

**TTC標準**  
Standard

JT-Q4062

IoT 試験フレームワーク

Framework for IoT Testing

第 1.0 版

2021 年 2 月 18 日制定

一般社団法人  
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE



本書は、一般社団法人情報通信技術委員会が著作権を保有しています。  
内容の一部又は全部を一般社団法人情報通信技術委員会の許諾を得ることなく複製、転載、改変、転用及びネットワーク上での送信、配布を行うことを禁止します。

## 目次

<参考>	4
1. 規定範囲	5
2. 参考文献	5
3. 定義	5
3.1 他の標準にて定義された用語	5
3.1.1 デバイス [ITU-T Y.4000/Y.2060]	5
3.1.2 Internet of Things (IoT) [ITU-T Y.4000/Y.2060]	5
3.1.3 コンフォーマンス試験 [ITU-T Y.4500.15/Q.3955]	5
3.1.4 Denial of Service (DOS) [ITU-T X.800]	5
3.2 本標準にて定義する用語	5
4. 略称	6
5. 慣例	7
6. 試験種別	7
7. 試験手順	8
7.1 コンフォーマンス試験	8
7.2 接続性試験	8
7.2.1 接続性試験	8
7.2.2 ストレス試験	9
7.3 互換性試験	10
7.4 ネットワーク種別分類のための応答時間試験	13
8. 試験手順の考慮事項	14
8.1 ネットワーク試験	14
8.2 ID 認証システム	16
8.3 試験タイミング	17
8.4 試験対象デバイスのグループ化	17
8.5 IoT デバイス遠隔試験	18
<b>付属資料 a 有線無線混在ネットワークにおける IoT デバイスおよび他の IP 機器の統合試験に対する考慮事項</b>	<b>23</b>
<b>Annex A</b>	<b>25</b>
<b>Appendix I</b>	<b>48</b>
<b>Appendix II</b>	<b>51</b>
<b>Appendix III</b>	<b>55</b>

## <参考>

### 1. 国際勧告などとの関連

本標準は IoT 試験のフレームワークについて規定しており、2020 年 9 月に ITU-T SG11 において発行された ITU-T 勧告 Q.4062 に準拠している。

### 2. 上記勧告などに対する追加項目など

#### 2.1 オプション選択項目

なし

#### 2.2 ナショナルマター決定項目

なし

#### 2.3 その他

本標準は上記 ITU-T 勧告に対し、有線と無線が混合したネットワーク環境での IoT 機器を含む IP 接続された機器の試験方法について付属資料（本付属資料は仕様の一部となる）を追加している。

#### 2.4 原勧告との章立て構成比較表

章立てに変更なし

### 3. 改版の履歴

版数	発行日	改版内容
第 1 版	2021 年 2 月 18 日	制定

### 4. 工業所有権

本標準に関わる「工業所有権の実施の権利に係る確認書」の提出状況は、TTC ホームページでご覧になれます。

### 5. その他

#### (1) 参照している勧告、標準など

TTC 標準

ITU-T 標準 Q.3952, Y.2060, Y.4500/Q.3955

ISO/IEC 標準

### 6. 標準作成部門

信号制御専門委員会

## 1. 規定範囲

IoT は、BAN、PAN、LAN、WLAN、LPWAN、FAN、MAN、WAN、セルラーネットワークなどのさまざまな異なるタイプの通信ネットワークに対し、多様なアクセス技術を使用する。したがって、単一アクセス技術を使用するドメインだけでなく、複数のアクセス技術を使用する統合ドメインにおける仕様適合性および相互運用性試験が IoT では必要である。

この勧告の主な目的は、複数のアクセス技術が用いられる統合ドメインの試験に適用する IoT の試験フレームワークを明確化することである。単一アクセス技術による統合ドメインの仕様適合性および相互運用性試験は、それらアクセス技術に関連する標準化団体で考慮されているため、この勧告の規定範囲外である。

## 2. 参考文献

以下の ITU-T 勧告およびその他の参考文献には、規定条項が含まれており、本標準の本文で参照することによって、本標準の規定条項を構成することになる。出版の時点では、表示されている版が有効である。これら全ての標準や勧告とその他の参考文献は、改定される可能性があるため、本標準の利用者は、以下に示された標準、勧告および参考文献の最新版の適用可能性を確認することを推奨する。現在有効である ITU-T 勧告リストは定期的に発行されている。この推奨事項内のドキュメントへの参照は、単独のドキュメントとして、推奨事項のステータスを示すものではない。

[ITU-T Q.3952] Recommendation ITU-T Q.3952, *Architecture and Facilities of Model Network for IoT Testing*.

[ITU-T Y.4000/Y.2060] Recommendation ITU-T Y.2060, *Overview of Internet of Things*.

[ITU-T Y.4050/Y.2069] Recommendation ITU-T Y.2069, *Terms and definitions for the Internet of Things*.

[ITU-T Y.4500.15/Q.3955] Recommendation ITU-T Y.4500.15/Q.3955, *oneM2M – Testing framework*.

[ITU-T X.800] Recommendation ITU-T X.800, *Security architecture for Open Systems Interconnection for CCITT applications*.

## 3. 定義

この標準では以下の用語を定義する。

### 3.1 他の標準にて定義された用語

この標準では、他の標準にて定義された以下の用語を用いる。

#### 3.1.1 デバイス [ITU-T Y.4000/Y.2060]

Internet of Things に関して、通信の必須機能、及び、センシング、アクチュエーション、データキャプチャ、データストレージ、およびデータ処理のオプション機能を備えた機器を示す。

#### 3.1.2 Internet of Things (IoT) [ITU-T Y.4000/Y.2060]

情報社会のためのグローバルインフラストラクチャ。既存および進化する相互運用可能な情報通信技術に基づいて（物理的および仮想的な）ものを相互接続することにより、高度なサービスを可能にする。

#### 3.1.3 コンフォーマンス試験 [ITU-T Y.4500.15/Q.3955]

実装がプロトコル標準に準拠していることを試験するためのプロセス。試験対象の実装に対して実行される試験スクリプトを使用して、プロトコルをシミュレートする試験システムによって実現される。

#### 3.1.4 Denial of Service (DOS) [ITU-T X.800]

リソースに対し許可されているアクセスの妨害、または、タイムクリティカルな操作の遅延。

### 3.2 本標準にて定義する用語

この標準で新たに定義する用語はない。

#### 4. 略称

本標準では、下記の略称を使用している。

6LoWPAN IPv6 over Low power Wireless Personal Area Networks

ACK	Acknowledgment
ADC	Analog to Digital Converters
AP	Access Point
ARB	Arbitrary Waveform Generators
BER	Bit Error Rate
CDF	Cumulative Distribution Function
CIR	Committed Information Rate
CoAP	Constrained Application Protocol
CRC	Cyclic Redundancy Check
DDoS	Distributed Denial of Service
DTE	Data Terminal Equipment
DUT	Device Under Test
EDGE	Enhanced Data Rates for Global System for Mobile Communications (GSM) Evolution
EIR	Excess Information Rate
FAN	Field Area Network
FCC	Federal Communications Commission
FIN	Finish
GPRS	General Packet Radio Service
GW	Gateway
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ID	Identifier
IoT	Internet of Things
IP	Internet Protocol
IS	Identification System
ISM	Industrial Scientific and Medical
JSON	JavaScript Object Notation
LE	Low Energy
LPWAN	Low Power Wireless Access Network
LTE	Long Term Evolution
LTE-A	LTE-Advanced
M2M	Machine-to-Machine
MAC	Medium Access Control
MAN	Metropolitan Area Network
MQTT	Message Queue Telemetry Transport
NB-IoT	Narrow Band Internet of Things
OBW	Occupied Bandwidth

OS	Operating System
PAN	Personal Area Network
PER	Packet Error Rate
QE	Qualified Equipment
QoE	Quality of Experience
QoS	Quality of Services
RBW	Resolution Bandwidth
REFhi	Maximum Radiated Power for highest channel frequency
REFlo	Maximum Radiated Power for lowest channel frequency
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
RST	Reset
RTMP	Real Time Messaging Protocol
RTSP	Real Time Streaming Protocol
RTT	Round Trip Time
Rx	Receiver
SDC	Smart Device Communications
SDO	Standards Developing Organization
SFD	Start of Frame Delimiter
SLA	Service Level Agreement
SQL	Structured Query Language
SSID	Service Set Identifier
SYN	Synchronization
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
UART	Universal Asynchronous Receiver/Transmitter
UDP	User Datagram Protocol
VBW	Video Bandwidth
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

## 5. 慣例

本標準で特記すべき慣例はない。

## 6. 試験種別

IoT デバイスの性能試験と特性の確認方法は、下記に示す4種類がある。IoT デバイスの特性、ネットワーク機器との通信に関する技術的フィージビリティ、及び、あらゆるタイプのネットワークのオペレーションの統一性を確認するためには、ネットワークおよびそのコンポーネントを試験する必要がある。

- コンフォーマンス試験：技術標準で規定された技術特性を保証する試験
- 接続性試験：当該アーキテクチャにおいて、IoT ハードウェアとネットワーク要素の正常な通信や、多様なネットワークのインフラストラクチャと IoT ネットワークの通信手法を決定する試

験

- 互換性試験：異なるサプライヤの IoT ハードウェアとソフトウェアのオペレーション互換性を確認する試験
- ネットワーク種別分類のための応答時間試験：ネットワークの応答時間に基づき、対象ネットワークの種別を推測する試験

## 7. 試験手順

### 7.1 コンフォーマンス試験

IoT デバイスおよび IoT システムを構成する多様な IoT 技術に関連するコンフォーマンス試験の要求条件は、それら IoT 技術に関連する標準仕様の要求条件により決定される。IoT のためのコンフォーマンス試験は、関連する試験仕様の標準に関する試験と類似している。コンフォーマンス試験の特性は IoT デバイスにより異なるため、試験の実行方法も多様である。

コンフォーマンス試験は本勧告の規定範囲外である。

### 7.2 接続性試験

#### 7.2.1 接続性試験

IoT フレームワークは、ネットワークを介したデバイス間の通信を可能にするために、IoT 通信技術およびプロトコル特有のインタフェースを持つべきである。IoT フレームワークの接続性試験手順は、標準やインタフェースに関する開発者マニュアルに基づく。

例えば、インタフェース試験が終了した時に、フレームワークのユーザはフレームワークの開発者が定義した全てのオペレーションと、試験によって得られたオペレーションの結果を比較し、試験が問題なく完了したか確認しなければならない。

IoT フレームワークは単一/複数プラットフォームの両方をサポートするコンフィグレーションマネージャを使用すべきであり、フレームワークは IoT 試験ツール、通信技術定義モジュール、リアルタイム統計ロガー、RF チャネルモデリングモジュール、キャプチャモジュール、グラフィカルなユーザインタフェース、遠隔制御モジュールの機器及び試験セット、入力データモデラ、セキュリティチェッカ、デモ設定ウィザードなどの拡張機能をもつモジュールを含むことができる。

通信技術定義モジュールは、試験で使用する RF 信号と波形セットを表現し、IoT デバイス間で相互作用する全試験プラットフォームで使用可能な信号を形成する外部の機器を制御することができる。

アプリケーションやネットワークレイヤで動作する WEB サーバベースの IoT 試験ツールモジュールは、ハードウェア、ファームウェア、モジュールベンダ、ソフトウェア、ネットワークのあらゆるタイプやバージョン間の互換性試験が実施できるよう構成される。IoT 試験ツールモジュールは、さまざまな IoT ベンダの異なる OS 上の試験アプリケーションや異なるデバイス間の相互接続性の試験をするための WEB サーバベースシステムとして機能する。

キャプチャモジュールは、IoT デバイスのプロトコルレイヤの性能を計測し、エンド・エンドのアプリケーションをセンサーからの符号化データを用いて試験することができる。

遠隔コントローラモジュールや試験セットは、RF 物理レイヤの形成、トリガと計測及び収集、電力消費量の計測など付加的な試験のために外部のあらゆる機器と通信することができる。

IoT デバイスは、電源に接続せずに数年間運用することが必要であるため、電力消費に対する要求条件は厳しく、電力消費やバッテリー寿命予測の検証のために試験環境下における電圧と電流を正確に測定しなければならない。そのための試験手順の詳細を付属資料 A (Annex A) に示す。



## 7.2.2 ストレス試験

IoT デバイスのストレス試験では、IoT デバイスとネットワーク間の通信を確認する。

ストレス試験の重要な目的として、IoT トラフィックに対するルータの安定性の検証がある。IoT のトラフィックとパラメータの特性は既存のトラフィックモデルと異なる。

IoT システムの開発や構築を計画する場合、アプリケーションとシステムの性能を確認することも重要である。

ネットワークの容量、遅延、トラフィック量、パケットロス、デバイス数また、デバイスのエネルギー消費や温度などの環境パラメータをストレス試験では考慮すべきである。図 7.2-1 に IoT デバイスのストレス試験モデルを示す。

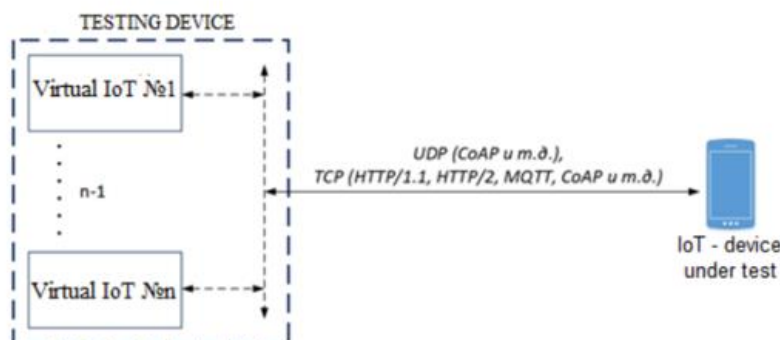


図 7.2-1 IoT デバイスのストレス試験モデル

試験デバイスに含まれる仮想 IoT (Virtual IoT) は、多数の IoT デバイスによる高負荷状態を模擬する必要がある場合において、実際の IoT デバイスをシミュレーションする機能である。仮想デバイスは、物理 IoT デバイスのすべての属性を持ち、識別子 (例えば、MAC アドレス) と論理アドレス (例えば、IPv4) を含む。

デバイスのストレス試験では、IoT デバイスの特徴である下記特性を持つトラフィックを生成する必要がある。

- ・ データフィールドがパケットヘッダより小さい
- ・ 膨大なパケット量 (ネットワークに接続した IoT デバイスが膨大であるため)
- ・ 時間分散に関するその他の法則 (IoT のネットワークではデバイス特性が類似することに加え、非持続的トラフィックを生成するため)

IoT デバイスのストレス試験では以下を考慮する。

- 1) ユニークなパラメータ (ユニークな MAC アドレス、IP、識別番号など) を使用した一連の試験デバイスを作成するための、仮想 IoT からの同時並列的なトラフィック生成。
- 2) 各仮想 IoT において、下記に示す主要なタイプの考慮。以下、主要タイプのデバイス例。
  - センサー (物理状態または化学成分を測定し、観察された特性に対応する電子信号を送信する電子デバイス)
  - アクチュエータ (入力信号によって励起された後、物理的な動作を開始するデバイス) ;
  - マルチメディアデバイス (マルチメディア情報、つまり、テキスト、画像、音声、映像、3 次元パノラマ画像、デジタルマップなど、さまざまな種類の情報コンテンツと情報の処理を使用してユーザが享受するデジタル情報を送信するデバイス)
- 3) IoT オペレーションの主なシナリオのサポート。各 IoT には、開発者によって定められた独自の動作アルゴリズムがある。以下、IoT シナリオの主なタイプ例。

