia, Denmark, Finland, France, Netherlands, Norway, Portugal, Spain, and Sweden), which have introduced a special range of numbers for M2M communication. These special ranges typically have number blocks which use a longer number sequence (up to the full 15 digits) in E.164 format. The length of E.164 numbers for mobile users was selected to balance the needs of the efficient use of numbering with the human factors of communicating and dialing a convenient length. To achieve that balance, in Europe (including the UK) the average length of E.164 number ranges typically does not exceed 12 digits, which includes trunk code. Machines, however, have no such need for convenience and so for M2M communications a full 15-digit number allocation, as described in ITU E.164, could be considered.

iv. Country Case studies of M2M Numbering Policy

The country case studies of Singapore and Hong Kong are given at Appendix-3 and the summary of M2M numbering policy in various countries is given in Appendix-4

v. Report by Machina Research

According to the report released by Machina Research in 2015

1. A number of regulators have opted to implement a dedicated E.164 mobile number range for M2M
2. Ultimately addressing of all connected devices will be handled by IPv6
3. CEPT has sought to encourage adoption of dedicated numbering – most EU countries have adopted.

Therefore, from the above, it can be observed that the E.164 numbering resources (i.e. numbers in the national numbering plan) are the most appropriate solution for addressing M2M applications at least for short and medium run. The IP-based solutions with IPv6 addressing will become more important in the long run.

Table Q-3: Questions on Numbering & Addressing
15. Should there be a new numbering scheme to be introduced for IoT /M2M services? Should there be an access code used as prefix to (currently deployed) E.164 numbering series for IoT / M2M services or additional /new identifiers for IoT / M2M services? 16. How many digits should the numbering series for IoT / M2M devices comprise of? 17. Should the access code or the mobile network codes be allocated to IoT /M2M providers as well? Or IoT providers be restricted to e-SIMs only?

18. Do you see any potential security and fraud risks associated with private parties being assigned numbering resources, if considered for procuring and issuing SIM cards?
19. Should the numbering series support number portability?
20. Should the current E.164 numbering be continued as short term solution? What is the recommended timeline for the short-term adoption?
21. What should be the recommended time line for IPv6 adoption?
22. Should there be separate numbering ranges for Critical IoT?
23. Will switching from E.164 to new series at some later stage affect the market?

e) International roaming for IoT

One of the critical aspects of IoT is the ability to offer services on a global scale. Lack of specific regulations on permanent roaming in most countries has benefitted the IoT market so far. However, IoT roaming is growing exponentially. Permanent roaming offers key benefits, ranging from supply chain simplicity to wider coverage. For instance, many multinational companies like to avail services from a single IoT player. The cost of IoT services increases significantly on account of switching IoT players. The absence of permanent roaming feature in IoT device acts as a significant barrier to business. The following table summarizes the regulatory practices for permanent roaming.

Table 3.2 Regulatory Practices for International Roaming

Country / Regulator	**Position**
BEREC /EC	The European roaming regulatory framework applies in general to mobile connectivity in M2M services. However, certain exemptions have been made for M2M roaming services that are applicable to retail data roaming: Roaming providers need not send any automatic messages to M2M devices to inform the customer that roaming is ongoing, and provide information about prices. There is no obligation to provide M2M customers accumulated consumption of data or any maximum financial limits for specified periods of use. The EC roaming regulation do not obligate operators to offer permanent roaming

Germany	The telecom regulator, German Regulatory Authority for Industries: Telecommunications, Postal Services, Railways, Electricity (BNetzA), introduced new numbering rules in June 2016 to facilitate M2M services and to enable exterritorial use of numbers. The regulator has allowed the use of German IMSIs for M2M services in other countries. In addition, use of extraterritorial IMSIs is allowed in Germany.
Belgium	In August 2015, the Belgium telecom regulator, Belgian Institute for Postal Services and Telecommunication (BIPT), recommended that there should be more flexibility in the general extraterritorial use of Belgian numbering resources. For M2M services in particular, it recommended that permanent roaming be allowed for Belgian numbers abroad as well as for foreign numbers roaming in Belgium.
Ofcom, UK	UK has not taken any position on permanent roaming for M2M
Italy	The Italian regulator advocates adopting a global SIM approach
France	Telecom regulator, Regulatory Authority for Electronic Communications and Posts (ARCEP), favors leaving prices to commercial negotiation for M2M roaming.
Australia	Currently, there are no restrictions on permanent roaming.
Brazil	Permanent roaming is prohibited
Singapore	Permanent roaming is prohibited. In January 2016, IMDA embarked on a trial to see how an open GSMA standard (over-the-air subscription management) can enable embedded SIM (e-SIM) chips to switch between different MNOs. The interoperable standards are expected to lead to a more competitive environment for the deployment of M2M devices, by reducing costs and increasing adoption.

