



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.4062

(09/2020)

SERIES Q: SWITCHING AND SIGNALLING, AND
ASSOCIATED MEASUREMENTS AND TESTS

Testing specifications – Testing specifications for
IMT-2020 and IoT

Framework for IoT Testing

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2020

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Recommendation ITU-T Q.4062

Framework for IoT Testing

Summary

The IoT is one of the global infrastructures for the information society, delivering advanced services by interconnecting things based on, existing and evolving, interoperable information and communication technologies. Such a global infrastructure can be achieved by use of multiple access technologies for different types of communication networks such as BAN, PAN, LAN, WLAN, LPWAN, FAN, MAN, WAN and Cellular networks. Conformance and interoperability tests not only for domains with single access technology but also for the integrated domains with multiple access technologies are required. The main goal of this Recommendation is to specify the testing framework for IoT to accommodate the tests for such integrated domains with multiple access technologies. Conformance and interoperability tests for domains served by single unified access technology have been taken into account by relevant SDOs and therefore are out of scope of this Recommendation. This Recommendation describes the types of the tests for the domains with multiple access technologies and specifies the test procedures and the considerations correspond to the testing types.

Keywords

Test specification, IoT devices, test procedure, IoT technologies

Table of Contents

	Page
1 Scope.....	3
2 References.....	3
3 Definitions	3
3.1. Terms defined elsewhere:	3
3.2. Terms defined in this Recommendation	4
4 Abbreviations and acronyms	4
5 Conventions	6
6 Testing types.....	6
7 Test procedure	6
7.1 Conformance test.....	6
7.2 Connectivity test.....	6
7.3 Compatibility testing	9
7.4 Response time test for network type classification	11
8 Consideration for test procedure.....	13
8.1 Testing Network	13
8.2 Identification systems	14
8.3 Test timing.....	15
8.4 Grouping of target devices	15
8.5 Remote testing of IoT-devices.....	17
Annex A	22
Appendix I.....	44
Appendix II	47
Appendix III.....	51

Recommendation ITU-T Q.4062

Framework for IoT Testing

1 Scope

The Internet of Things (IoT) is achieved by use of multiple access technologies for different types of communication networks such as BAN, PAN, LAN, WLAN, LPWAN, FAN, MAN, WAN and Cellular networks. Therefore, conformance and interoperability tests not only for domains with single access technology but also for the integrated domains with multiple access technologies are required. The main goal of this Recommendation is to specify the testing framework for IoT to accommodate the tests for such integrated domains with multiple access technologies. Conformance and interoperability tests for domains served by single unified access technology have been taken into account by relevant SDOs thus are out of scope in this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[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 Definitions

3.1. Terms defined elsewhere:

3.1.1. Device [ITU-T Y.4000/Y.2060]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.2. Internet of Things (IoT) [ITU-T Y.4000/Y.2060]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

3.1.3 Conformance testing [ITU-T Y.4500.15/Q.3955]: Process for testing that an implementation is compliant with a protocol standard, which is realized by test systems simulating the protocol with test scripts executed against the implementation under test.

3.1.4. Denial of Service (DOS) [ITU-T X.800]: The prevention of authorized access to resources or the delaying of time-critical operations.

3.2. Terms defined in this Recommendation

None

4 Abbreviations and acronyms

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 Conventions

None.

6 Testing types

In order to test performance and to check characteristics of IoT devices, there are four types of testing. To check the characteristics of the IoT devices the technical feasibility of interacting with network units and the consistency in the operation of various types of networks, the network and all its components should be tested comprehensively. This procedure implies the following set of measures:

- **Conformance test** is a type of testing for certifying the technical characteristics declared by technical standards;
- **Connectivity test** is a type of testing to determine whether IoT hardware and network elements interact correctly within own architecture, and how this network interacts with the infrastructures of various networks;
- **Compatibility test** is a type of testing to verify the compatibility of IoT hardware and IoT software from different suppliers during its operation on the network.
- **Response time test for network type classification** is defined as a type of testing in which the type of the target network is estimated from the measured response time of the network. If the target network is not congested, in general, a packet injected into the target network will arrive at its destination IoT device with a certain level of transmission delay.