- ・ 一定のデータ送信：
 

各デバイスが定期的にデータをリモートクラウドサーバに送信する。デバイスは、センサーとマルチメディアデバイスの2つのデータタイプをシミュレートし、それらは自己相似性を有するトラフィックを生成する。このシナリオでは、コネクションレス型（UDP など）のトランスポート層プロトコルが最も一般的に使用され、接続の確立をサポートするコネクション型トランスポート層プロトコル（TCP など）は一般的には使用されない。
- ・ 要求に応じたデータ送信：
 

このシナリオでは、2つのデータタイプのセンサーとマルチメディアデバイスを有する。リモートコントロールサーバで実行されているアルゴリズムに応じて、自己相似性を有するトラフィックと非持続型トラフィックの両方を生成できる。また、このシナリオでは、コネクション型トランスポート層プロトコル（TCP など）が最も頻繁に使用される。IoT とクラウドサーバの両方がグローバルネットワークにアドレスを持っている場合は、コネクションレス型トランスポート層プロトコル（UDP など）の使用が可能である。
- ・ 制御信号によるデバイスから周囲への影響：
 

このシナリオでは、デバイスをアクチュエータタイプにすることができる。リモートコントロールサーバで実行されているアルゴリズムに応じて、自己相似性を有するトラフィックと非持続型トラフィックの両方を生成できる。このシナリオでは、最も一般的に使用されるトランスポート層プロトコルはコネクション型（TCP など）であり、場合によってはコネクションレス型トランスポート層プロトコル（UDP など）を使用することができる。

- 4) 時間分散に関する法則に従って、各 IoT からさまざまなタイプのトラフィックを生成する機能。
- 5) コネクション型トランスポート層プロトコルの使用を必要とするシナリオの試験に必要な、遠隔試験サーバとの通信。このサーバは、IoT のトラフィックによる高い負荷に対する遅延レベルを測定するために必要である。

上記のストレス試験モデルの機能をサポートすることに加えて、デバイスは、PON (Passive Optical Network) インタフェース、イーサネットインタフェース、無線 LAN インタフェースなどのさまざまな主要なタイプの物理データ転送インタフェースをサポートする必要がある。

### 7.3 互換性試験

互換性試験は、複数のデバイスが共存する環境において、他のデバイスと並行した動作、また、必要に応じ他のシステム及び他のデバイスとの相互動作を試験する。

多様な IoT 技術の互換性試験の考慮点は、IoT デバイスやプラットフォームの互換性を確保するために、プロトコル間のデータ変換と特定の属性を用いたプロトコル自体の識別を考慮すべきである。互換性の確保に向けては、デバイス、アプリケーション、システム、ネットワークなどにそれぞれに対して、いくつかの互換性レベルを考慮する必要がある。

図 7.3-1～7.3-3 に IoT デバイス、IoT ゲートウェイ、IoT クラウドの互換性試験のアーキテクチャを示す。

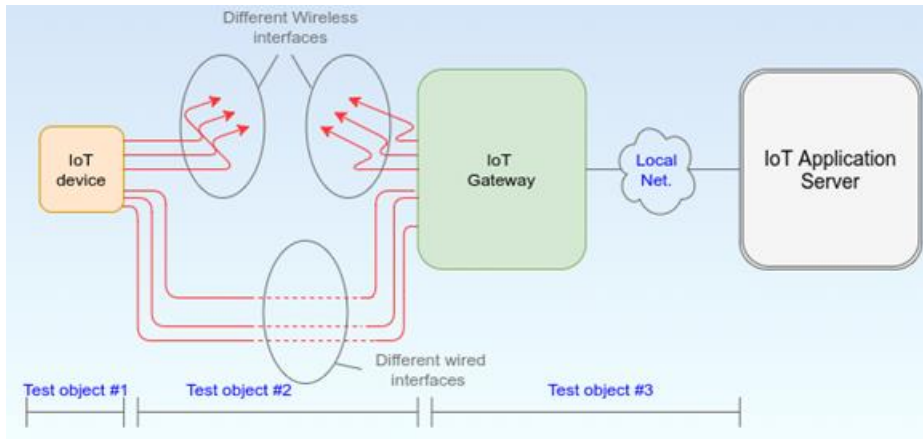


Figure. 7.3-1 IoT 互換性 デバイス試験

IoT デバイス試験の場合、図 7.3-1 に示すように、IoT デバイス、さまざまな有線および無線のインタフェース、IoT ゲートウェイとサーバのローカルネットワークで構成されるネットワーク部分が試験対象である。IoT デバイス試験は、センサーとアクチュエータ間の IoT インタフェース試験、さまざまなネットワークインタフェースを介したデータ送信のプロセス (図 7.3-1)、およびネットワークを介した IoT アプリケーションサーバとの互換性を対象とする。

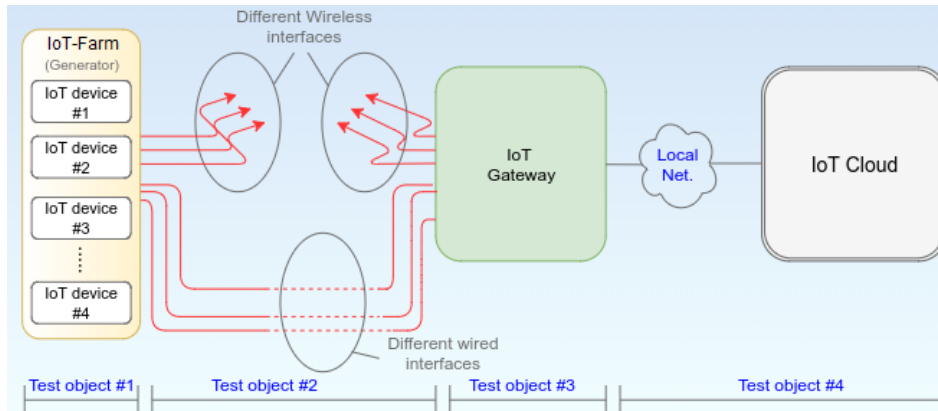


図 7.3-2 IoT 互換性 ゲートウェイ試験

IoT ゲートウェイ試験の場合、図 7.3-2 に示すように、複数の IoT デバイスで構成される IoT ファーム (IoT-Farm)、IoT ファームと IoT ゲートウェイ間の有線および無線インタフェース、IoT ゲートウェイと「ブラックボックス」のような IoT アプリケーションサーバとのローカルネットワークが試験対象となる。IoT ゲートウェイの試験には、定義された IoT ゲートウェイのインタフェース (有線および無線) を介した IoT ファームからの IoT デバイスとの互換性試験、IoT ファームからの IoT ゲートウェイの高負荷試験、および (ローカルネットワークとサーバの API 経由の) IoT ゲートウェイと IoT アプリケーションサーバの互換性試験が含まれる。

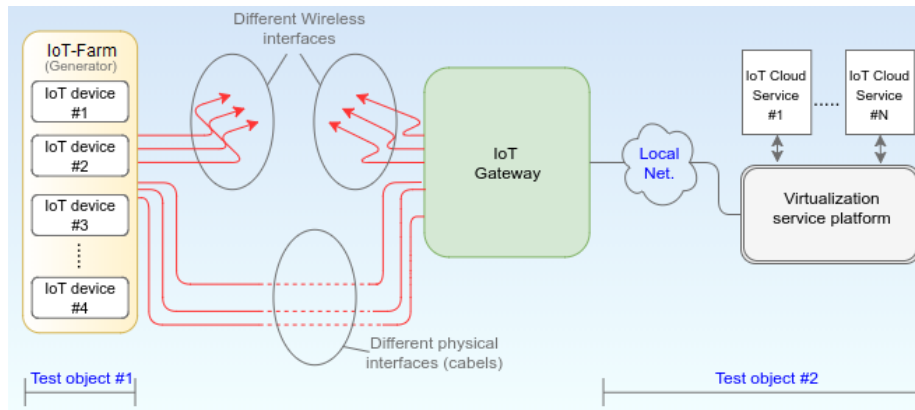


図 7.3-3 IoT 互換性 クラウドサービス試験

IoT クラウドサービス試験の場合、図 7.3-3 に示すように、IoT ファーム、及び、異なる IoT アプリケーションサーバを保有する仮想化サービスプラットフォームと接続するローカルネットワークが試験対象である。IoT クラウドサービス試験には、IoT デバイスと様々な IoT アプリケーションサーバ (API および定義された機能) 間の互換性試験、IoT ファームを使用した IoT アプリケーションサーバの高負荷試験が含まれる。

#### 互換性レベル

互換性試験では、次の互換性レベルを考慮する必要がある。

- ・ 完全な互換性 :  
IoT システムでは、情報リソースまたはその他の IoT エンティティは、入力および/または出力インタフェース、プロトコル、ソフトウェア、ハードウェアの変更や、(アダプター、ゲートウェイなど) デバイスを変換することなく、共有環境で情報を交換し、必要な機能を実行できる必要がある。
- ・ 互換性 :  
IoT システムでは、情報リソースまたはその他の IoT エンティティは、入力および/または出力インタフェース、使用されるプロトコル、ソフトウェア、ハードウェアを相互に、または環境に適合させる、あるいは、(アダプター、ゲートウェイなど) デバイスを交換することにより、共有環境で情報を交換し、必要な機能を実行できる必要がある。
- ・ 部分的な互換性 :  
IoT システムでは、情報リソースまたはその他の IoT エンティティは、ある程度情報を交換し、追加のツールの使用、入力を統合または変換、または出力インタフェース、使用されるプロトコル、ソフトウェアとハードウェアによって実装される手順により共有環境に必要な機能の一部を実行できる必要がある。部分的な互換性は、当事者間で機能に関する許容可能

な制約を交渉することによって達成される可能性がある。

- ・ 互換性無し：

IoT システムでは、情報リソースまたはその他の IoT エンティティは、その技術と機能要件または非機能要件の大きな違いにより、情報を交換したり、共有環境で必要な機能の一部をも実行したりすることができない。

#### 7.4 ネットワーク種別分類のための応答時間試験

ネットワーク種別分類のための応答時間試験では、対象ネットワークの応答時間の計測と、その結果によりネットワーク種別の推定を行う。応答時間は、対象となるネットワーク内の伝送遅延に関連する。また、非輻射状態における伝送遅延の数値範囲はネットワークの種別に関係するため、試験実施の前に非輻射状態の対象ネットワークに試験パケットを流入させて得られる伝送遅延と、伝送遅延の数値範囲により対象ネットワークの種別を推定することができる。Appendix A にネットワーク種別の分類の詳細を記載する。

この方法では、試験サーバと対象ネットワーク内の IoT デバイス間のラウンドトリップ時間 (RTT) を応答時間の尺度として使用する。試験サーバは、試験パケットを対象ネットワークの IoT デバイスに送信する。IoT デバイスは、試験パケットを受信すると、応答パケットを試験サーバに送り返す。試験サーバは、パケットの RTT を測定・収集し、RTT 値から対象ネットワークの種別を推定する。

試験ネットワークの例を図 7.4-1 に、また、ネットワーク種別分類の手順を図 7.4-2 に示す。この手順は次のとおりである。

1. P 個の試験パケット (図 7.4-1 の青いボックス : Testing Packet) をターゲットネットワークの Q 個のデバイスに送信する。
2. ターゲットネットワーク内のデバイスから応答 (図 7.4-1 の緑色のボックス) を受信し、試験パケットの送信から応答パケットの受信までの経過時間として RTT を測定する。
3. 試験の実施時期 (testing period) を変更し手順 1 と手順 2 を N 回繰り返す。ここで、N はラウンド数を示す。対象ネットワークの非輻射状況を見つけるため、各ラウンドの試験実施時期をランダムに (図 7.4-3 (a) 参照)、またはラウンドロビン方式で (図 7.4-3 (b) 参照) 変更する。
4. M 個の最小 RTT 値を選択し、選択した RTT 値の平均を算出する。ここで、M の値は P (試験パケット数)、Q (デバイス数)、N (ラウンド数) を超えないものとする。
5. 平均 RTT 値から対象ネットワークの種別を推定する。

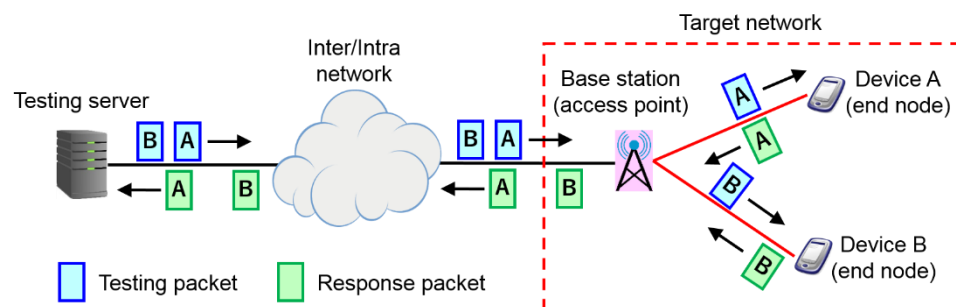


図 7.4-1 試験ネットワークの一例

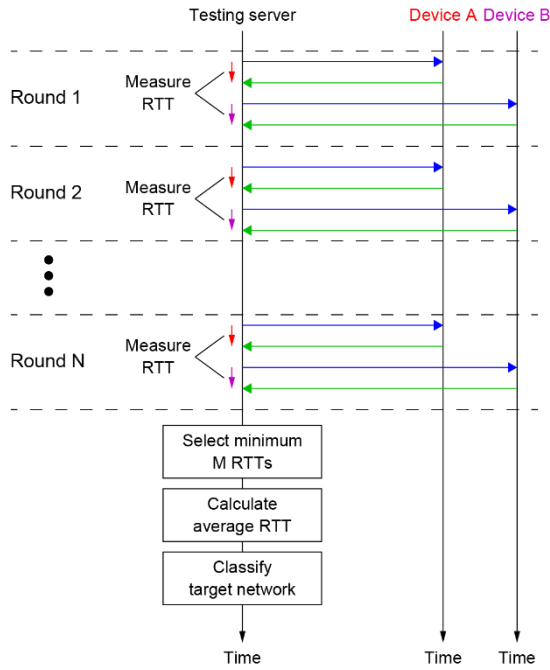


図 7.4-2 ネットワークタイプ分類試験の手順

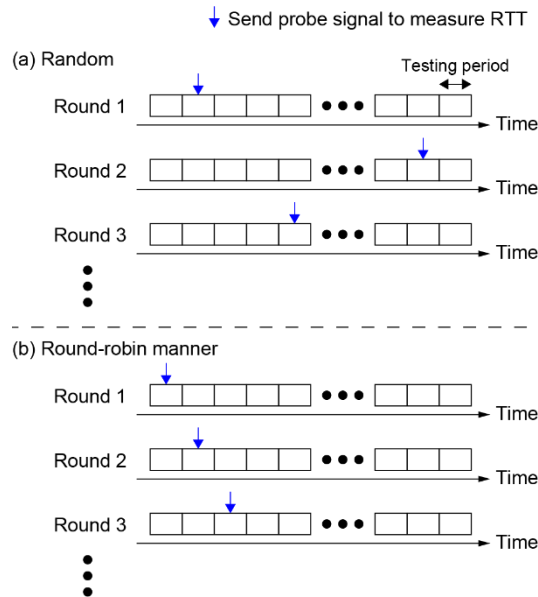


図 7.4-3 試験パケット送信タイミングの一例.