Source : [9]

[9] Source: "BEREC Report on Enabling the Internet of Things," BEREC IoT Workshop, 1 February 2017; "Fostering the advancement of the IoT," The Department of Commerce Internet Policy Task Force & Digital Economy Leadership team, January 2017; "Guidelines for submission of application for services based operations license," IMDA, December 2016; VHF radio spectrum for the Internet of Things," Ofcom, March 2016; ," Ofcom, July 2014. around: "VHF radio spectrum for the Internet of Things," Ofcom, March 2016 and

f) **Report on Permanent Roaming by Machina Research**

Permanent roaming "Extra-territorial use of E.164 numbering" is probably the thorniest issue in M2M regulation today. Supporting overseas connections is critical and there is an existing large installed base of permanent roaming SIMs. The regulatory situation is unclear, and changing.

g) **ITU:** The ITU in December 2018 has designated the Mobile Country Code (MCC) 901 as a shared MCC. This allows for the provision of Mobile Network Codes (MNCs) that are not tied to any one national market. Service providers that qualify for an MNC under MCC 901 are able to operate cross-border services using a single SIM with a single price for data connectivity. ITU mentions that the demand for global connectivity for IoT and M2M applications is motivating an increasing number of IoT and M2M players to apply for ITU-allocated 'global IMSI ranges'. Global International Mobile Subscriber Identity (IMSI) ranges are signified by the shared Mobile Country Code '901', a code without ties to any particular country. Global IMSI ranges enable 'global SIMs', providing network-agnostic, cross-border connectivity at a single price.

The manufacturers of M2M shall prefer to install M2M identification functionality at the time of manufacture and not to install country specific SIM modules. Therefore, for M2M devices to have IMSI numbers that are independent of the underlying service providers. One solutions could be shared MCC and National Roaming, to facilitate more seamless switching between service providers,[10]

h) From the above discussion, it can be concluded that very few countries have explicitly banned permanent roaming for M2M devices and most of the countries follow the same regulations which are applicable for P2P SIMs.

Point of view of the industry is required on the following:

Table Q-4: Questions on International Roaming
24. Should the national and / or international roaming be permitted? 25. In order to facilitate roaming, should IoT operators be assigned a unique National Mobile Network Code (MNC)? What would be its benefits and potential drawbacks? 26. Should Mobile Operators use separate MNC for offering IoT services?

"Promoting investment and innovation in the Internet of Things," Ofcom, July 2014.Regulating Permanent Roaming for M2M and IoT devices by Ovum

[10] https: / /nta.gov.np /wp-content /uploads /Consultation-paper-for-IOT-and-M2M.pdf

27. Should Global SIM be permitted? Is market ready to adopt such arrangement?

i) IoT Quality of Service

Different machines (e.g., sensors, meters) in an IoT system capture "events" (e.g., temperature, inventory level), which are transmitted through a network (e.g., wireless, wired or hybrid) to an application that translates them into meaningful information (e.g., items need to be restocked). From the QoS perspective, in the service provisioning process, networks of different characteristics can be used. According to that, the challenge is how to provide end-to-end QoS guarantees despite the limitations of different means of communication. Namely, when providing services in IoT systems, service providers have to be very careful when agreeing on certain QoS parameters.

Although some initial efforts in the area of IoT standardization have been made, notably within the European Telecommunications Standards Institute (ETSI) and the 3rd Generation Partnership Project (3GPP). QoS in IoT has not yet been considered. However, the problem of QoS in IoT systems has been identified.