7 Test procedure

7.1 Conformance test

Conformance requirements for IoT devices and systems which consist of different IoT technologies should be determined from requirements for the relevant standards. Conformance tests for IoT framework are similar to tests regarding to the relevant test specification standards. Due to the fact that the characteristics for different IoT devices differ, the methodology for conducting conformance testing also varies.

Conformance testing is not scope of this Recommendation.

7.2 Connectivity test

7.2.1 Connectivity test

IoT framework should have the interfaces which enable a device to communicate with other devices over the network. The interfaces are based on specific IoT communication technologies or protocols. IoT framework connectivity tests are based on testing procedures which are described in standards or developer manual's requirements for the interface.

For example, if interface for testing finished its work, the framework's user should check whether or not testing finished successfully by comparing every decelerated operation by framework developers (in special standard or manual) with the result of this operation obtained by the test. Comparison can be both quantitative and qualitative.

IoT framework should have unified and multi-platform support with configuration manager and can include several modules with expansion abilities, such as the IoT test tool, communication technology definition module, real-time statistics logger, real RF channel modeling module, capture module, graphical user interface, instrument and test set remote controller module, input data modeler, security checker, and demo configurator wizard.

Communication technology definition module describes RF signals used in testing and use a set of waveforms and can control external instruments to form real signals usable across all test platforms interacting with IoT devices.

IoT test tool module based on web server that works in application and network layers forms compatibility test between different types and versions of hardware and firmware, module vendors, software, networks. IoT test tool module can also act as web-based system for testing interoperability between different IoT vendors, testing of application on different OS and devices (desktop/mobile).

Capture module can measure the performance of IoT devices at the protocol layer and test end-to-end application with encoded data from sensors via network layer, measure packet error trends.

Instrument and test set remote controller module can communicate with wide variety set of external instruments for additional testing. RF physical layer forming, triggering and measurement, data collecting, power consumption measurement.

IoT devices have tight requirements for power consumption in order to maintain expected battery life times for multiple years without a connection to a power supply. In order to verify the power consumption and expected battery life time, voltage and current have to be measured accurately for different operating states of the device under test.

The detail testing procedure can be shown in Annex A of this Recommendation.

7.2.2 Stress test

Stress test of IoT-devices aims to check the interworking between IoT devices and network infrastructure. The verification of the routers' stable performance to the IoT traffic is one of the most important objectives of IoT stress test. The characteristics of traffic and parameters of IoT are different from existing traffic models.

To check the performance of the application and the system is also important. The results of testing can help planning development and implementation of IoT systems.

The network capacity, latency, traffic value, packets loss, number of devices (that may be enormous) and so on should be considered during stress test. Furthermore, the device and environment parameters like energy consumption and temperature should also be considered. The testing model of IoT devices stress testing is shown on the Figure 7.2-1.

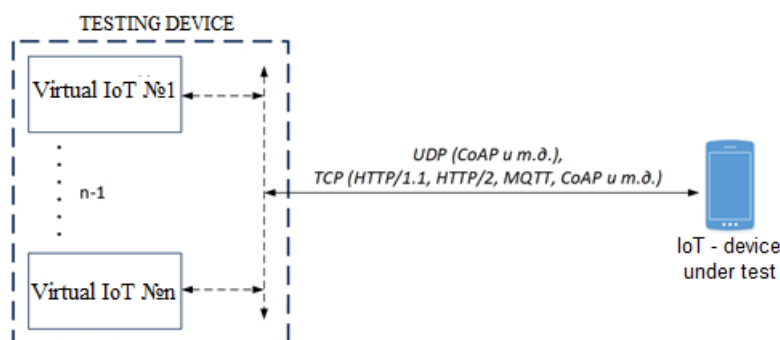


Figure 7.2-1 – The IoT - devices stress testing model

Virtual IoT in testing devices is a simulated function of real IoT devices when it is required to simulate a high load from many IoT devices. Virtual devices have all attributes of physical IoT devices and contain an identifier (for example, a MAC address) and a logical address (for example, IPv4)

For device stress testing, testing device needs to generate typical traffic of IoT devices that are characterised by:

- packet size. The data field is in most cases smaller than the packet header;
- number of packets due to the large number of Internet of Things connected to the network;
- other laws of time distribution. In addition to the properties of self-similarity, which was observed in communication networks of the next generation, Internet of Things can generate anti-persistent traffic.