## 8. 試験手順の考慮事項

### 8.1 ネットワーク試験

#### 8.1.1 実ネットワークにおける試験

IoT デバイスとアプリケーションの試験は、それらが実際に動作する環境で行われるべきである。実ネットワークを使用することで、IoT デバイスとアプリケーションのあらゆる種類の試験を行うことが可能であり、また、その結果により IoT デバイスとアプリケーションが実際に使用される環境における性能が明らかになる。

### 8.1.2 モデルネットワークにおける試験

技術的または経済的な問題のために実ネットワークですべての試験を実行することが不可能な場合は、代替のアプローチが必要である。勧告 ITU-T Q.3952：「IoT テスト用のモデルネットワークのアーキテクチャと設備」は、さまざまな IoT 統合シナリオが実装されているモデルネットワーク（図 8.1-1）を示している。勧告 Q.3952 では、IoT デバイス試験に使用されるモデルネットワークのアーキテクチャを定義し、モデルネットワークの個別のセグメントを提示している。モデルネットワークは、設計されたネットワークと既存のネットワークの両方のアーキテクチャ、およびそれらの様々な組み合わせを再現している。トラフィックジェネレータ、遅延、干渉などの追加の構造単位を適用することで、あらゆるシナリオでネットワークを試験することができる。

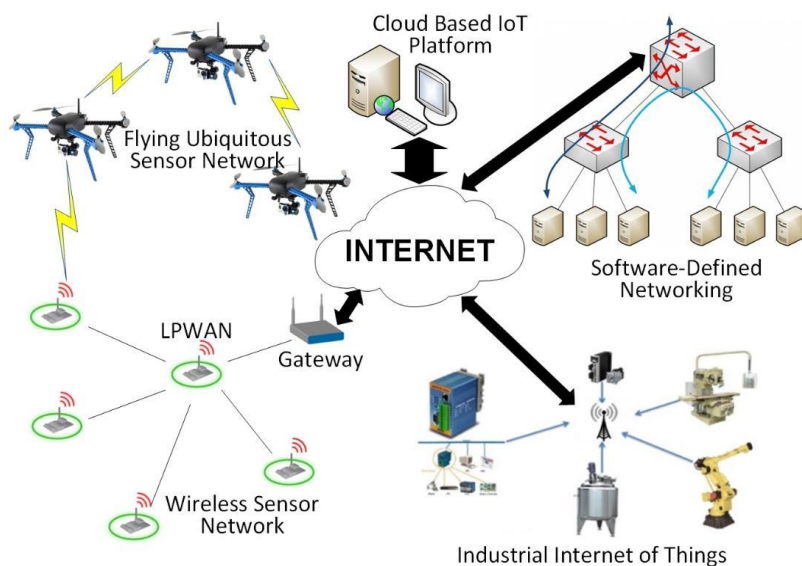


図 8.1-1 IoT デバイス及びアプリケーション試験のためのモデルネットワークの構成 [ITU-T Q.3952]

モデルネットワークには個別ネットワークと分散ネットワーク 2つのタイプがある。個別ネットワークとは、他のモデルネットワークとは接続されていない公共通信ネットワークの一部である。これは、一般的な試験と互換性および相互接続性の試験に使用される。個別ネットワークは、データリンク層によって相互接続された少なくとも 2つのノードによって構成され、ノードの 1つは試験対象の機器であり、もう一方は当該モデルネットワークである。分散モデルネットワークは、公共通信ネットワークまたは他のタイプのネットワークを介して接続された複数のモデルネットワークと考えることができる。これは、QoS パラメータのチェック、及び、ネットワークと情報セキュリティ対策への準拠の要件同様に他の技術要件との互換性と相互接続の試験に使用される。

モデルネットワークは、物理形式と仮想形式のどちらの手法でも実装できる。仮想形式では、実際のハードウェアより膨大な範囲をエミュレートできる。これにより、多数のネットワーク構成要素が単一のソフトウェアプラットフォームで実現できるため、ネットワーク機器コストとネットワーク構築コストを削減できる。

セグメント化は、モデルネットワークの構造を簡略化するための手法であり、ネットワークを個々のセグメントに分割することである。各セグメントでは、シミュレートされた技術を使用し、その特性を反映するように設計された公共通信ネットワークセグメントの運用を可能とする。個々のセグメントの運用シナリオを事前に規定できるため、システムを柔軟に構成できる。

## 8.2 ID 認証システム

IoT 試験の初期段階における認証として、ID 認証システムを使用すべきである。ID 認証システムの種別により IoT デバイス試験方法は異なる。全ての ID 認証システムは以下の要求条件を満たす必要がある。

- ID 認証システムは、一意的な IoT 識別子により IoT デバイスを一意に特定すること
  - ID 認証システムは、IoT デバイス間の通信のために特異なセキュリティシステムをサポートすること
  - ID 認証システムは、如何なるデータ種別に対してもデータ伝送サービスの条件を満たすこと
- 選択する ID 証明システムは開発者や標準的な要求条件を満たさなければならない。



### 8.3 試験タイミング

セルラーネットワーク、無線 LAN、LPWAN などの無線ネットワークのサービス品質は、ネットワークの種類、運用環境、時間帯によって大きく変化する。無線ネットワークの輻輳レベルは日中変動し、輻輳レベルのパターンは、図 8.3-1 に示すように、オフィスや住宅地など地域によって異なる。無線アクセスネットワークに接続された IoT デバイスを含むすべての機器の試験を効率的に行うためには、ネットワークの種別ごとに試験タイミングを考慮する必要がある。図 8.3-1 の場合、オフィスエリアでは、混雑度が比較的低く、試験パケットのトラフィック量の増加によるネットワーク混雑を回避できる可能性があるため、深夜または早朝を試験タイミングとして選択することが推奨される。住宅地では、正午頃に試験のタイミングを選択する方が良いかもしれない。多くのデバイスを一度に試験できることも、このタイミング選択の利点である。

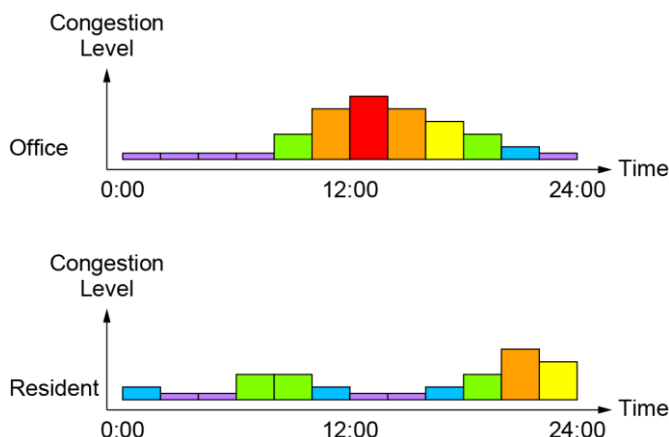


図 8.3-1 輻輳レベルの変動の例

### 8.4 試験対象デバイスのグループ化

一般的に、IoT の試験では試験対象のデバイスの数は膨大であるため、試験の過程においてネットワークに膨大な試験パケットが投入され、試験の実行によりネットワークの輻輳を引き起こす場合がある。このことから、試験トラフィックのための不要な帯域を削減し、アクセス技術の帯域の容量超過を回避するために、試験対象デバイスをいくつかのグループに分割し、グループ毎に異なるタイミングで試験を行うことが望ましい。このことにより、試験全体に要する時間を短縮することが可能になる。

デバイスの複数グループへの分割の例として、デバイスの識別子による分類、伝送速度や遅延などのデバイスの通信特性による分類などがある。

#### ● デバイスの識別子によるグループ化

試験対象デバイスにはそれぞれ独自のデバイス識別子がある。対象ネットワークで複数の（サブ）グループを作成する場合、デバイス識別子に基づいてグループ化することが最も簡単な方法の 1 つである。対象ネットワークが IP ネットワークの場合、試験対象デバイスは次の方法でグループ化できる。

##### ➤ IP アドレスによる分割

一般に、対象ネットワークは IP アドレスの範囲が異なる複数のネットワークセグメントで構成されているため、ネットワークセグメントごとに試験対象デバイスを容易にグループ化できる。

##### ・ IP4 ネットワークの場合の分割例

aaa.bbb.ccc.0~aaa.bbb.ccc.255 を aaa.bbb.ccc.0~127 と aaa.bbb.ccc.128~255 に分割

##### ・ IPv6 ネットワークの場合の分割例

GGGG:HHHH:IIII:JJJJ:0:0:0:0~GGGG:HHHH:IIII:JJJJ:ffff:ffff:ffff:ffff を

GGGG:HHHH:IIII:JJJJ:0:0:0:0~GGGG:HHHH:IIII:JJJJ:7fff:ffff:ffff:ffff と

GGGG:HHHH:IIII:JJJJ: 8000:0:0:0~GGGG:HHHH:IIII:JJJJ:ffff:ffff:ffff:ffff に分割

➤ ドメイン名による分割

通常、1つ以上の範囲の IP アドレスが（サブ）ドメイン名に割り当てられる。したがって、IP アドレスに基づくグループ化と同様に、試験対象デバイスは次のように（サブ）ドメイン名でグループ化できる。

- DOMAIN\_NAME1.com と DOMAIN\_NAME2.com に分割
- SUBDOMAIN\_NAME1.MMM.com と SUBDOMAIN\_NAME2.MMM.com に分割

対象ネットワークが非 IP 網である場合は、MAC アドレスやネットワーク依存のデバイス識別子を利用することも可能である。以下にネットワーク依存のデバイス識別子の例を示す。

- LoRa ネットワーク: DevAddr 或いは DevEUI
- Wi-SUN: Destination PAN ID 且つ/1 または Destination Address
- ZigBee: DstAddress

●通信特性に基づくグループ化

対象ネットワークには通常、伝送速度や RTT 値などの通信特性がある。これらの特性を用いて試験対象デバイスをグループ化することにより、対象ネットワークに送信可能な試験パケットの量を予測でき、試験パケットによる輻輳を回避することができる。例えば、次の通信特性を使用して、試験対象デバイスをグループ化する事が可能である。

➤ 伝送速度に基づくグループ化

対象ネットワークに送信できる試験パケットの量、または、一度に試験対象デバイスに送信できる試験パケットの量は、試験対象デバイスの伝送速度によって異なる。伝送速度の異なるデバイスが共存する場合は、複数のデバイスグループにグループ化して、同じグループ内のデバイスの伝送速度を同じにすることができる。伝送速度に基づいて試験対象デバイスをグループ化し、適切なパケット転送レートで試験パケットを送信することは効率的な試験実行の方法である。伝送速度は時間とともに変化するため、効果的な試験を実行するには、瞬時伝送速度を使用して試験対象デバイスをグループ化する必要がある。平均伝送速度もパフォーマンス評価試験の場合のグループ化にも使用できる。

➤ RTT 値に基づくグループ化

一部のデバイスグループで、すべて、または、一部のデバイスの RTT 値が異常に大きい場合、これらのデバイスが接続されているネットワークが輻輳している可能性がある。これは、各デバイスが試験/応答パケットを送信する機会が少なく、衝突による再送信がネットワークで頻繁に発生するためである。このような場合、元のデバイスとは異なるタイミングでデバイスを試験するために、そのデバイスをグループから分離して、RTT に基づき新しいデバイスグループを作成するか、または、他のデバイスグループに入れることもできる。

## 8.5 IoT デバイス遠隔試験

### 8.5.1 デバイスの検出と分類

IoT デバイスの検出は試験の中で最も重要なステップである。オープンなネットワークポートのスキャンは、IoT デバイスの検出に使用される場合がある。

試験対象の IoT デバイスが発するトラフィックが経由するデータリンクにアクセスせずに IoT デバイスを検出するには、インターネットに接続されているデバイスをスキャンしてオープンなネットワーク通信ポート

を見つける既存のポートスキャンが利用可能である。IoT では、多くの場合、TCP、UDP のトランスポート層プロトコルを利用するため、TCP、UDP ポートの検出をするためのスキャンも実行する。

TCP ポートスキャン実行には複数の方法がある。最も早く容易に実行可能な方法は、仮想スキャンデバイスが組み込まれているオペレーティングシステムのネットワーク機能を使うことである。仮想スキャンデバイスは連続的にポートスキャンを繰り返し実行し、ネットワークノードでオープンなポートを分析する。分析したデバイスにオープンなポートがあることを検出すると、オペレーティングシステムは、SYN, SYN-ACK, ACK を用いた three-way handshake である 3 ステップの確立手順を実施し、その後接続に利用可能なポートを確認し、その後ポートをクローズする。一連の分析プロセスでは、仮想スキャンデバイスの異なるポートから複数のポートに対し並列にスキャンを行うことで、所要時間を削減することができる。

UDP ポートのスキャンは、コミュニケーションセッションの概念がなく、分析するデバイスのポートのデータが到達する保証がないため、スキャン実行にはより多くの時間とコストを要する。しかしほとんどのコミュニケーションノードでは、ICMP メッセージの送出によりクローズした UDP ポートへの流入パケットに回答するためネットワークポートは利用不可であることが分かる。また、このメッセージに回答がない時は UDP ポートがオープンであることが分かる。この方法はデータ伝送の保証がないため、1 ポートに対して複数の要求を送信する必要がある。

IOT の多くは、前述のような特定のネットワークポートを占有する特定のデータ転送プロトコルを使用する。例としては、CoAP、MQTT、HTTP、HTTP/2、RTMP、RTSP などがある。非営利団体「Internet Assigned Numbers Authority」（以下「IANA」）は、特定の目的に使用される固定ポートデータ番号を決定し、それらの番号と適用されるアプリケーション層プロトコルとの間の対応を確立する。スキャンしたデバイスで検出されたネットワークポートのリストと IANA データベースを比較することにより、このネットワークポートで使用されているアプリケーションデータ転送プロトコルを判別できる。

データ転送に TCP を使用する IANA データベースのリストにない他のポートは、通常、任意の要求に対して応答を送信する。デバイスから受信した応答により、ポートが使用しているアプリケーション層プロトコルを判別できる。

IOT デバイスの種別を判別するために、要求に対して受信した応答のデータフィールドを分析する。たとえば、HTTP 要求への応答には、オペレーティングシステムや製造元の名前など、デバイスに関する情報が含まれる場合がある。

下記に HTTP ヘッダの例を示す：

```
HTTP/1.1 200 OK;  
Date: Wed, 26 Jan 2016 11:06:42 GMT;  
Server: Linux/2.x UPnP/1.0 Avtech/1.0;  
Connection: close;  
Last-Modified: Wed, 08 Jan 2014 09:36:39 GMT;  
Content-Type: text/html.
```

“Server” ヘッダには下記有効な情報が含まれる：

- Linux/2.x - デバイスが使用するオペレーティングシステムのコア；
- UPnP - ホームあるいは共同する環境でデバイスの接続専用のネットワークプロトコルのセットを含むテクノロジー；
- Avtech- ビデオカメラメーカー

以上のことから、応答を受信したデバイスはビデオカメラであると推定できる。

デバイス種別は、使用するプロトコルとオープンなポートから受信した応答に基づき決定される。たとえば、HTTP を使用し次のヘッダを使用して応答を送信するオープンポート 15757 のデバイスがある。

```
HTTP / 1.1 401 N / A
Router Webserver
close
Basic realm = "TP-LINK Wireless N Router WR841N"
5. text / html
```