Some standards for M2M / IoT systems were proposed by the 3GPP where each IoT device attaches to the existing mobile cellular infrastructure. In that way, their solution is not applicable in every IoT system, because some IoT solutions may not be based on the cellular mobile network.

QoS needs vary widely between usage, devices, applications and industries in IoT. The vast array of connected devices makes it difficult to prescribe and monitor QoS measures. There are a number of communication technologies for the deployment of IoT services and each one has specific nuances and protocols. A combination of different technologies is used for end service provisioning. In addition, various industries have separate regulators, each with its distinct set of requirements. For IoT services, it would be difficult to adhere to individual guidelines, which may significantly differ from each other.

It is suggested that the quality of service aspects may be left to the market forces for the time being. However the services being provided using the licensed spectrum band are already being regulated under the respective licenses. Service providers should have maximum flexibility to design their networks instead of defining SLAs at various points through regulatory mandates. In the case of IoT, the QoS may be left to a mutual agreement between stakeholders.

Feedback is sought on the following:

Table Q-5: Questions for QoS
28. What should be QoS criteria (if any) for IoT services in unlicensed band? 29. Should the existing QoS criteria for mobile broadband be considered adequate for IoT services or new parameters should be defined? *(3GPP has defined QoS parameters for various IoT services operating in licensed bands.)*

j) IoT Security, Privacy and Data Protection

In IoT networks, the physical objects in our everyday lives increasingly detect and share observations about us, so consumers will definitely want a continued privacy. In IoT, where most of the communication happens without human intervention, intrusion of privacy is a tricky aspect. There are challenges in determining whether specific information is personal in nature or not. This distinction gets blurred when more stakeholders are involved, increasing the data sharing interfaces and thus resulting into more vulnerability to privacy and protection of information. Therefore, disruptions of information during the designed operations, either intentionally or unintentionally, will likely bring great inconvenience and possibly monetary losses to users and providers of IoT technology. If not managed properly, these IoT devices could also be exploited to launch attacks on other networks, resulting in Distributed Denial of Services ("DDoS").

Wireless communication in today's Internet is typically made more secure through encryption, which is also seen as key for ensuring information security in the IoT. However, many IoT devices are not currently powerful enough to support robust encryption. To enable encryption on the IoT, algorithms needs to be made more efficient and less energy consuming, and efficient key distribution schemes are needed.

Managing security and privacy issues has the goal to significantly reduce attacker's access to private data which could cause physical harm in cases, such as, medical devices, connected vehicles and many others. This could be achieved by:

1) Ensuring security and vulnerability patching of devices and of the whole IoT system design process,
2) Ensuring individual control of profiles, &
3) Development of co-regulation to protect security and privacy of personal data with more cooperation between telecom companies, telecom regulators and other related parties.

There are few other challenges, such as, efficient encryption algorithms running IoT devices and networks need higher processing power (low CPU power vs effective

encryption). Traditional security approaches used in electronic communications may be not sufficient to address low cost devices used by many IoT services. Also the Crypto algorithms have a limited lifetime before they are broken, which may outlive the original running application.

The GSMA IoT Security Guidelines in this regard, which explain how an entity providing a cellular IoT service can secure its service end-to-end from most cyber-attacks, can be used as a reference set for security and privacy best practice guidelines. NIST Cyber-security Framework also acts as a reference point for security measures.

In many countries, there are strict rules and regulations around securing and storing personal data of customers. However, there are no consistent norms for data privacy across geographies. Multi-party real-time information flows may be hampered if privacy issues are not addressed at the outset. In the current scenario, there are patchworks of geographically bound laws that do not apply in the same manner to different technologies and sectors. Information collected in one country may be termed as personal data in a different jurisdiction. Increasingly, various stakeholders are resorting to using aggregated and anonymized data through which no individuals can be identified. There is growing debate on how to balance individual rights on one hand and ensure law enforcement and maintain surveillance on the other. However, the regulatory position for private data collected by IoT devices is similar to that used for that collected by other means.

Table 3.3 Regulatory Practices for personal data collected by IoT devices

Country / Regulator	**Position**
BEREC	Personal data may be collected by a number of connected devices. • There is no need for special treatment with regard to EU Data Protection Principles (e.g., consent-based data collection and processing also apply in M2M context). • Careful adaptation or evolution is required in the M2M context (e.g., user-friendly information and consent procedures for smart homes).