For stress testing of the IoT devices, the following functions are to be considered:

1) Possibility of parallel traffic generation from virtual IoT to create a set of testing devices with unique parameters (unique MAC, IP, identification number, etc.);

2) Each virtual IoT running on a device needs to have one of the main types of IoT devices, for example:

- sensor (an electronic device that measures the physical state or chemical composition and delivers an electronic signal corresponding to the observed characteristic);
- actuator (a device that initiates a physical action after being excited by an input signal);
- multimedia device (a device that sends multimedia information, i.e., digital information in which many types of information content and information processing are used to inform or entertain users, for example, text, images, audio, video, three-dimensional panoramic images and digital maps);

3) Support for the main scenarios of IoT operation. Each IoT has a unique algorithm of work laid down in it by the developer, but there are major types of IoT scenarios as follows:

- constant data sending. Each device periodically sends data to a remote cloud server. In this case, the device can have two data types of – sensor and multimedia device. They generate self-similar traffic. For this scenario, the most commonly used transport layer protocols are connectionless (for example, UDP), less commonly used protocols that support the establishment of a connection (for example, TCP);
- sending data on request. In this case, the device can have two data types of sensor, and multimedia device. It can generate both self-similar traffic and antipersistent traffic, depending on the algorithm running on the remote control server. For this scenario, connection-oriented transport layer protocols (for example, TCP) are most often used, in some cases, for example, in cases where both the IoT and the cloud server have an address in the global network, it is possible to use connectionless protocols (for example, UDP);
- impact on the surrounding world from a device by a control signal. In this case, the device can be the actuator type. It can generate both self-similar traffic and antipersistent traffic, depending on the algorithm running on the remote control server. For this scenario, the most commonly used transport layer protocols are connection-oriented (for example, TCP), in some cases, it is possible to use connectionless protocols (for example, UDP).

- 4) The ability to generate various types of traffic from each IoT according to a certain distribution law.
- 5) Communication with a remote test server, required for testing scenarios that require the use of connectivity transport protocols. This server is necessary to measure the latency level at high levels of equipment load with IoT traffic.

In addition to support the capabilities of the above stress testing model, the device needs to support various major types of physical data transfer interfaces such as Passive Optical Network (PON) interface, Ethernet interface, and WLAN interface.

7.3 Compatibility test

Compatibility test of an item measures how satisfactorily the item works in parallel with other independent elements in a common environment (co-existent) and, as necessary, interacts with other systems or system elements.

The consideration points of the compatibility testing of various IoT technologies are inter-protocol data conversion and identification of the protocol itself using certain (semantic) attributes to ensure the compatibility of devices and platforms of the IoT. Compatibility issues can be addressed by considering specific compatibility levels for devices, applications, systems, networks, and other elements of IoT systems.

Figure 7.3-1 to Figure 7.3-3 show architectures for compatibility testing of IoT devices, IoT gateways and IoT cloud, which are elements of IoT eco-system.

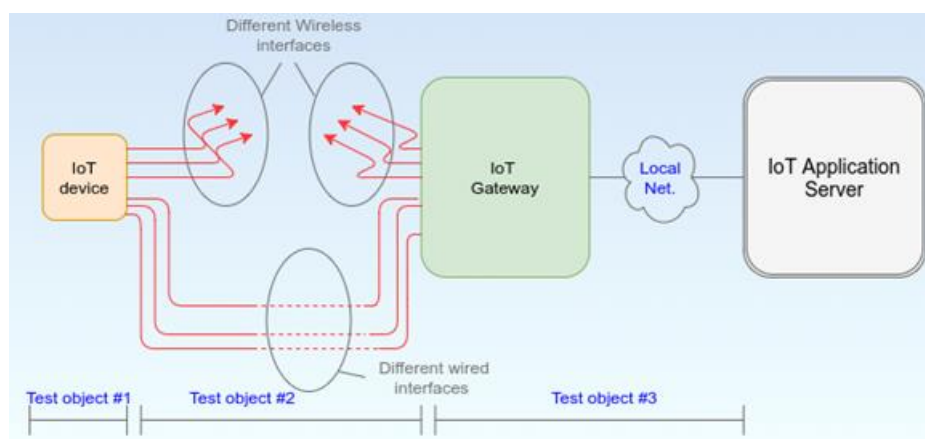


Figure. 7.3-1 – Compatibility IoT - device testing

In case of IoT device testing, the following test objects, as shown in Figure.7.3-1, are tested: IoT-device, different wired and wireless interfaces and the network part, which consist of IoT-gateway and local network to server. The IoT-device testing includes testing of IoT interfaces between sensors and actuators, processes of data sending via different network interfaces (Figure.7.3-1), and compatibility with IoT Application Server through the network.