上記のオープンポートの情報とヘッダ情報から、デバイスの種別はワイヤレスルーターと推定できる。IoT で使用する多くのデバイス（特にビデオカメラ、家電製品などのシリアルデバイス）には Web インタフェースがある。このようなデバイスの Web ページ情報の分析は、デバイス種別を判別するのに役立つ。この IoT デバイス種別の決定方法は、すべての IoT デバイスに Web インタラクティブインタフェースを有する Web of Things の概念の出現により、より適切になっていることは注目に値する。

ただし、デバイスに Web インタフェースがないこと、または HTTP、HTTPS、および HTTP/2 を介して動作するオープンなネットワークポートがないことは、そのデバイスが IoT デバイスではないことを意味するものではない。Web of Things の概念をサポートしていないが、インターネットに接続されている IoT 通信プロトコルは他にも多くある。この点で、ポートスキャンによる IoT デバイス種別特定は、受信したパケットのデータフィールドに含まれる情報を分析できるように、IoT の一般的なプロトコルごとに応答形式をデータベースとして持つ必要がある。検索システムの構造の例を図 II. 1 に示す。

特定のアルゴリズムを使用してデバイスに関する利用可能なすべての情報を分析することで、デバイスが IoT デバイスであるかどうか、その種別を判別し、通信するためにデバイスにアクセスすることができる。詳細については、付録 II (Appendix II) を参照。

### 8.5.2 IoT デバイスの遠隔試験

パケット分析システムは、情報パケットからの情報に基づき（特殊なプロトコル、デバイスからのパケットの平均サイズ、パケット送信頻度、トラフィックの非持続性や自己相似性、使用されるネットワークポートのセット、パケットが属するデバイス上のオペレーティングサーバに関する情報などの）IoT デバイスを特徴付ける一意のパラメータを利用して、ローカルネットワークを通過するトラフィックをスニффイングしてデバイスを判別する。このように、取得できる情報を用いてパケット分析システムはローカルネットワークで動作している IoT デバイスを判別できる。

モデルネットワークに基づいて、IoT デバイスの遠隔試験の手法を確立することを推奨する。IoT デバイス（既知の IP アドレス用）を「ブラックボックス」とすることが提案されている。試験の過程で、特別なリクエストがリモートサーバを備えた IoT デバイスに送信され、そのリクエストはネットワークインタフェースへの入力となる。リクエストを受信した後、IoT デバイスはネットワークインタフェースの出力から応答サービスパケットを送信する。リモートクラウドサーバは受信したこれらのパケットをさらに分析する。IoT デバイスの試験では、IoT デバイスインターフェイスの 1 つの IP アドレスまたは追加の識別子と、IoT 識別サーバのデータベースに保存されている一意の識別子が必要である。

IOT デバイスからパケットを受信するクラウドサーバは、IoT デバイスによって処理および送信されるパケットのフォーマットを識別する。トラフィックの詳細な分析をすることにより、パケットのフォーマットとその構造は決定される。ここで、IoT デバイスの暗号化を使用する場合は、最初に IoT デバイスとのインタラクションを調整するためのキーを取得する必要がある。

IOT デバイスからのパケットの形式に関するデータを利用し、IoT デバイスの種別を判別できる。

- アクチュエータタイプ；
- センサータイプ（ITU-T Y. 4050 / Y. 2069）；
- 混合タイプ（アクチュエータとセンサの両方）。
- マルチメディア情報を転送するためのデバイス（ITU-T Y. 4050 / Y. 2069）；

試験サーバは、試験デバイスから試験対象のデバイスに関する情報を受信する。試験デバイスは、パケット分析システムを使用して、ローカルネットワーク内のデバイスを検出する。

IoT デバイスの遠隔試験のモデルを図 8.5-1 と図 8.5-2 に示す。IoT デバイスの遠隔試験のアルゴリズムを図 8.5-3 に示す。

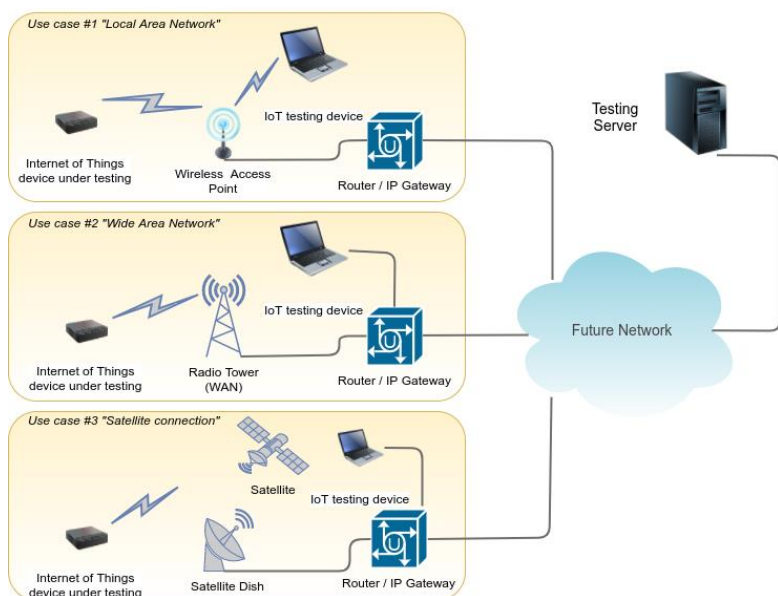


図 8.5-1 無線技術のための IoT デバイスの遠隔試験の一例

この方法はローカル IPv4 / IPv6 ネットワーク内にある試験デバイスを使用した IoT デバイスの遠隔試験の際に使用される。モバイルデバイス（車両、衛星など）が IPv4 / IPv6 ネットワークに基づいて動作し、試験デバイスが試験対象のデバイスをインターネットに接続する通信チャンネルにアクセスできる場合、この試験方法を使用できる。

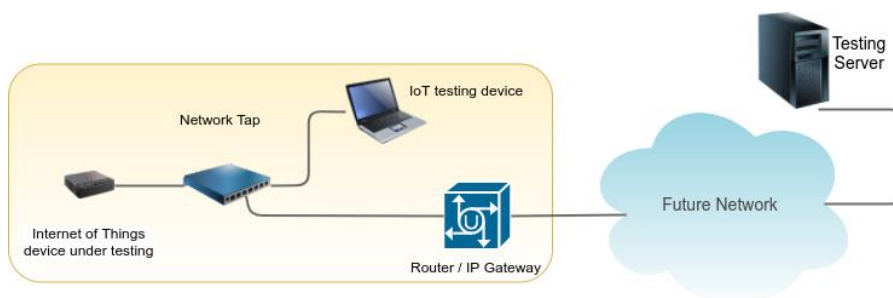


図 8.5-2 優先技術のための IoT デバイスの遠隔試験の一例

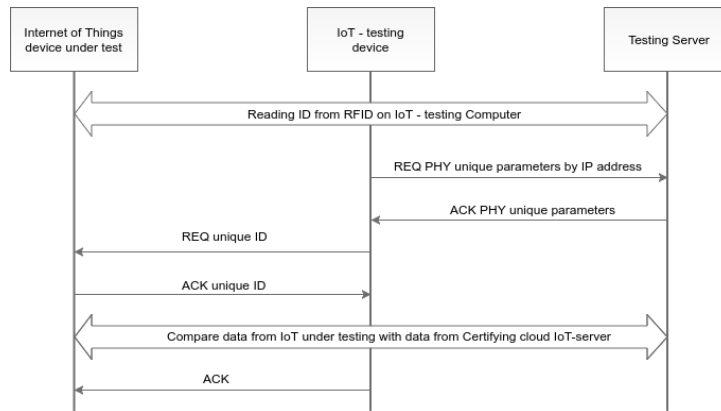


図. 8.5-3 IoT デバイス遠隔試験のアルゴリズム

デバイスを検出するプロセスを図 8.5-3 に示す。

IoT 試験デバイスは、デバイスの検出プロセス中に、IoT デバイスからのトラフィックデータに基づいて、パケット分析システムを使用してデバイスの種別を判別する。次の設定を使用して分析できる：プロトコルタイプ (CoAP、MQTT など)、パケットの平均サイズ、パケット伝送速度、トラフィックプロファイルなど。その後、IoT デバイスが試験サーバで初期化される。手順を以下に示す。

1. 試験中の IoT デバイス (ID、IoT 識別サーバのデータベースに保存されている一意の識別子) の識別子を転送する。
2. IoT 試験デバイスが、試験サーバから試験中の IoT デバイスの転送された IP アドレスに基づいて一意の物理パラメータを要求する。
3. 試験中の IoT デバイスと IoT 試験デバイス間でサービスメッセージの交換が行われ、デバイスの ID を確認する。
4. 試験を実行する。試験実行後、パケットが分析され、認証済みのクラウド IoT サーバからのデータと比較される。試験が完了すると、試験デバイスは試験中の IoT デバイスに確認応答を送信する。

パケットフォーマットと IoT デバイス種別を決定することによりパケットを生成可能になる。IoT デバイスの脆弱性と特性のチェックは次のように行われる。

- コンピューティングデバイスとインタフェースするための標準ポート (80、8080、21、22、23 など) の可用性を確認する。
- プロンプトが表示された時、または誤った値を送信した時に IoT デバイスの動作を確認する。
- DDoS 攻撃に対する IoT デバイスの脆弱性をチェックする。

## 付属資料 a 有線無線混在ネットワークにおけるIoTデバイスおよび他のIP機器の統合試験に対する考慮事項

(本付属資料は仕様の一部である。)

### a. 1. 概要

ITU-T 勧告 Q. 4062 は、有線無線混在ネットワーク環境における IoT デバイスの試験方法について規定している。日本国内において、IoT デバイスだけでなく IP で接続された全ての機器を統合的に試験するために、本勧告の記載項目のうちいくつかを検討すべきである。

### a. 2. IoT デバイスおよび他の IP 機器の統合試験

一般的に通信ネットワークは、図 a. 1 に示すように、有線で接続された有線網とセルラ網のような基地局からデバイスまで無線接続された無線網によって構成される。無線網には、IoT デバイス向けの小電力無線アクセス (LPWA) 網や無線 LAN などを含む。

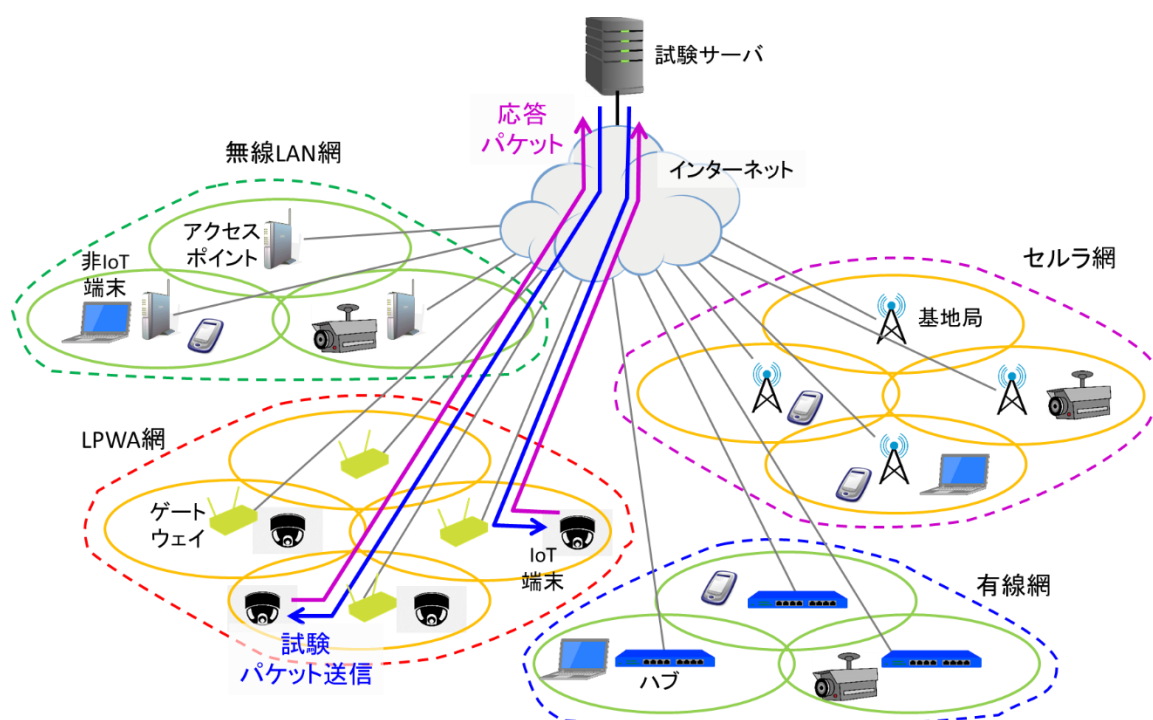


図 a. 1 有線無線混在ネットワークの IP 機器の統合試験

このような通信ネットワークには、IoTデバイスだけでなくパーソナルコンピュータ (PC) などの非IoT端末もIPにより接続されている。遠隔に設置された試験サーバからIP機器の接続性などを試験する場合には、有線網、無線網を含めIP機器が接続されているネットワークの形態を考慮する必要がある。

### a. 3. 統合試験実施時の考慮事項

有線無線混在ネットワーク環境における IoT デバイスを含む IP 機器の試験を実施する場合、IP 機器が接続されたネットワークを推定するため、本標準の本文に示された以下の項目を考慮する必要がある。

#### ー 7.4 ネットワーク種別分類のための応答時間試験

また、通信ネットワークが大規模になることから、試験実施時に本標準の本文に示された以下の項目を考慮することが望ましい。

- － 8.3 試験タイミング
- － 8.4 試験対象デバイスのグループ化



## Annex A

### Testing specifications

(This annex forms an integral part of this Recommendation.)

There is reference information about types of testing which include CIR test, EIR, Test of Traffic Policing. Some of references are based on example networks, such as BLE, ZigBee, Thread. Also, there are compulsory types of functional testing, objectives and conditions of their conduction, schemes of connection (configuration of stand), and the requirements for the report for each of the given tests. There are also examples of tables and formulas for calculations, which should also be presented in the report on the relevant type of testing.

### ***Ethernet testing (standards 10Base-T, 100Base-T, 1000Base-T, 10GBase-T)***

**Table A.1**

Test number	№01
Test name	The network configuration testing
Testing Layer	Network
Type of Test	Functionality
Status	Optional
Test goal	The services testing on the SLA conformity
Configuration	<pre> graph TD     QE[QE] --- ROUTER[ROUTER]     ROUTER &lt;--&gt; DUT1[DUT]     ROUTER &lt;--&gt; DUT2[DUT]     style DUT1 fill:none,stroke:none     style DUT2 fill:none,stroke:none             </pre>
Testing procedure	<ol style="list-style-type: none"> <li>1. Test CIR;</li> <li>2. Test EIR;</li> <li>3. Test Traffic Policing.</li> </ol> <p><i>*The time for each test is not more than 60s</i></p>
Expected results	SLA conformity

#### ***Test device***

IoT device with Ethernet interface.

#### ***Test CIR***

Test CIR is the test for definition of guaranteed capacity. Test can be conducted for load 25 %, 50%, 75%, 100% of guaranteed capacity. The schedule of the CIR test is shown on the Figure. A.1.