Singapore	Governed by the Personal Data Protection Act (PDPA 2012) that comprises various rules governing the collection, use, disclosure and care of personal data.

Source: Legislation and guidelines," PDPC Singapore.

Suggestions and comments on Security related matters is sought:

Table Q-6: Questions on Security and Privacy and Data Protection

30. Would mandating the security standards specified by International Standardization bodies be adequate for data security and privacy?
31. Please suggest additional measures, if any, for securing IoT networks and data privacy.
32. Are the existing standards for mobile networks data privacy and security sufficient for Cellular IoT providers? Should the same standards be applicable and sufficient for the other (non-cellular) IoT service providers?
33. Please provide your valuable suggestions and comments on any of the related matters that are not being covered in the consultation papers?

4. Conclusion

A comprehensive response of the industry is sought on the consultation questions in Annex- A, for assessment of the industry opinion, in developing regulatory regime for IoT.

5. Questionnaire for feedback

Table Q-1: Licensing / Regulatory Framework

1) Should there be a separate category of Class Value Added license / registration for IoT service provisioning? What should be the scope of IoT Service Providers license / registration? Please, recommended terms and conditions and other regulatory requirements for the IoT service providers' license / registration?
2) Should there be a regional IoT license (14 telecom regions) or provincial or nationwide?
3) Should all of the existing telecom licensees be allowed to offer IoT services? If so, what should be the recommended method to regulate them? Should such licensees be allowed to offer IoT services under their respective licenses with necessary /required amendments in their existing licenses on case to case basis?
4) Should IoT in licensed frequency bands be allowed under MVNO's regime?
5) Should there be a requirement to register IoT base stations with Frequency Allocation Board (FAB)?
6) Should there be a regulatory categorization of critical and non-critical IoT services? And should there be specific permissions /authorizations for critical and non-critical IoT? Which services should fall under critical IoT category?
7) Should the Critical IoT services be allowed under cellular services only or also for or individual licenses for IoT?
8) Should other domain regulators and authorities (like, oil & gas, power, agriculture, transportation, highways, climate control, etc.) have their own policies and regulations regarding IoT applications, or they may be governed under the telecommunication license? Is it recommended to develop collaborative regulations for IoT in consultation with other domain regulators & authorities?
9) If embedded SIMs (e-SIMs) are to be used for IoT devices, what should be the mechanism for their registration?
10) Any other aspect not mentioned here should be shared with details and justifications.

Table Q-2: Spectrum requirements for IoT

11) Are there any other frequency bands which may be considered for LPWAN besides those recommended by Frequency Allocation Board (FAB)? How to ensure interference mitigation for incumbent services being offered in adjacent bands (e.g., Mobile (GSM) in 900 MHz, PPDR (LTE) in 865 MHz).
12) What is the recommended transmit power (EIRP) requirement in 433 MHz and 920 MHz bands for popular LPWAN technologies like LoRA and Sigfox for both end terminal and base stations?

13) Does the allocated spectrum seem to meet the future demand of IoT devices or additional spectrum (licensed or unlicensed) may be required?
14) Are there any other comments or suggestions related to the topic?

Table Q-3: Numbering & Addressing

15) Should there be a new numbering scheme to be introduced for IoT /M2M services? Should there be an access code used as prefix to (currently deployed) E.164 numbering series for IoT / M2M services or additional /new identifiers for IoT / M2M services?
16) How many digits should the numbering series for IoT / M2M devices comprise of?
17) Should the access code or the mobile network codes be allocated to IoT /M2M providers as well? Or IoT providers be restricted to e-SIMs only?
18) Do you see any potential security and fraud risks associated with private parties being assigned numbering resources, if considered for procuring and issuing SIM cards?
19) Should the numbering series support number portability?
20) Should the current E.164 numbering be continued as short term solution? What is the recommended timeline for the short-term adoption?
21) What should be the recommended time line for IPv6 adoption?
22) Should there be separate numbering ranges for Critical IoT?
23) Will switching from E.164 to new series at some later stage affect the market?