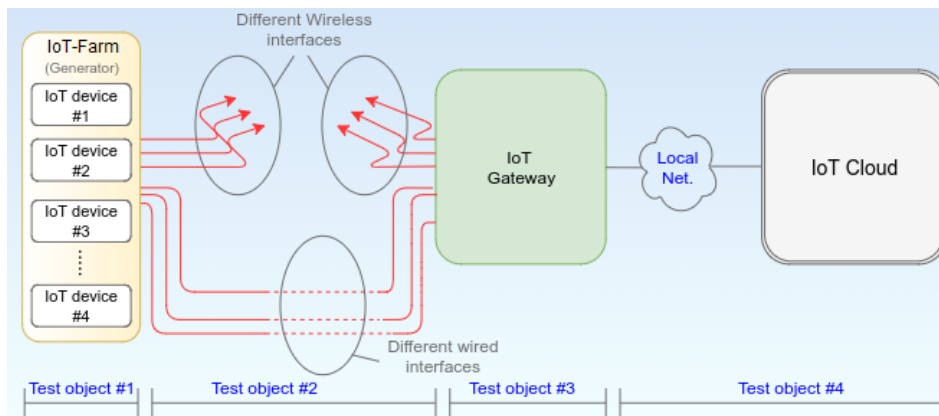


Figure. 7.3-2 – Compatibility IoT - gateway testing

In case of IoT gateway testing, the following test objects, as shown in Figure.7.3-2, are tested: IoT-farm, which consists of the number IoT-devices, wired and wireless channels between IoT-farm and IoT gateway, IoT-gateway, network with IoT application server like the “black box”. The IoT-gateway testing includes compatibility testing with IoT-device from IoT-farm via defined IoT-gateway’s interfaces (wired and wireless), high-load testing of IoT-gateway from IoT-farm, and also compatibility testing between IoT-gateway and IoT application server (via local network and server’s API).

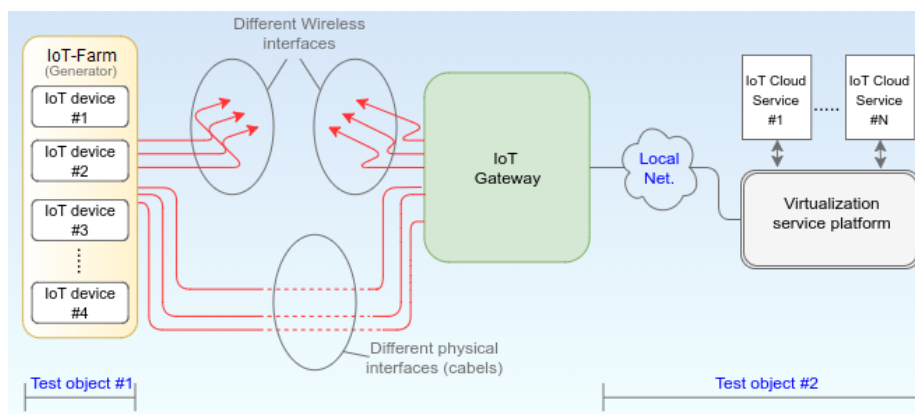


Figure. 7.3-3 – Compatibility IoT - Cloud service testing

In case of IoT cloud service testing, the following test objects, as shown in Figure.7.3-3, are tested: IoT-farm, local network with virtualization service platform, which have a different IoT application servers. The IoT cloud service testing includes the compatibility testing between IoT-device and different IoT application servers (API and defined functionalities), high-load testing the IoT application server with help of IoT-farm.