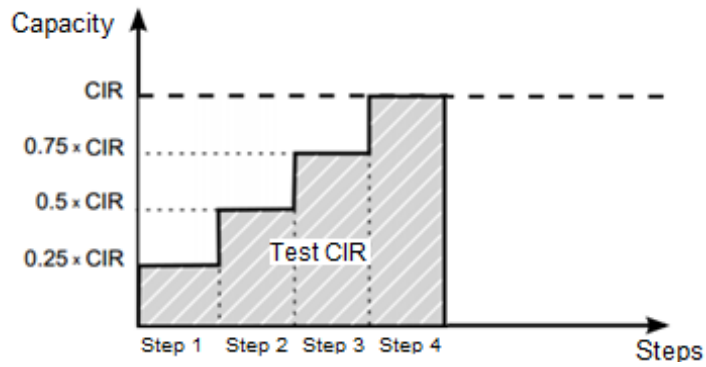


Figure A. 1 – The schedule of the CIR test

**Test EIR**

Test EIR is the test for verification that the capacity to each service will not more than permissible value when the load value is the CIR+EIR. This test is conducted in the conditions from guaranteed capacity CIR up to maximum of the non-guaranteed capacity EIR (Best Effort conditions). The schedule of the EIR test is shown on the Figure. A.2.

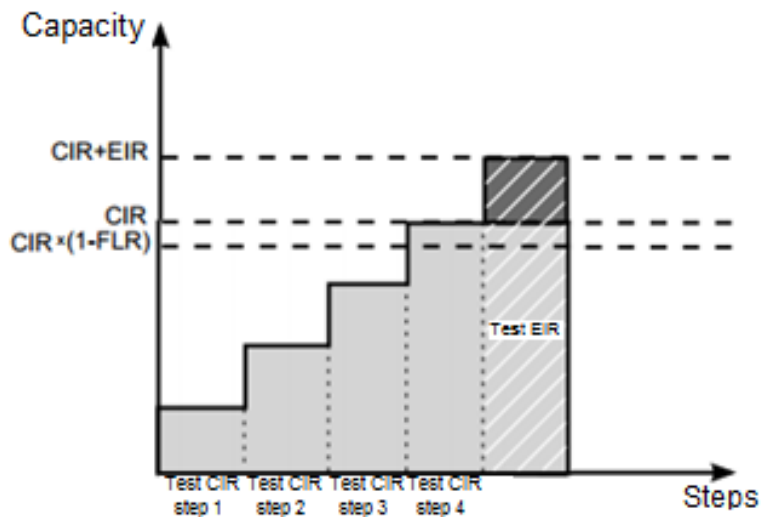


Figure A. 2 – The schedule of the EIR test

**Test of Traffic Policing**

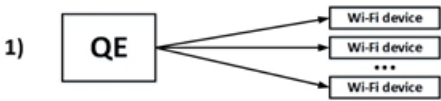

Test of Traffic Policing is conducted for verification that the network will limited the capacity to separate service if the real traffic of this service will be more than authorized traffic.

**Report of Testing**

The guaranteed and non-guaranteed capacity which were observed during testing should be marked in the report.

**IEEE 802.11 (WLAN) standard testing**

Table A.2

Test number	№02
Test name	The complex test of WLAN with using precision measuring equipment which allows simulation of the real network performance simulation.
Testing Layer	Network
Type of Test	Functionality
Status	Mandatory
Test goal	The definition of the value of the main WLAN networks parameters (SSID, RSSI, frequency, encryption type, BER, PER, channel utilization and so on.)
Configuration	<p>1) </p> <p>2)* </p> <p>* Simulating a real WiFi network</p>
Test procedure	<ol style="list-style-type: none"> <li>1. Set up measuring equipment in accordance with its technical terms and conditions.</li> <li>2. Detect the WLANs which should be testing.</li> <li>3. Define the values of the main parameters.</li> </ol> <p>*The measurement equipment can allow simulate the wireless channel with different errors.</p>
Expected results	The set of WLAN parameter values.

**Test device**

IoT devices with WLAN interfaces, WLAN AP.

**Testing procedure**

The following metrics should be tested:

- mobility;
- interoperability with WLAN equipment;
- the main parameters that estimate the WLAN throughput and QoS and QoE;
- scalability.

At first, the tests should be made for main parameters without traffic. The load testing should be made on the next step when the real networks conditions will be simulated.

The precision measuring equipment, such as oscilloscope and spectrum analyzer, can be used for testing.

**Report**

The report about testing performed in the table which includes the following parameters:

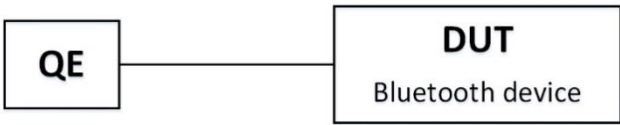
- WLAN network identifier (SSID);

- the received signal strength (RSSI);
- frequency;
- encryption type (WEP, WPA, WPA2);
- BER (permissible value  $10^{-5}$  for WLAN) [19];
- PER (permissible value  $10^{-2}$  for WLAN) [19];
- channel utilization (in %).

*\*The table can be extended if testing scenario requests to add some special parameters.*

**IEEE 802.15.1 (Bluetooth, Bluetooth LE) standards testing**

**Table A.3**

<b>Test number</b>	<b>№03</b>
Test name	BER definition
Testing Layer	Network
Type of tests	Functionality
Status	Mandatory
Tests goal	BER definition on the IEEE 802.15.1 standard base
Configuration	
Testing procedure	<ol style="list-style-type: none"> <li>1. Connect QE and Bluetooth device;</li> <li>2. Generate the pseudo-random bit sequence at the Bluetooth device;</li> <li>3. Define the value of BER.</li> </ol>
Expected results	Value of BER

**Test device**

IoT device with Bluetooth interface.


**Report**

The testing results should be reported in the table.

**Table A.4**

<b>№</b>	<b>Number of the bit which were send</b>	<b>BER</b>	<b>Check sum (CRC)</b>	<b>Time</b>
1				
2				
...				
n				

Table A.5

<b>Test number</b>	<b>№04</b>
Test name	PER definition
Testing Layer	Network
Type of Tests	Functionality
Status	Mandatory
Tests goal	PER definition on the base of standard IEEE 802.15.4
Configuration	 <pre> graph LR     subgraph QE [QE]         ZGW[ZigBee GW]     end     subgraph DUT [DUT]         ZEP[ZigBee End Point]     end     ZGW --- ZEP             </pre>
Testing procedure	<ol style="list-style-type: none"> <li>1. Connect GW and ZigBee End Point;</li> <li>2. Generate at ZigBee-device specified number of packets;</li> <li>3. Define PER.</li> </ol>
Expected results	PER values

**Test device**

IoT device with ZigBee interface.

**Testing procedure**

ZigBee End Point device and ZigBee gateway are used for testing. The value of RSSI is observed on the ZigBee micro controller and PER is calculated. A generic purpose sniffer software can be used for detailed packets analysis.

**Report**

The testing results should be reported in the table.


Table A.6

№	RSSI	Number of packets which were send	PER	Probability of packets delivery	Time
1					
2					
...					
n					

**Mobile technologies testing**

Table A.7

<b>Test number</b>	<b>№05</b>
Test name	Mean value of data transmission rate

Testing layer	Network
Type of tests	Functionality
Status	Mandatory
Tests goal	Mean value of data transmission rate in case of web-content download
Configuration	
Testing procedure	<ol style="list-style-type: none"> <li>1. Connect by TCP/IP terminal and remote server using protocol HTTP;</li> <li>2. Download the file of specified size.</li> <li>3. Define time that was needed for full file download.</li> <li>4. Define rate of data transmission.</li> <li>5. Repeat the procedure more times.</li> </ol>
Expected results	Mean value of data transmission rate

**Test device**

IoT device with modules GPRS, EDGE, 3G/4G (LTE).

**Testing procedure**

The mean rate of data transmission is calculated by:

$$\text{Kbit/s} = \frac{\sum_{i=1}^n V}{n}, \text{ where}$$

V – rate of data transmission using protocol HTTP from remote server to terminal,

n – number of tests.

$$V = \frac{P}{t_{\text{initial}} - t_{\text{final}}}, \text{ where}$$

P – test file size,

$t_{\text{initial}}$  – time of the start of transmission;

$t_{\text{final}}$  – time of the end of transmission.

**Report**

The testing results should be reported in the table.

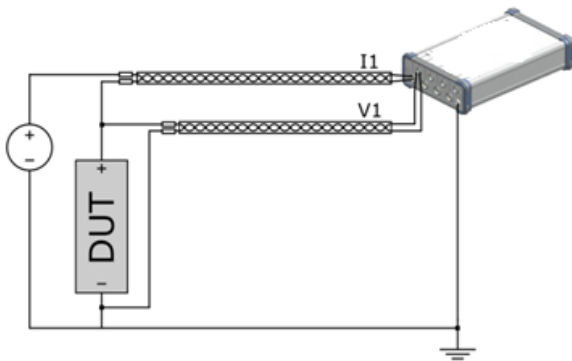
**Table A.8**

№	Test file size	Time of start	Time of end	Rate
1				
2				
...				
n				
<b>Mean rate _____ kbit/s</b>				

**Battery life testing**

**Table A.9**

<b>Test number</b>	<b>№09</b>
<b>Test name</b>	<b>Battery life</b>

Testing Layer	Physical
Type of tests	Functionality
Status	Mandatory
Tests goal	IoT Power Consumption Measurement
Configuration	
Testing procedure	<ol style="list-style-type: none"> <li>1. Connect LoRa and gateway device;</li> <li>2. Connect power nodes from DUT to multichannel probe with oscilloscope;</li> <li>3. Define the power consumption.</li> </ol> <p>Use oscilloscope with 3 enabled traces and multichannel probe: the 1st plot for both the supply voltage plot and the current drain over time. In this plot, the current drain during packet transmission can be seen. The 2nd plot shows the total power consumption over time. Using the area (integral) measurement function on the math channel with gating enabled allows to measure the energy consumed during one transmit frame. Measure sleep mode energy consumption using Markers. (Table A.9a).</p> <p>Battery life for NB-IoT, Bluetooth, LTE, 3GPP communication technologies can be measured automatically using communication tester and software package (Table A.9b).</p>
Expected results	<b>Battery life in hours</b>

**Test device**

IoT LoRa device.

**Report**

The testing results should be reported in the tables.

Table A.9a

Nº	transmit frame length, ns	supply voltage, V	current drain, mA	Sleep mode current drain, mA	consumed energy, W*s
1					
2					
...					
n					
<b>Current battery life ____ h</b> <b>Capacity of battery ____ mAh</b>					

Table A.9b

№	Capacity of battery	Voltage avg	Current avg	Power avg	battery life
1					
2					
...					
n					
Current battery life ___h					

*Receiver testing*

Table A.10

Test number	№10
Test name	<b>Receiver test</b>
Testing Layer	Physical
Type of tests	Functionality
Status	Mandatory
Tests goal	Rx sensitivity measurement
Configuration	<pre> graph LR     Gen1[Gen1 (analog)] -- RF --&gt; Combiner[Combiner]     Gen2[Gen2 (vector)] -- RF --&gt; Combiner     Combiner -- RF --&gt; LoRaDUT[LoRa DUT]     LoRaDUT --&gt; PER[PER meter software]             </pre>
Testing procedure	<ol style="list-style-type: none"> <li>1. Connect vector and analog generator to power combiner</li> <li>2. Connect LoRa testset device to power combiner;</li> <li>3. Run PER testset measurement software</li> </ol> <p>The test setup consists of two signal generators, the signals from which are fed to the DUT as a sum signal via a power combiner. Generator #1 generates an unmodulated, sinewave interference signal which is transmitted either with a spacing of 200 kHz relative to the wanted signal (adjacent channel blocking) or at the same frequency as the wanted signal (on-channel blocking). Generator #2 supplies the LoRa wanted signal, which is generated via LoRa ARB waveform files. The Packet Error Rate value is measured using the LoRa test tool.</p> <p>For the Rx sensitivity test, load a set of LoRa ARB waveform files in the Vector Signal Generator for testing the sensitivity of the receiver. The set of files contains waveforms with various signal bandwidths and spreading factors. A RF carrier signal is modulated using these baseband ARB files, which are loaded in the vector signal generator, and fed to the receiver in the appropriate frequency range.</p>



	While the signal power is being reduced, the LoRa test tool is used to read out and monitor the packet error rate (PER). The receiver sensitivity up to which no bit errors or very few bit errors occur depends on the used spreading factor and ranges from approx -117 dBm to -137 dBm. For testing standalone modules without test tool provided by manufacturer see software Wireshark method.
Expected results	Rx sensitivity level, blocking level

**Test device**

IoT LoRa testset.

The testing results should be reported in the tables.

**Table A.10a**

**Receiver Test**

<b>№</b>	<b>Frequency, MHz</b>	<b>Level. dBm</b>	<b>Modulation, SF type</b>	<b>PER, %</b>
1				
2				
...				
n				
<b>Current PER, %</b>				

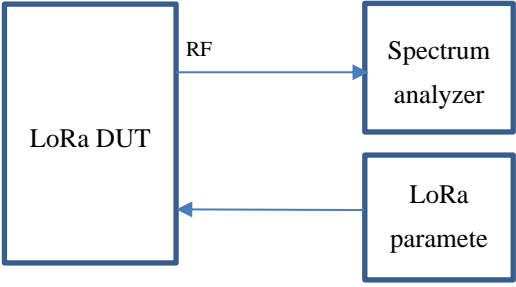
**Table A.10b Blocking Test**

<b>№</b>	<b>Frequency gen1, MHz</b>	<b>Level gen1. dBm</b>	<b>Modulation gen1, SF type</b>	<b>Frequency gen2, MHz</b>	<b>Level gen2, dBm</b>	<b>PER, %</b>
1						
2						
...						
n						
<b>Current PER, %</b>						

**6dB bandwidth testing**

**Table A. 11**

<b>Test number</b>	<b>№11</b>
Test name	<b>6 dB Bandwidth</b>
Testing Layer	Physical
Type of tests	Functionality

Status	Mandatory
Tests goal	Transmitter test
Configuration	
Testing procedure	<ol style="list-style-type: none"> <li>1. Connect LoRa testset device to spectrum analyzer</li> <li>2. Run LoRa parameter set software</li> </ol> <p>Using the spectrum analyzer with Central Frequency=current DUT frequency (902 MHz to 928 MHz), span=1.5 MHz, RBW=100 kHz, VBW=300 kHz, choose trace function with Positive Peak detector and Max Hold. Set reference level such that the maximum value of the signal is below the reference level. Use marker function for calculating "n dB down" for 6 dB Value. Following condition must be fulfilled: n dB down BW <math>\geq</math> 500 kHz.</p>
Expected results	6 dB Bandwidth

**Test device**

IoT LoRa testset.

**Report**

The testing results should be reported in the tables.