Table Q-4: International Roaming

24) Should the national and / or international roaming be permitted?
25) In order to facilitate roaming, should IoT operators be assigned a unique National Mobile Network Code (MNC)? What would be its benefits and potential drawbacks?
26) Should Mobile Operators use separate MNC for offering IoT services?
27) Should Global SIM be permitted? Is market ready to adopt such arrangement?

Table Q-5: Quality of Service

28) What should be QoS criteria (if any) for IoT services in unlicensed band?
29) Should the existing QoS criteria for mobile broadband be considered adequate for IoT services or new parameters should be defined? *(3GPP has defined QoS parameters for various IoT services operating in licensed bands.)*

Table Q-6: Security and Privacy and Data Protection

30) Would mandating the security standards specified by International Standardization bodies be adequate for data security and privacy?
31) Please suggest additional measures, if any, for securing IoT networks and data privacy.

32) Are the existing standards for mobile networks data privacy and security sufficient for Cellular IoT providers? Should the same standards be applicable and sufficient for the other (non-cellular) IoT service providers?
33) Please provide your valuable suggestions and comments on any of the related matters that are not being covered in the consultation papers?

6. Abbreviations

3GPP	3rd Generation Partnership Project
AR	Augmented Reality
BEREC	The Body of European Regulators for Electronic Communications
CEPT	European Conference of Postal and Telecommunications
CMO	Cellular Mobile Operator
EC	European Commission
ECC	Electronic Communications Committee
EIRP	Effective Isotropic Radiated Power
ERP	Effective Radiated Power
e-SIM	Embedded SIM
ETSI	European Telecommunications Standards Institute
FAB	Frequency Allocation Board
GOP	Government of Pakistan
GPS	Global Positioning System
GSA	General Services Administration
GSMA	GSM Association
IMDA	Info-communications Media Development Authority
IMSI	International Mobile Subscriber Identity
IOT	Internet of Things
ITU	International Telecommunications Union
LPWAN	Low Power Wide Area Network
M2M	Machine 2 Machine
MCC	Mobile Country Code
mMTC	Massive Machine Type Communication

MNC	Mobile Network Code
MNO	Mobile Network Operator
MOIT&T	Ministry if Information Technology & Telecommunications
MSISDN	Mobile Station International Subscriber Directory Number
MVNO	Mobile Virtual Network Operator
NB-IOT	Narrow-band IOT
NIST	US National Institute of Standards & Technology
NNP	National Network Plan
NRA	National Regulatory Authority
NSN	National Significant Number
OECD	Organization for Economic Co-operation and Development
P2P SIM	Person 2 Person SIM
PTA	Pakistan Telecommunications Authority
QoS	Quality of Service
SBO	Service Based Operator
SIM	Subscriber Identification Module
SRD	Short Range Device
TSP	Telecom Service Provider
UHD	Ultra High Definition
UNB	Ultra Narrow Band
URLLC	Ultra-Reliable Low-Latency Communication
VR	Virtual Reality

7. Appendices - Numbering and Addressing

Appendix-1	Electronic Communications Committee (ECC) Reports
Appendix-2	AT&T comments on Ofcom consultation document pertaining to IoT Numbering and addressing.
Appendix-3	The country case studies of Singapore and Hong Kong
Appendix-4	Summary of M2M Numbering Policy adopted by Countries

Appendix-1

Numbering and Addressing (Electronic Communications Committee (ECC) Reports)

i. Important points of ECC report 153, November, 2010

a) The number length of network external numbers should be as long as possible (max 15 digits according to ITU-T Rec. E.164).

b) As a long term solution IPv6 addresses, or numbers /addresses other than E.164 numbers should preferably be used for device based communication applications. These numbering /addressing schemes or switching from E.164 numbering plan to a new plan should not prohibit market development or competition.

c) There are possible situations where a new number range should be opened. For example, the number range in question may require different regulatory treatment, e.g. relating access to emergency services, or the services to be provided have certain characteristics (e.g. M2M applications in fixed networks) where existing mobile number ranges may not be adequate.

ii. Options suggested by ECC

For planning MSISDN (ITU Rec E.164) numbering resources for M2M devices / Gateways, ECC documents have suggested the following four options:

Table A-1 Licensing / Regulatory Practices for IoT

Options	*Suggestion*
Option A	Existing mobile number ranges, including possible expansion of them (E.164 numbers)
Option B	A new number range for M2M or similar applications (E.164 numbers) (for example longer numbers than normally, however max 15 digits according to E.164)
Option C:	An international numbering solution (E.164 numbers)
Option D:	Network internal numbers

iii. Analysis of these options is as follows:

Option A: Existing mobile number ranges

Complies with ITU-T Rec. E.164 (interconnection and international traffic is possible; max. 15 digits),

- Number portability is directly applicable (flexibility to change operator)
- May not allow separate back-office solutions for M2M applications
- A risk of exhausting the existing ranges
- Less new capacity than the network internal number Option D

- In the case of non-geographic and existing Premium Rate Service (PRS) numbers, limitations on access from overseas;
- Inter-operator billing difficulties and a risk of incurring unnecessary expense

Option B: New number range

- Must comply with ITU-T Rec. E.164 (interconnection and international traffic is possible; max 15 digits)
- Number portability is applicable (flexibility to change operator)
- Enough capacity available if full number length is used
- A fresh start for number analysis
- Different regulatory requirements possible if needed
- May allow easier back-office solutions, such as charging and billing

Option C: international number range

- Comply with ITU-T Rec. E.164 (interconnection and international traffic is possible; max 15 digits)
- Number portability is applicable (flexibility to change operator)
- Full capacity of numbers is available
- Number range needs to be assigned by the ITU and the applicant needs to be qualified
- International number, i.e. international prefix has to be always used
- Challenges in number analysis and effective routing
- New interconnection agreements might be negotiated
- May need to be treated in the same way as other international Traffic

Option D: Network internal numbers

- Not regulated in many countries; decisions and management by operators
- Same numbers can be used in every network allowing multiplied capacity
- Allows long numbers with much capacity – even longer than 15 digits numbers are possible if technical feasible
- No need for determining number length
- Allows use of hexadecimal digits if technical feasible
- Number portability is in practice not possible
- M2M SP is locked with one operator => possible competition issues

- Difficult or impossible to evolve to 'network external' mode if required for some reason
- Didn't comply with ITU-T Rec. E.164

iv. Significant points of ECC /REC / (11)03, May 2011

a) The number length in the new number range(s) accommodating future mass M2M applications should be as long as possible (in case of E.164 numbers maximum of 15 digits according to ITU-T Rec. E.164).
b) The NRA should ensure that the new number range(s) are not used as an alternative to existing number ranges to escape regulatory requirements.
c) As some existing regulatory requirements (e.g. access to emergency services) may not be relevant or useful for IoT / M2M applications, exceptions regarding existing regulatory requirements could be applied to new numbering range(s) accommodating these applications.

v. ECC report on M2M, Brussels, November, 2013

ECC had published a report in November, 2013 in Brussels, ensuring the availability of numbering and addressing resource. The conclusions are as given below:

a) The potential number of M2M applications /connections may have a big impact on National Numbering Plans;
b) Reports help regulators to develop efficient numbering solutions and to avoid numbering exhaustion (existing and new national numbering ranges);
c) Meet the needs of operators and M2M Service Provider and to avoid possible lock-in of M2M users
d) The IP addresses might be a long term solution;
e) The E.164 number length for new M2M numbering range should be as long as possible (maximum of 15 digits including Country Code);

vi. ECC recommendations (15)02, April, 2015

ECC vide their recommendations (15)02, issued guidelines for major changes to National numbering and dialing plans concerning E. 164 numbers which was approved in April, 2015. The important recommendations of this report are as given below:

Sufficient capacity is always made available for the growing demand for numbers for mobile services, and also for M2M services in accordance with ***ECC /REC /(11)03 of May 5, 2011.***

Appendix-2

1. AT&T comments on Ofcom consultation document pertaining to IoT Numbering and addressing.

AT&T had commented on the Office of Communications, U.K. (Ofcom) consultation document, promoting investment and innovation in IoT, during October 2014.[11]

Machines are required to be uniquely identified and addressed in order to communicate; therefore, it is likely that E.164 numbers will be necessary for a long term with the M2M / IoT devices. For many devices and applications developed today, E.164 numbers are used and will continue to be used throughout the lifecycle of the product. With many consumer and industrial products having lifetimes of 10 to 20 years, an ongoing supply of E.164 numbers will be needed.