Compatibility levels

For the compatibility testing, the following compatibility levels should be considered:

- **Fully compatible:** In IoT systems, information resources or other IoT entities need to be capable of exchanging information and performing their required functions in a shared environment without any needs of modifying their input and/or output interfaces, protocols, software and hardware or converting devices (adapters, gateways, etc.).
- **Compatible:** In IoT systems, information resources or other IoT entities needs to be capable of exchanging information and performing their required functions in a shared environment by adapting their input and/or output interfaces, used protocols, software and hardware to each other or to the environment, or converting devices (adapters, gateways, etc.).

- **Partially compatible:** In IoT systems, information resources or other IoT entities need to be capable of exchanging information to some extent and performing a constrained set of their required functions in a shared environment, a help of additional tools unifying or converting their input and/or output interfaces, used protocols, procedures implemented by their software and hardware. The partial compatibility may be reached by negotiating the acceptable constraints on functionality among the parties.
- **Incompatible:** In IoT systems, information resources or other IoT entities are not capable of exchanging information and performing even a constrained set of their required functions in a shared environment due to the significant differences in technology and functional or non-functional requirements.

7.4 Response time test for network type classification

Response time test for network type classification measures the response time of the target network and estimates its network type. The response time highly depends on the transmission delay in the target network. The range of the transmission delay in non-congested situations highly depends on the network type of the target network, and the network type can be classified by comparing the transmission delay in a non-congested situation of the testing packet injected into the target network and the range of the transmission delay that is obtained in advance. Appendix I shows the detail method of the network type classification.

In this method, the round trip time (RTT) between the testing server and IoT device(s) in the target network is used as the measure of response time. The testing server sends testing packet(s) to IoT device(s) in the target network. The IoT device sends back response packet(s) to the testing server once it receives the testing packet(s). The testing server measures, collects the round trip times (RTTs) of the packets, and then classifies the RTT values to estimate the type of the target network.

An example of the testing network is shown in Figure. 7.4-1, and the procedure of the network type classification test is illustrated in Figure. 7.4-2. The procedure of this test method is as follows;

1. Send P testing packets (as shown by blue boxes in Figure. 7.4-1) to Q devices in the target network.
2. Receive the response(s) (as shown by green boxes in Figure. 7.4-1) from the device(s) in the target network, and measure their RTT as the elapsed time from sending testing packet(s) to receiving response packets.
3. Repeat 1. and 2. N times with changing the testing period to send the testing packets. Here, N denotes the number of rounds. In each round, the testing period to send the testing packets is chosen at a random (as shown in Figure. 7.4-3 (a)) or by a round-robin manner (as shown in Figure. 7.4-3 (b)) to find non-congested situation(s).
4. Select the minimum M RTT values, and take the average of the selected RTT values. Here, M is not greater than PQN .
5. Classify the type of target network from the averaged RTT value.

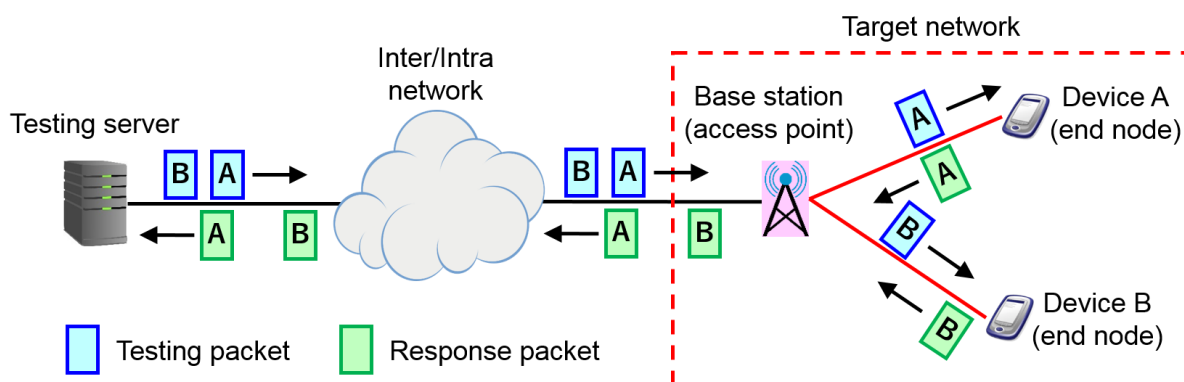


Figure 7.4-1 – An example of testing network.