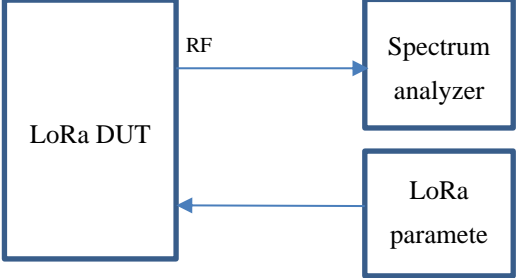
**Table A.11a 6 dB Bandwidth**

№	Frequency, MHz	Spreading Factor	Bandwidth, kHz	n dB down BW, kHz
1	915 MHz	SF7		
2				
...				
n				
<b>Span=___MHz, RBW=___kHz, VBW=___kHz (3 x RBW)</b> <b>6 dB Bandwidth= ___kHz</b>				

**Occupied bandwidth testing**

**Table A.12**

<b>Test number</b>	<b>№12</b>
Test name	<b>Occupied bandwidth</b>

Testing Layer	Physical
Type of tests	Functionality
Status	Mandatory
Tests goal	Transmitter test
Configuration	 <pre> graph LR     DUT[LoRa DUT] -- RF --&gt; SA[Spectrum analyzer]     Param[LoRa paramete] --&gt; DUT </pre>
Testing procedure	<ol style="list-style-type: none"> <li>1. Connect LoRa testset device to spectrum analyzer</li> <li>2. Run LoRa parameter set software</li> </ol> <p>According to FCC 15.247, the output power of a transmitter in the frequency range 902 MHz to 928 MHz must not exceed 1 W or 30 dBm. The total output power and the band power respectively are determined by integrating the power over the signal bandwidth. The signal bandwidth corresponds to the occupied bandwidth (OBW). The OBW is the bandwidth in which 99 % of the signal power is contained.</p> <p>Using the spectrum analyzer with Central Frequency=current DUT frequency (902 MHz to 928 MHz), span=2 MHz, RBW=30 kHz, VBW=100 kHz, sweep time=2ms, choose trace function with Positive Peak detector and Max Hold. Set Reference Level such that the maximum value of the signal is at least <math>10\log(\text{OBW}/\text{RBW})</math> below the reference level. Use measurement function and marker for calculating "Occ BW, kHz" Value.</p>
Expected results	occupied bandwidth

**Test device**

IoT LoRa testset.

**Report**

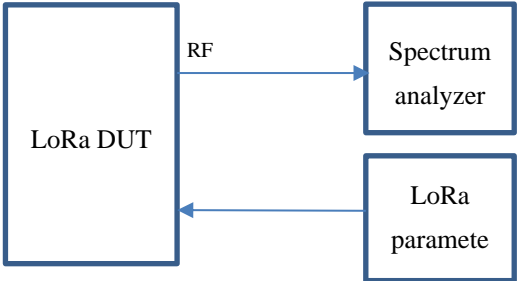
The testing results should be reported in the table.

**Table A.12a Occupied Bandwidth**

*Emission output power testing*

№	Frequency, MHz	Spreading Factor	Bandwidth, kHz	Span, MHz	OBW, kHz
1	915 MHz	SF7		2	
2					
...					
n					
<p><b>Span=___MHz (1.5 to 5 x OBW), Sweep=2ms,</b>  <b>RBW=___kHz (1% to 5% of the OBW), VBW=___kHz (3 x RBW)</b>  <b>Occ BW= ___kHz</b></p>					

Table A.13

Test number	№13
Test name	<b>Emission Output Power</b>
Testing Layer	Physical
Type of tests	Functionality
Status	Mandatory
Tests goal	Transmitter test
Configuration	 <pre> graph LR     DUT[LoRa DUT] -- RF --&gt; SA[Spectrum analyzer]     LP[LoRa parameter] --&gt; DUT             </pre>
Testing procedure	<ol style="list-style-type: none"> <li>1. Connect LoRa testset device to spectrum analyzer</li> <li>2. Run LoRa parameter set software</li> </ol> <p>Use Average mode on trace1 with RMS detector type. Choose average count at least 100. Set sweep Time to 50 ms. Set marker 1 for the transmit frequency of the DUT. Use the Band Power function with Span value = OBW value from previous measurements. Power spectral density. Perform single measurement on the spectrum analyzer; wait until the number of averaging operations have been performed. The result of the measurement is Band Power in dBm.                      The following conditions must be fulfilled: Band power <math>\leq 30</math> dBm</p>
Expected results	Emission Output Power

*Test device*

IoT LoRa testset.

**Report**

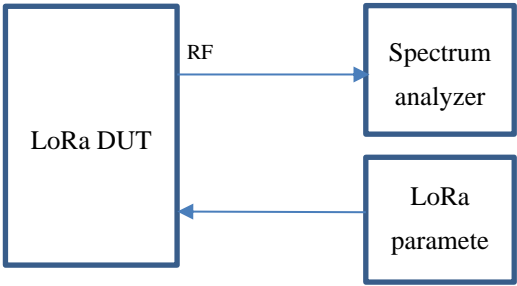
The testing results should be reported in the tables.

**Table A.13a Emission output power**

№	Frequency, MHz	Spreading Factor	Sweep Time, ms	OBW, kHz	Band power, dBm
1	915 MHz	SF12	50		
2	915 MHz	SF7	50		
...					
n					
<b>Average Count=100,</b>					

**Power spectral density testing**

**Table A.14**

Test number	№14
Test name	<b>Power spectral density</b>
Testing Layer	Physical
Type of tests	Functionality
Status	Mandatory
Tests goal	Transmitter test
Configuration	 <pre> graph LR     LDUT[LoRa DUT] -- RF --&gt; SA[Spectrum analyzer]     LPAR[LoRa paramete] --&gt; LDUT             </pre>
Testing procedure	<ol style="list-style-type: none"> <li>1. Connect LoRa testset device to spectrum analyzer</li> <li>2. Run LoRa parameter set software</li> </ol> <p>Using the spectrum analyzer with Central Frequency=current DUT frequency (902 MHz to 928 MHz), span=1.5xOBW value from Table A.13, RBW=3 kHz, VBW=10 kHz, sweep time=10 ms for SF7 or 500 ms for SF12, use Average mode on trace1 with RMS detector type. Choose average count at least 100. Set Auto Reference Level. Perform single measurement on the spectrum analyzer; wait until the number of averaging operations have been performed. Use Marker peak measurement function. The result of the measurement is Power marker M1</p>

	in dBm. The following conditions must be fulfilled: Power marker M1 $\leq$ 8 dBm.
Expected results	power spectral density

**Test device**

IoT LoRa testset.

**Report**

The testing results should be reported in the table.

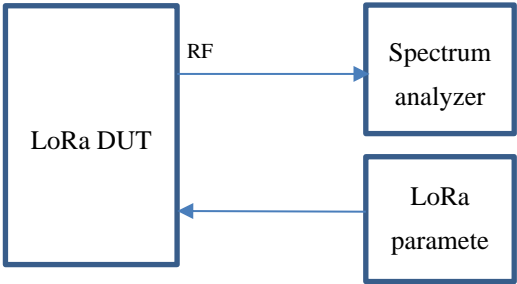
**Table A.14a Power Spectral Density**

<b>№</b>	<b>Frequency, MHz</b>	<b>Spreading Factor</b>	<b>OBW, kHz (from Table A.14)</b>	<b>PSD. dBm</b>
1	915 MHz	SF7		
2	915 MHz	SF12		
...				
n				

**Span=\_\_\_MHz (1.5 x OBW), Sweep=10ms for SF7, Sweep=500ms for SF12,  
RBW=\_3 kHz, VBW=\_10 kHz (3 x RBW)**

**Emission in non-restricted bands testing**

**Table A. 15**

<b>Test number</b>	<b>№15</b>
Test name	<b>Emissions in non-restricted bands</b>
Testing Layer	Physical
Type of tests	Functionality
Status	Mandatory
Tests goal	Transmitter test
Configuration	 <pre> graph LR     DUT[LoRa DUT] -- RF --&gt; SA[Spectrum analyzer]     Param[LoRa parameter] --&gt; DUT           </pre>
Testing procedure	<ol style="list-style-type: none"> <li>1. Connect LoRa testset device to spectrum analyzer</li> <li>2. Run LoRa parameter set software</li> </ol>

	<p>Measure maximum radiated power (REFlo) for lowest channel frequency for a 500 kHz wide LoRa signal (uplink), SF7 (903 MHz).</p> <p>Measure maximum radiated power (REFhi) for highest channel frequency for a 500 kHz wide LoRa signal (uplink), SF7 (914,2 MHz).</p> <p>Set the spectrum analyzer on central frequency Ftx=903 MHz, according to lowest channel center frequency for a 500 kHz wide LoRa signal (uplink), SF7. Choose span at least 1.5x(n dB down BW) from Table A.12 (1.5 MHz), RBW=100 kHz, VBW=(3xRBW)kHz, auto sweep. Use trace function with Positive Peak detector and Max Hold. Adjust the reference level accordingly to the maximum signal level with amplitude function. Use marker peak function for REFlo calculation.</p> <p>Use trace function with Positive Peak detector and Max Hold. Adjust the reference level accordingly to the maximum signal level with amplitude function. Use marker peak function for REFhi calculation. Use marker-to-peak search measurement function, define a range (upper and lower edges of the ISM band), turn on the Auto Max Peak function. The marker will indicate the highest level value M1 within the frequency range to be analyzed.</p> <p>The following condition must be fulfilled: <math>REFhi - M1 \geq 30</math> dB</p> <p>Using the marker-to-peak search function measure maximum radiated power at upper and lower edge of ISM band.</p> <p>The following condition must be fulfilled: <math>REFlo - M1 \geq 30</math> dB</p>
Expected results	Emissions in non-restricted bands

**Test device**

IoT LoRa testset.

**Report**

The testing results should be reported in the table.

**Table A.15a Emissions in non-restricted bands**

<b>№</b>	<b>Frequency, MHz</b>	<b>Spreading Factor</b>	<b>REFlo, dBm</b>	<b>REFhi, dBm</b>	<b>REFhi-M1, dB</b>	<b>REFlo-M1, dB</b>
1	903 MHz	SF7		-		
2	915 MHz	SF12	-			
...						
n						

**20dB bandwidth testing**

Table A.16

<b>Test number</b>	<b>№16</b>
Test name	<b>20 dB Bandwidth</b>
Testing Layer	Physical
Type of tests	Functionality
Status	Mandatory
Tests goal	Transmitter test
Configuration	<pre> graph LR     DUT[LoRa DUT] -- RF --&gt; SA[Spectrum analyzer]     Param[LoRa paramete] --&gt; DUT     </pre>
Testing procedure	<ol style="list-style-type: none"> <li>1. Connect LoRa testset device to spectrum analyzer</li> <li>2. Run LoRa parameter set software</li> </ol> <p>DUT settings=LoRa, 915 MHz, SF7, 125 kHz. Using the spectrum analyzer with Central Frequency=915 MHz. sweep=5ms, span= at least 2 to 3 times the 20 dB bandwidth, RBW= 1% of the 20 dB bandwidth, VBW= 3 x RBW, choose trace function with Positive Peak detector and Max Hold. Set auto reference level. Use marker function for calculating "n dB down" for 20 dB Value. If necessary, use the measured value for the 20 dB bandwidth (n dB down BW) to adjust the span and resolution bandwidth in line with the conditions named above. The following condition must be fulfilled: <math>n \text{ dB down BW} \leq 500 \text{ kHz}</math>.</p>
Expected results	20 dB Bandwidth

**Test device**

IoT LoRa testset.

**Report**

The testing results should be reported in the table.

Table A.16a 20 dB Bandwidth

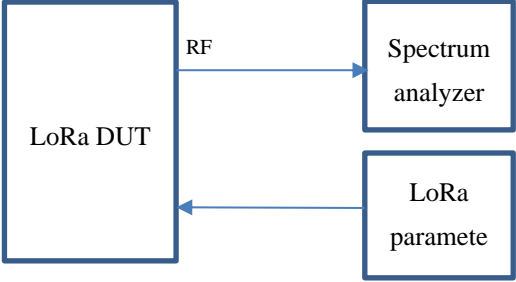
№	Frequency, MHz	Spreading Factor	Bandwidth, kHz	n dB down BW, kHz
1	915 MHz	SF7	125kHz	
2	915 MHz	SF7	250kHz	
...				
n				



Span=\_\_\_\_MHz, RBW=\_\_\_\_kHz, VBW=\_\_\_\_kHz (3 x RBW)  
 20 dB Bandwidth= \_\_kHz

*Power spectral density testing*

Table A. 17

Test number	№17
Test name	<b>Power spectral density (hybrid mode)</b>
Testing Layer	Physical
Type of tests	Functionality
Status	Mandatory
Tests goal	Transmitter test
Configuration	 <pre> graph LR     DUT[LoRa DUT] -- RF --&gt; SA[Spectrum analyzer]     Param[LoRa paramete] --&gt; DUT   </pre>
Testing procedure	<p>1. Connect LoRa testset device to spectrum analyzer          2. Run LoRa parameter set software</p> <p>Step 1          Using the spectrum analyzer with Central Frequency=current DUT frequency (902 MHz to 928 MHz), span=600 kHz or (1.5 to 5x)OBW, RBW=10 kHz or (1% to 5% of the OBW), VBW=30 kHz or (3xRBW), sweep time=10 ms for SF7 or 100 ms for SF12, use trace function with Positive Peak detector and Max Hold. Choose average count at least 100. Set Reference Level such that the maximum value of the signal is at least <math>10\log(OBW/RBW)</math> below the reference level. Use measurement function OBW (Power Measurements) for SF7 125 kHz and SF12 125 kHz.</p> <p>Step 2          Measurement of PSD. Set span=(1.5xOBW), RBW=3 kHz, VBW=10 kHz, sweep time=10ms for SF7 or 100ms for SF12, use Average mode on trace1 with RMS detector type. Choose average count at least 100. Set Auto Reference Level. Perform single measurement on the spectrum analyzer; wait until the number of averaging operations have been performed. Use Marker peak measurement function. The result of the measurement is Power marker M1 in dBm. The following conditions must be fulfilled for both SF7 and SF12: Power marker M1 <math>\leq</math> 8 dBm</p>
Expected results	Power spectral density (hybrid mode)

*Test device*

IoT LoRa testset.

**Report**

The testing results should be reported in the table.

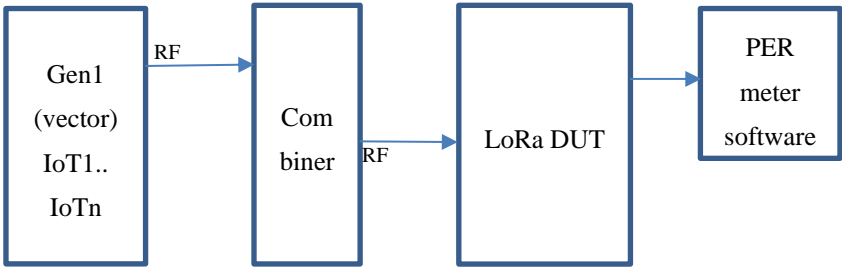
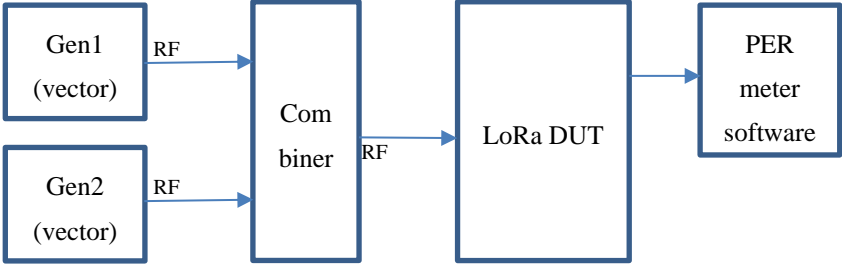
**Table A.17a Power Spectral Density (hybrid mode)**

<b>№</b>	<b>Frequency, MHz</b>	<b>Spreading Factor</b>	<b>Bandwidth, kHz</b>	<b>OBW, kHz</b>	<b>PSD. dBm</b>
1	915 MHz	SF7	125 kHz		-
2	915 MHz	SF12	125 kHz		
3					
n					
s					

**Interworking testing**

**Table A.18**

<b>Test number</b>	<b>№18</b>
Test name	<b>Interworking</b>
Testing Layer	physical
Type of tests	Functionality
Status	Optional
Tests goal	Coexistence test

Configuration	<p style="text-align: center;"><b>Setup</b></p>  <p style="text-align: center;"><b>Setup (alternative)</b></p> 
Testing procedure	<p>The test setup consists of one vector generator with two RF outputs or ability to generate several IoT signals on Baseband or two independent vector signal generators, the signals from which are fed to the DUT as. Generator(s) supplies the LoRa wanted signals, which is generated via several LoRa ARB waveform files. The Packet Error Rate value is measured using the LoRa test tool.</p>
Expected results	Coexistence immunity

**Test device**

IoT LoRa testset.