For the highly integrated nature of high-volume, low-cost, electronic modules, a retrofit or upgrade to an alternate numbering resource would be uneconomical. For instance, after expending substantial effort and incurring considerable expense, IPv6 use has seen considerable growth over the last few years. However, there may be a substantial overlap period where both IPv6 and E.164 numbers are in use. It is estimated that it will take 5 to 10 years for IPv6 to become widely available. If the field lifecycle of a device is 20 years, E.164 numbers could be needed for the next 30 years. However, issuance of new E.164 numbers could only begin to be phased out when IPv6 becomes widely available and then only for those devices that do not need to rely on PSTN-based addressing.

[11] AT&T Comments on Ofcom Consultation Document, Promoting Investment and Innovation in the Internet of Things, 1 October 2014.

Appendix-3

The country case studies of Singapore and Hong Kong on Numbering and Addressing

1) Singapore

a. Singapore Public Consultation

There was a public consultation on proposed M2M Access Code Allocation Framework, by Infocomm Development Authority (IDA) Singapore.[12] Important points on M2M Numbering, described in Annex A-3:

b. National Numbering Plan, IDA Singapore[13]

Important points on M2M Numbering plan in Singapore:

i. Service-based Operator (SBO) (Individual) licensees providing M2M services are eligible for '144XX' access code.
ii. The M2M access code allocated may be used with international connectivity and international roaming services.
iii. Licensees providing M2M services using the M2M access codes, i.e. '144XX' are encouraged to maximize the allowable numbering capacity with a 13-digit numbering format (excluding country code) for each M2M access code.
iv. In Singapore, mobile as well as fixed line numbers are of 8 digits. Without using the existing numbering resource, they have planned a new 13 digits numbering scheme for M2M services.

c. Highlights of Consultation on IoT numbering and addressing

i. In developing the pilot M2M framework in 2010, IDA assessed that it would not be appropriate to open up existing telephone number levels for M2M services as these number levels are established primarily for persons-to-persons telecommunication. For instance, the NNP provided the 8-digit number levels for fixed-line telephone services (starting with prefix "6") and mobile telephone services (starting with prefixes "8" and "9"), took into consideration the total capacity to cater for the long-term growth of these services and the ease of dialing by users. Allowing M2M services to use these number levels may exhaust the numbering capacity much sooner than expected.
ii. To ensure that there is sufficient numbering capacity for all M2M devices and machines in the future, and to differentiate M2M services from other services, IDA has reserved a block of 4-digit M2M Access Code (i.e. "144X") for M2M services. IDA

[12] Public Consultation on Proposed M2M Access Code Allocation Framework, iDA Singapore.Proposed Machine -To- Machine ("M2M") Access Code Allocation Framework ,11 April 2013

[13] National numbering Plan(Issue 1 – 1 October 2016) Info-communications Media Development Authority,Singapore

also took the view that a maximum digit length should be adopted. Based on the International Telecommunication Union ("ITU") E.164 numbering format, Singapore would allow numbers of up to 13-digit length, using the designated 4-digit Access Code (excluding the country code), based on current network routing technology and arrangements.

2) Hong Kong

a) Code of Practice Relating to the Use of Numbers and Codes

Hong Kong is having 8 digit numbering scheme in fixed and mobile service, excluding country code. The code of practice relating to the use of numbers and codes in the Hong Kong Numbering Plan was revised in April 2015. Important points related to M2M numbering proposed in Hong Kong are as given below[14]:

In differentiating the "4500X" M2M numbers from the ordinary subscriber numbers, following guidelines were issued to the operators while assigning "4500X" numbers:

i. The numbers should be of 12 digits in length.

ii. The numbers shall not be required to support number portability.

iii. No mandatory requirement of inter-network routing is imposed on the numbers. Operators may freely enter into commercial arrangements with their interconnecting partners for routing of 12-digit "4500X" M2M numbers across networks based on their own business decisions.