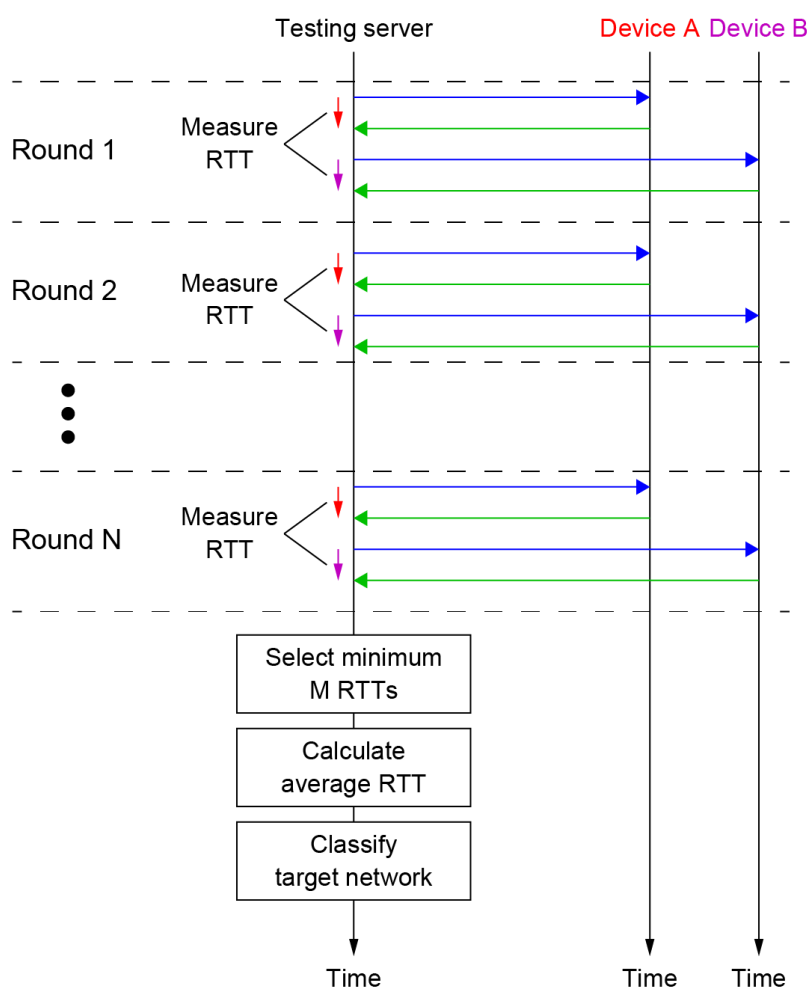


Figure 7.4-2 – Procedure of the network type classification test.

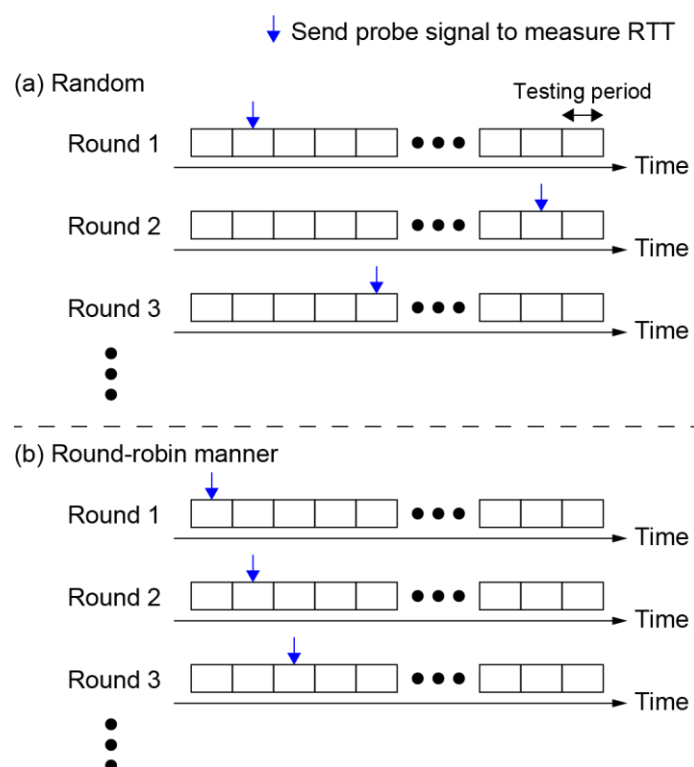


Figure 7.4-3 – An example of timing to send testing packet.