**Report**

The testing results should be reported in the table.

**Table A.18a Power Spectral Density (hybrid mode)**

№	Frequency, MHz	Spreading Factor	Bandwidth, kHz	IoT devices	PER
1	915 MHz	SF7	125 kHz		
2	915 MHz	SF12	125 kHz		
3					
n					
s					

*Packet collision simulation testing*

**Table A.19**

<b>Test number</b>	<b>№19</b>
<b>Test name</b>	<b>Packet collision simulation</b>
<b>Testing Layer</b>	Physical/data
<b>Type of tests</b>	Functionality
<b>Status</b>	Optional
<b>Tests goal</b>	Performance of a LoRa gateway
<b>Configuration</b>	<p style="text-align: center;">Setup</p> <pre> graph LR     Gen1[Gen1 (vector)] -- RF --&gt; Combiner[Com biner]     Combiner -- RF --&gt; LoRaDUT[LoRa DUT]     LoRaDUT --&gt; PER[PER meter software]     </pre>
<b>Testing procedure</b>	<p>The test setup consists of one vector generator, the signal from which are fed to the DUT. Generator supplies special LoRa signals with collision, which is generated via several LoRa ARB waveform files.</p> <p>ARB files can be converted from MATLAB.</p> <p>The Packet Error Rate value is measured using the LoRa test tool.</p>
<b>Expected results</b>	PER

**Test device**

IoT LoRa testset.

**Report**

The testing results should be reported in the table.

**Table A.19a Power Spectral Density (hybrid mode)**

<b>№</b>	<b>Frequency, MHz</b>	<b>Spreading Factor</b>	<b>Bandwidth, kHz</b>	<b>Collisions</b>	<b>PER</b>
1	915 MHz	SF7	125 kHz		
2	915 MHz	SF12	125 kHz		
3					
n					
s					

*Ethernet decoding testing*

**Table A.20**

<b>Test number</b>	<b>№20</b>
Test name	<b>Ethernet decoding</b>
Testing Layer	Physical/data
Type of tests	Functionality
Status	Optional
Tests goal	Performance of a LoRa link
Configuration	<p style="text-align: center;">Setup</p> <pre> graph LR     LG[LoRa gateway] -- LAN --&gt; O[Oscilloscope]     LP[LoRa paramete] --&gt; LG     </pre>
Testing procedure	The test setup consists of one oscilloscope with triggering and decode ability for Ethernet signals.
Expected results	<ul style="list-style-type: none"> <li>Start / end of frame</li> <li>Frame</li> <li>Error frame</li> <li>Preamble / SFD / FrameCheck</li> <li>Destination address</li> <li>Source address</li> <li>Address</li> <li>Data</li> </ul>

**Test device**

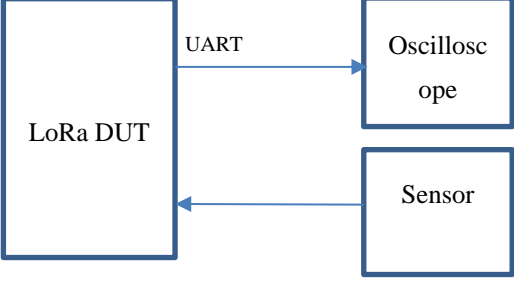
IoT LoRa gateway.

**Report**

The testing results should be reported in the table.

*Sensors data decoding testing*

Table A.21

Test number	№21
Test name	<b>Sensors data decoding</b>
Testing Layer	Physical/data
Type of tests	Functionality
Status	Optional
Tests goal	Performance of a sensor
Configuration	<p style="text-align: center;">Setup</p>  <pre> graph LR     LDUT[LoRa DUT] -- UART --&gt; OSC[Oscilloscope]     S[Sensor] --&gt; LDUT             </pre>
Testing procedure	The test setup consists of one oscilloscope with triggering and decode ability for protocol busses like UART.
Expected results	Start and stop bits Start error, stop error, parity error Parity bit Word Word contains error

**Test device**

IoT LoRa DUT.

**Report**

The testing results should be reported in the table.

*Network type classification testing*

**Table A.22**

<b>Test number</b>	<b>№22</b>
Test name	Response time test for network type classification
Testing Layer	Network
Type of tests	Functionality
Status	Optional
Tests goal	Determine the network type of the target network
Configuration	
Testing procedure	<ol style="list-style-type: none"> <li>1. Send testing packets to the IoT devices connected to the target network;</li> <li>2. Receive the responses from the devices, and measure their RTT;</li> <li>3. Repeat measuring RTTs by changing the timing to send testing packets;</li> <li>4. Select several minimum RTTs, and take their average;</li> <li>5. Classify the type of target network by the average RTT and pre-determined thresholds.</li> </ol>
Expected results	Response time and type of network

**Test network**

Network to which IoT device(s) belongs.

**Report**

The response time and estimated network type of the target network should be reported in the table.

# Appendix I

## Estimation method on network types from RTT samples

(This appendix does not form an integral part of this Recommendation.)

There is reference information of the document about the network type classification test.

In non-congested situations, the RTT of target network distributes in different range according to the network types. It means that the type of the target network can be classified if the borderlines between the RTT ranges of each network type are obtained. The detailed procedure of the classification is as follows.

1. Collect RTT values of candidate networks such as LAN (Ethernet), WLAN, 3GPP LTE and LPWAN (Wi-SUN) and so on, in non-congested situations by preliminary experiment or simulation.
2. Obtain the classification thresholds by applying a clustering algorithm such as k-means clustering to the RTT values collected by Step 1.
3. Compare the target RTT value (i.e., the average value of RTTs obtained by Step 4 in clause 7.5) and the borderlines, and detect the network type whose RTT range includes the target RTT.

Figure I.1 shows the samples of RTT values to validate above classification method. The candidate networks are LAN (Ethernet), WLAN, 3GPP LTE and LPWAN (Wi-SUN). RTT values were obtained by indoor experiment and simulations assuming that the target network is in an intra-network. As shown in this figure, each network has different range of RTTs, and the RTT thresholds are finely obtained by k-means clustering.

For the network classification test in an intra-network, the regions of the target RTTs  $t_{rt}$  to classify the target network as LAN, WLAN, LTE, Wi-SUN, and other extremely narrow band network, that can be obtained from Figure. I.1, is summarized in Table. I.1.

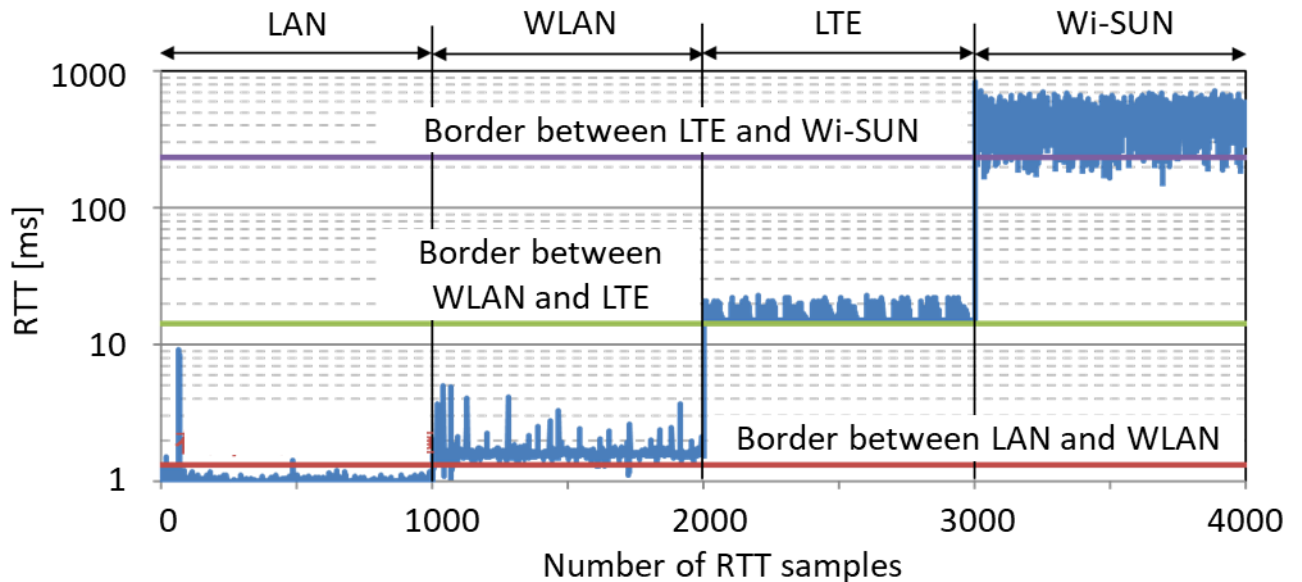


Figure I.1 – Examples of RTTs in LAN, WLAN, 3GPP LTE and Wi-SUN. and thresholds to classify the network types obtained by k-means algorithm in an intra-network.

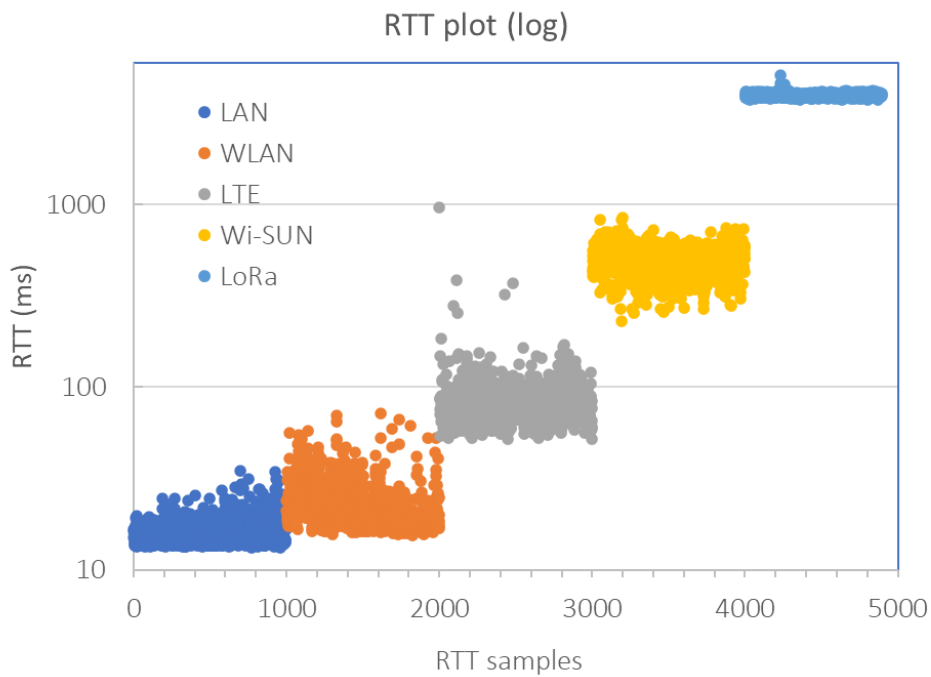


**Table I.1 – The regions of the target RTTs ( $t_{rtt}$ ) to classify the target network in an inter-network based on Figure. I.1.**

Range of target RTT ( $t_{rtt}$ )	Classification output
$t_{rtt} < 1.3 \text{ ms}$	LAN
$1.3 \text{ ms} \leq t_{rtt} < 14 \text{ ms}$	WLAN
$14 \text{ ms} \leq t_{rtt} < 220 \text{ ms}$	LTE
$220 \text{ ms} \leq t_{rtt} < 2000 \text{ ms}$	Wi-SUN
$2000 \text{ ms} \leq t_{rtt}$	Extremely narrow band network

Figure I.2 shows the samples of RTT values measured over the Internet to validate above classification method. The target networks to be tested were LAN, WLAN, 3GPP LTE, Wi-SUN, and LoRa. RTT values were experimentally obtained over the Internet with a testing server which geographically apart from the target networks. Figure I.3 shows the cumulative distribution function (CDF) of RTT samples for the target networks. As shown in these figures, the range of RTTs overlaps between LAN and WLAN. In other word, the RTT range of LAN is similar to that of WLAN, so it is difficult to distinguish between LAN and WLAN, and thus they should be classified as “LAN/WLAN.”

For the network classification test over the Internet, the regions of the target RTTs  $t_{rtt}$  to classify the target network as LAN/WLAN, LTE, Wi-SUN, and LoRa (or other extremely narrow band network), that can be obtained from Figures.

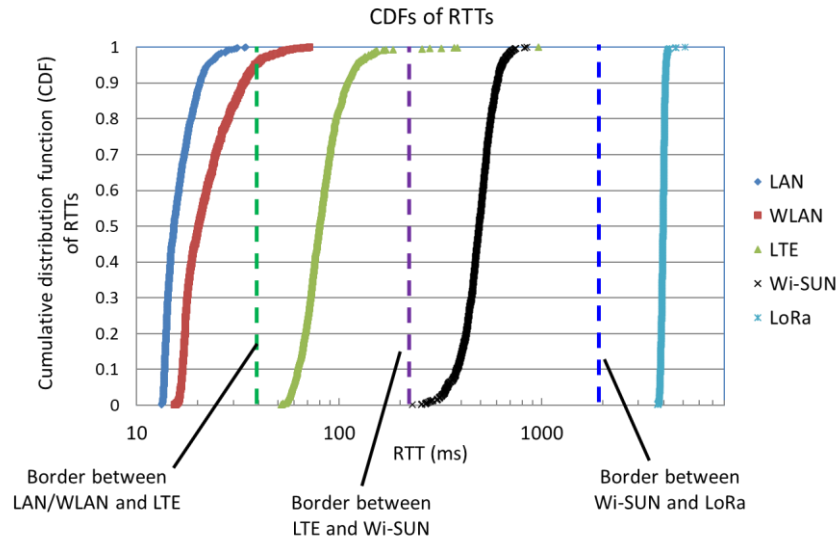


I.2 and I.3, are summarized in Table I.2.

RTT samples

**Figure I.2 – RTTs measured over the Internet for the target networks including LAN, WLAN, 3GPP LTE, Wi-**

## SUN and LoRa



**Figure I.3 – Examples of CDF of RTTs in LAN, WLAN, 3GPP LTE, Wi-SUN and LoRa obtained over the Internet, and thresholds to classify the network types beyond the Internet.**

**Table I.2 – The regions of the target RTTs ( $t_{rtt}$ ) to classify the target network beyond the Internet based on Figures. I.2 and I.3.**

Range of target RTT ( $t_{rtt}$ )	Classification output
$t_{rtt} < 40$ ms	LAN/WLAN
$40$ ms $\leq t_{rtt} < 220$ ms	LTE
$220$ ms $\leq t_{rtt} < 2000$ ms	Wi-SUN
$2000$ ms $\leq t_{rtt}$	LoRa (or extremely narrow band network)

## Appendix II

### Examples of IoT device detection and classification

(This appendix does not form an integral part of this Recommendation.)

For remote testing of IoT devices, it is necessary to device detection and classification. One of the possible device detection and classification approaches is presented in sub-clause 8.5.1.

A searching system with structure described in this section can be used for device detection and classification.