iv. The numbers should not be used for voice and SMS communications. In case any M2M application would require communications via SMS, operators should assign ordinary 8-digit subscriber numbers for the application. Mobile network operators, MVNOs, fixed network operators, services-based operators in providing Class 1 or Class 2 services, and paging operators who provide M2M communications through the public telecommunications network using E.164 numbers may apply for the allocation of "4500X" M2M numbers.

b) MSISDN less Numbering plan

In 3GPP Release-12 /13, M2M HLR has a feature "MSISDN-less subscription". This feature makes it possible to define MSISDN-less M2M subscriptions in R12 /13 HLR, meaning that this type of subscription may not have a valid MSISDN assigned to it. This feature may potentially reduce the pressure on MSISDN number series assigned to the PLMN operators and to some extent the risk of running into shortage of MSISDN numbers during large scale deployment of M2M services. The MSISDN sent

[14] https: / /www.coms-auth.hk /filemanager /statement /en /upload /385 /cop-numbering_e.pdf

to the network for a MSISDN-less M2M subscription is the Network Application specific dummy MSISDN stored in M2M profile. However, MSISDN less M2M subscription cannot be examined at this stage because of lack of information about use cases and probable lack of any regulatory policy.

Appendix-4

Summary of M2M Numbering Policy adopted by Countries

Table A-4 Summary of M2M Numbering Policy adopted by countries

Country	M2M Numbering Policy
Belgium	Non-geographic, fixed mobile agnostic network code, dedicated to M2M;
Denmark	IMSI only identifier to be used for M2M. No dedicated number range specified.
Finland	Fixed length of 11 digits of national (significant) numbers for mobile numbers beginning with 049. The purpose is to use numbers beginning with 049 primarily for machine-to-machine communication (M2M) or similar purposes where the number's user friendliness is not on a top priority.
United Kingdom	Ofcom believes the limits on the availability of telephone numbers will not be a barrier to the development of the IoT as a range of alternative identifiers, such as Internet Routing Codes, SIM or equipment identifiers and IP addresses could be used. It also considers that migration to IPv6 in the longer term is likely.
Netherlands	Dedicated M2M number ranges for mobile
Norway	Dedicated M2M number ranges for mobile
Spain	Dedicated M2M number ranges for mobile
Sweden	Separate dedicated M2M number ranges for fixed and for mobile
Hong Kong	allocate "4500X" numbers in 12-digit length for M2M services; 450(1-9)X" numbers with digit length of 12 will be reserved to meet the future demand for M2M services; For M2M services. Numbers shall be assigned to machines but not subscribers. Numbers shall not be portable across networks and not be mandated to route
Brazil	M2M service providers are MVNO with separate IMSI block of their own.
Australia	In responding to the expected demand for new mobile numbers, in 2012 the ACMA made available a new mobile number range (05 range) to supplement the existing (04) mobile number range. The

	ACMA will continue to monitor changes in demand for mobile numbers used in M2M communications.
Singapore	Licensees providing M2M services using the M2M access codes, i.e. '144XX' are encouraged to maximize the allowable numbering capacity with a 13-digit numbering format (excluding country code) for each M2M access code
Saudi Arabia	13 digits with 12 digits National Significant Number (NSN)- 3 digits service indication code and 9 digits subscriber number. 0 83Z YY XX XXXXX, Z=0, Y=0-9, YY indicates licensee. M2M numbers may be allocated to fixed and mobile licensees in 100 sequential blocks ('XX') of 100K numbers ('XXXXX'). Once an initial allocation has been made within a particular value of range '083ZYY' (10M total numbers), CITC will generally designate all numbers within that range for the same licensee but, at its sole and reasonable discretion, may allocate within that range to another licensee for sequential allocation in blocks of 100K. The utilization ratio is 75% before the licensee may apply for a new block.

Source[15]

[15] : Consultation on 'Numbering for Machine-to-Machine Communications', Commission for Communications Regulation, Ireland(Comreg13 /33, 28th March 2013), "M2M number resource requirements and options" published by Telecom Engineering Centre, India, Nov 2015, National numbering Plan, Saudi Arabia; National numbering Plan(Issue 1 – 1 October 2016)Info-communications Media Development Authority, Singapore; National Numbering Plan, Hong Kong