8 Consideration for test procedure

8.1 Testing Network

8.1.1 Existing network for testing

Testing of IoT devices and applications should be, in principle, conducted under the environment where they are used. With the existing network, any kinds of testing for IoT devices and applications can be performed and their results reflect the performance in the real situation where the IoT devices and applications are really used.

8.1.2 Model networks for testing

If it is impossible to perform the full range of tests on the existing network due to either a technical or economic issue, an alternative approach is necessary to conduct testing. The Recommendation ITU-T Q.3952: “Architecture and Facilities of Model Network for IoT Testing” presents a model network shown in Figure 8.1-1 on which various IoT integration scenarios are implemented. The Recommendation defines the architecture of model networks to be used for IoT testing and presents individual segments of model network. The model network reproduces the architecture of both the designed network and the existing network, as well as their various combinations. Application of additional structural units such as traffic generators, delays and interference allows studying the network in any conceptual scenario.

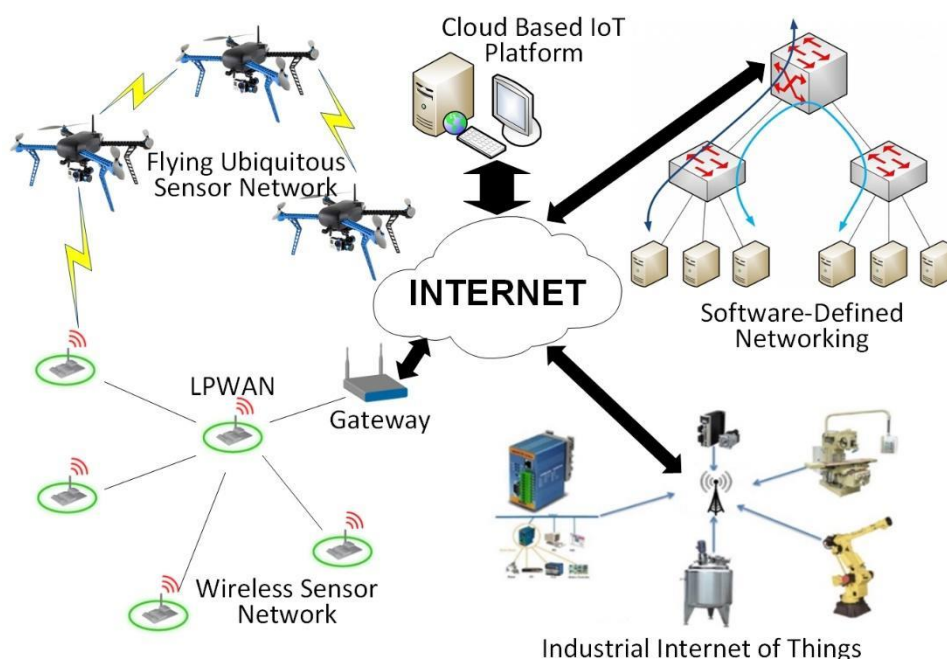


Figure 8.1-1 – Structure of model network for testing IoT devices and applications[ITU-T Q.3952]

There are two types of model networks; dedicated networks and distributed networks. A dedicated network is a part of a public communication network that is not connected with other model networks in any way. It is used for general testing and compatibility and interoperability testing. It is formed by at least two nodes interconnected by data link layers. One of the nodes is the equipment being tested; the second is the model network itself. A distributed model network can be thought of as several model networks connected via public telecommunications networks or other types of networks. It is used for compatibility and interaction testing, as well as for checking QoS parameters, requirements for interaction with other technical requirements, as well as requirements for compliance with network and information security measures.

Model networks can be implemented in both physical and virtual forms. Their virtualization allows moving away from the real “hardware” to a huge range of emulators. This modification allows reducing both material costs of network equipment and network deployment cost because number of the network's structural elements are represented by a single software platform.