A searching system includes several subsystems:

- **A storage subsystem** – is designed to store data about detected devices in a database. The overall system is centralized, so all information is stored in one database.

- **A subsystem for processing user requests** – is a web application with which users can enter search requests and receive answers in the form of a list of devices that match the requests.

- **A subsystem for scanning devices connected to the network** – the subsystem collects information about devices, as well as transferring the information to the storage subsystem.

The subsystem for scanning devices connected to the network includes two modules:

- **A device search module** – is designed to search and determine the availability of devices in the network, scan device ports, determine the application layer protocols that are used by the device to transmit the data.

- **An indexing module** – is designed to analyze and transfer the information, which were received in the device search model, to the database.

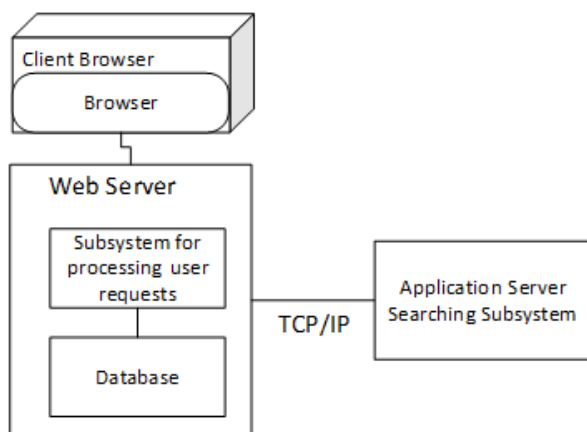
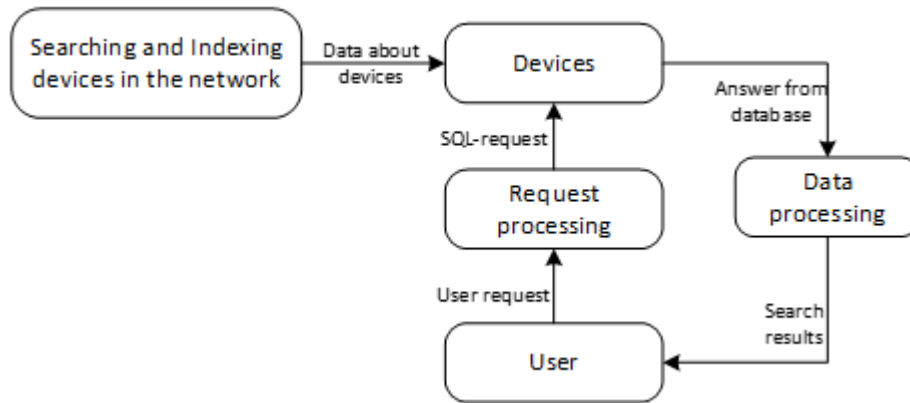


Figure II.1 – Searching system structure.

The data flow exchanged between the subsystems is shown in Figure II.2.



**Figure II.2 – UML diagram of data flow.**

The figure shows the data flow that occurs between the data storage subsystem and the user request processing subsystem. The structure of the transmitted data includes:

- Information about devices;
- User requests in the form of HTTP GET request parameters;
- Data responses in JSON format to user requests (using JSON format is an example of implementation);
- SQL queries to interact with the database.

In the database, there are following tables:

- IP table – for saving devices IP addresses;
- Open\_ports\_info table – for saving information about all open ports that are detected in the network;
- Protocol table – for saving the names of all protocols that the search program recognizes;
- Region\_info table – for saving information about the region in which the detected devices are locate;
- Type table – for saving the names of types of devices that were detected in the network.

The search subsystem has two modules for solving two related tasks:

- Search for devices in the network and collect information about each of them;
- Transforming, analyzing and forwarding the received information to the database.

The first module is composed of the following tasks:

- Determining devices availability by IPv4;
- Searching for open ports through which the device sends data;
- Defining the application layer protocol for each open port;
- Sending test requests and receiving responses for each application protocol.

Device availability is determined by sending ICMP Echo-Request packets to the target address and receiving ICMP Echo-Reply responses as how the ping utility works.

The search for open ports provides a search for existing communication channels. The task is to find as many of these communication channels as possible and identify those that are in a standby state. There are several ways to scan TCP ports:

- Scanning using the connect () function, which allows to connect to one of the ports on the remote device. If the port with which the connection is being attempted is open, then a connection to the server will be made; otherwise, the port is closed. This method provides a high searching speed if the methods of asynchronous or non-blocked input-output is

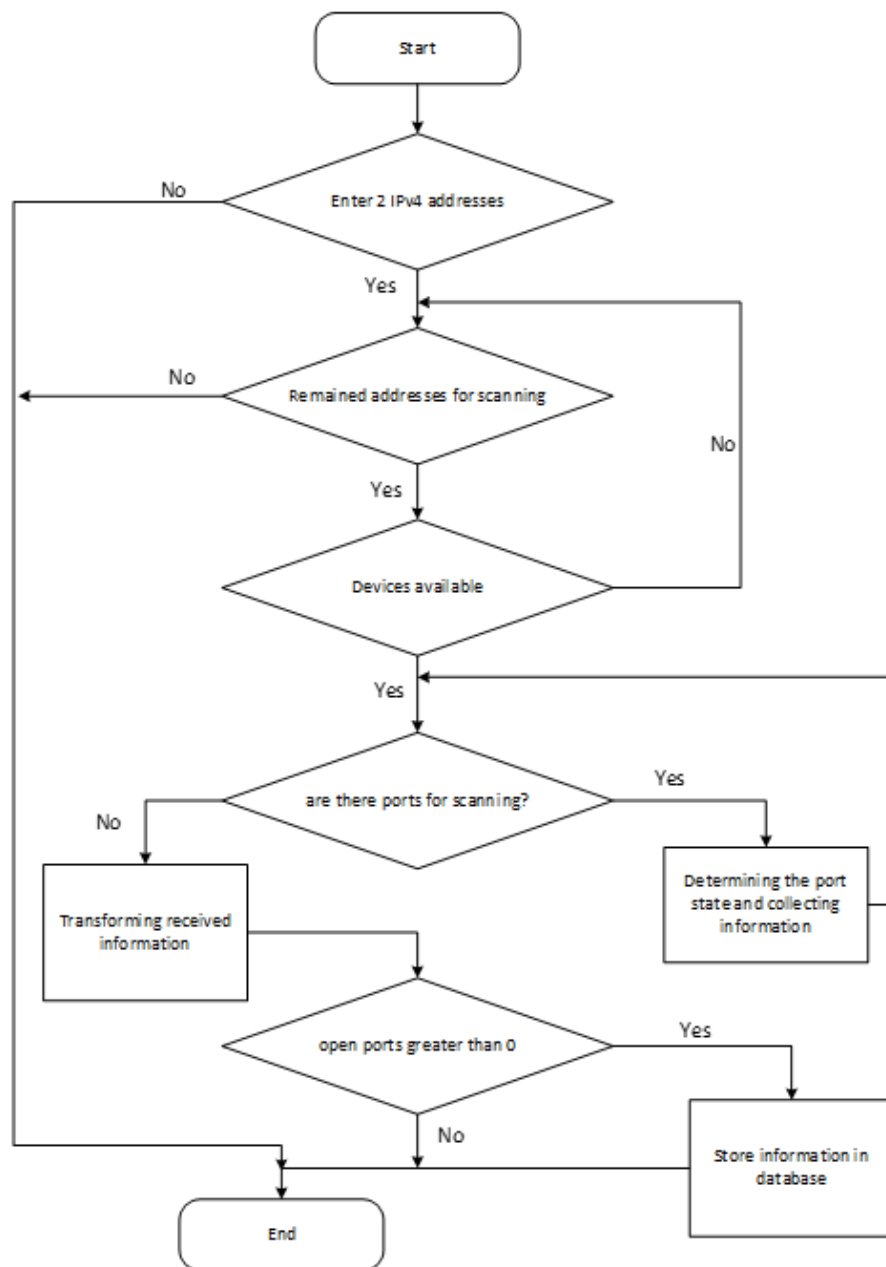
available. However, the disadvantage of this method is the high probability of detecting a scan followed by filtering.

- Scanning with the SYN flag - the scanner sends a packet that contains the SYN flag to the server for creating a connection and waits for a response. If a packet with the ACK flag is replied, it means that the port of the device is open. If a packet with the RST flag comes in the response, then this means that the port is closed, and the connection cannot be established. In the case of an ACK packet, the scanner immediately sends a packet with the RST flag in response to reset the connection. This scanning is hardly detected. However, this is available only for scanners on UNIX operating systems, and it is required to have root permission.

- Scanning with the FIN flag – this method is used to bypass security features and mask port scanning attempts. The scanner sends a packet with a FIN flag and awaits a response. If the answer does not come, then the port is open, since FIN packets are ignored by open ports. If a packet with the RST flag comes in response, then the port is closed. However, this method has its drawbacks. Not all operating systems support the scheme described above, therefore, there is scanning immunity with the flag FIN.

The second module of the search subsystem determines what type of devices belongs to and its location, and then to save the information to the database. The type of device is determined based on the protocols that it uses, as well as based on the responses that were received from open ports as mentioned above.

The Figure II.3 shows a block diagram of the operation of searching for devices connected to the network.



**Figure II.3 – A block diagram of the operation of searching.**

## Appendix III

### Detail test procedure for LoRa connectivity

(This appendix does not form an integral part of this Recommendation.)

Oscilloscope and special multichannel power probe can be driven via instrument and test set remote controller module. There should be included in a test plan for both signaling and power measurements which show the detailed value of the power consumption in different signaling states as well as an estimation of overall lifetime given a certain battery capacity.

#### III.1. LoRa devices test

Hardware and Tools to use:

1. Multichannel probe.
2. Instrument and test set remote controller module.
3. Battery Life Measurement for LoRa.
4. Real RF channel modeling module

Parameters for testing IoT devices:

- a) Multichannel probe with 2 or 4 simultaneous voltage and current measurement channels depending on IoT device under test.

Each channel should have 18-bit resolution analog to digital converters (ADC), 5 MSA/s sampling rate, channels are able to handle voltages up to  $\pm 15$  Volts and 10 Ampere when using the internal shunt. The accuracy can be increased by selecting the correct range for the ADC when working with lower voltages and currents.

- b) Depending on the IoT device under testing, it is possible that an instrument and test set remote controller module control several instruments that used during the testing phase. Communication tester with power measurement software in network emulation mode or oscilloscope with RF generator is usable. (Table A.9a).
- c) Battery Life Measurement for LoRa devices: in order to calculate the total service time or end of life using the same set of battery, the measurement of the power consumption per packet transmission is necessary. The devices are generally in sleep mode for most of the lifetime and only get active in operational mode in order to transmit data to the LoRa gateway. The power consumption in sleep mode needs to be measured in order to endorse the battery lifetime. (Table A.9b).
- d) IoT standards, for example LoRaWAN defines the media access protocol (MAC) and the system architecture for a wide area network (WAN). Using Real RF channel modeling module, it is possible to simulate different communication technologies such as RFID, ZigBee, 6LoWPAN, ETSI M2M, IEEE, 3GPP LTE and LTE-A, and TIA SDC.

#### III.2. LoRa receivers test

Hardware and Tools to use:

1. Vector signal generator with built-in ARB generator.
2. USB stick with a set of LoRa ARB waveform files for signal generator.
3. Software/hardware test tool provided by the manufacturer of the LoRa hardware module.
4. Analog signal generator
5. RF power combiner
6. Device under test (DUT)

Parameters for testing receivers:

- a) RF blocking measurement at a LoRa receiver.

The blocking test is used to check the behavior of the receiver when an interference signal is applied. The Packet Error Rate value is measured using the LoRa test tool.

- b) reception of the test RF LoRa signal

For the Rx sensitivity test, load a set of LoRa ARB waveform files in the Vector Signal Generator for testing the sensitivity of the receiver. While the signal power is being reduced from generator output, the LoRa test tool is used to monitor the packet error rate (PER). (Table A.10)

#### III.3 LoRa transmitter test

Hardware and Tools to use:

1. Spectrum analyzer
2. Software/hardware test tool provided by the manufacturer of the LoRa hardware module.
3. Device under test (DUT)

A test signal is generated using a test tool of the transmitter module manufacturer. The transmit signal generated is fed

and analyzed using the compact spectrum analyzer displaying the results at high resolution on the large touchscreen with gesture control.

Parameters for testing transmitters:

- a) 6 dB bandwidth  
In the frequency range 902 MHz to 928 MHz the 6 dB signal bandwidth of a digitally modulated signal must be at least 500 kHz for LoRa. (Table A.11)
- b) Occupied bandwidth  
According to FCC 15.247, the output power of a transmitter in the frequency range 902 MHz to 928 MHz must not exceed 1 W or 30 dBm. The total output power and the band power respectively are determined by integrating the power over the signal bandwidth. The signal bandwidth corresponds to the occupied bandwidth (OBW). The OBW is the bandwidth in which 99 % of the signal power is contained. (Table A.12)
- c) Emission output power  
The measurement performed using the band power measurement function of the spectrum analyzer. The following conditions must be fulfilled: Band power  $\leq$  30 dBm (Table A.13)
- d) Power spectral density  
According to FCC 15.247(e), the power spectral density of a transmitter in the frequency range 902 MHz to 928 MHz must at no time exceed the value of 8 dBm relative to a bandwidth of 3 kHz during an ongoing data transmission.  
The following conditions must be fulfilled:  
$$\text{Power marker M1} \leq 8 \text{ dBm. (Table A.14)}$$
- e) Emissions in non-restricted bands  
According to FCC 15.247(d), the radiated power outside the ISM band (902 GHz to 928 GHz) must be at least 30 dB below the maximum RF emission within the ISM band. Below is an example demonstrating the analysis of the RF emissions of a LoRa signal with SF7 at the lower and upper band limit.  
The following condition must be fulfilled:  
$$\text{REFhi-M1} \geq 30 \text{ dB}$$
$$\text{REFlo-M1} \geq 30 \text{ dB (Table A.15)}$$
- f) 20 dB bandwidth  
According to FCC 15.247, in the frequency range 902 MHz to 928 MHz the 20 dB bandwidth of a frequency hopping spread spectrum (FHSS) transmit signal must not exceed the value of 500 kHz. For a LoRa signal in FHSS mode. This means that the 20 dB bandwidth of 500 kHz must not be exceeded for the signal bandwidths 125 kHz and 250 kHz.  
The following condition must be fulfilled:  
$$n \text{ dB down BW} \leq 500 \text{ kHz. (Table A.16).}$$
- g) Power Spectral Density (Hybrid Mode)  
DUT settings=LoRa, 915 MHz, a) SF7, 125 kHz, b) SF7, 250 kHz, c) SF12, 125 kHz, d) SF12, 250 kHz.  
The following conditions must be fulfilled for both SF7 and SF12:  
$$\text{Power marker M1} \leq 8 \text{ dBm (Table A.17).}$$

### III.4 Additional testing

- a) Interworking. (Table A.18)  
Simulation several IoT coexistence on signal generator.
- b) Packet collision simulation (Table A.19)  
PER of a LoRa link in case of collision between LoRa packets modulated with different spreading factors.
- c) Ethernet decoding (Table A.20)  
Analyze Ethernet protocol variants by decoding the signal and searching within the decoded events. LoRa gateway testing.



d) Sensors protocol triggering and decoding (Table A.21)

Protocol decoding: The digitized signal data is displayed on the screen together with the decoded content of the messages in readable form, and the decode results are listed in a table.