Segmentation is another tool for improving the model network's structure. It refers to the division of the network into independent segments. Each of these segments triggers the operation of a public telecommunications network segment designed with the use of simulated technologies and reflects its properties. Scenarios for the operation of individual segments can be prescribed in advance, which provides flexible configuration of the system.

8.2 Identification systems

Identification system (IS) should be used for authentication in the early phase of IoT testing. Methods of testing IoT devices are different by the types of identification system. Every IS should meet the following requirements:

- IS should unambiguously identify IoT device (virtual or physical) by unique IoT identifier;
- IS should support special security system to communicate with IoT device (example: symmetric/asymmetric encryption etc.);
- IS should meet requirements of data transmission services for every data type.

The selected IS should also meet the developer or standard requirements.

8.3 Test timing

Quality of services for wireless networks, such as cellular networks, wireless LAN (or Radio LAN) and LPWAN, is completely different by types of the network, operation environment and time of day. The congestion level of wireless networks fluctuates within a day, and the pattern of congestion level depends on areas such as office and residential areas as shown in Figure. 8.3-1. In order to efficiently conduct test of all devices including IoT devices connected to wireless access networks, it is required to consider test timing for each network type. In the case of Figure 8.3-1, it is better to select test timing during mid-night or very early morning in office area, since congestion level is relatively low and it might be able to avoid severe network congestion due to increasing traffic volume by testing packets. In residential area, it might be better to select test timing around noon. Additional merit of this timing selection is that many terminals or devices can be tested at one time.

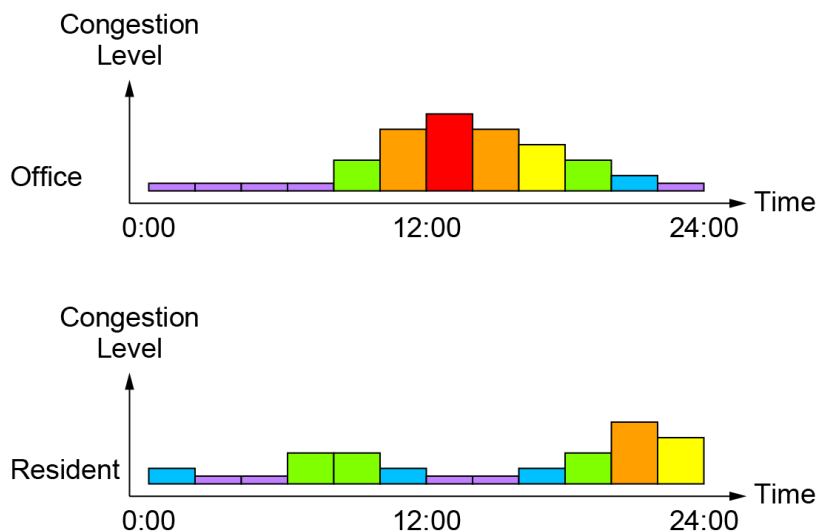


Figure 8.3-1 – Examples of fluctuation of congestion level.

8.4 Grouping of target devices

In general case of IoT testing, there are an extraordinarily large number of devices to be tested, so testing procedure may cause network congestion due to the injection of a large number of testing packets into the network. It is preferable to consider grouping target devices into multiple device groups and testing each group at different timing in order to reduce unnecessary amount of bandwidth for the test traffic, and to avoid over-capacity for each of access technology's bandwidth. It will resultantly contribute to shorten the total time for testing. There are several methods to form multiple device groups, for example, based on the identifier of devices or communication characteristics of target devices such as transmission speed (i.e. achievable data-rate) and delay performance as follows:

- Grouping based on device identifier

Each target device has its own device identifier. One of the simplest methods to form some (sub-)groups in the target network is to group based on device identifiers.

If the target network is an IP network, the target devices can be grouped by the following methods.

- Grouping based on IP address.

Generally, the target network consists of several network segments with different range of IP addresses, so it may be easy to group target devices by the network segments.

For example, if the network is an IPv4 network consisting of IP addresses

AAA.BBB.CCC.0 ~ AAA.BBB.CCC.255,

the target devices can be grouped like as

AAA.BBB.CCC.0 ~ AAA.BBB.CCC.127 and