International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Q

Supplement 71

(10/2019)

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

Testing methodologies of Internet related performance measurements including e2e bit rate within the fixed and mobile operators' networks

ITU-T Q-series Recommendations – Supplement 71

ITU-T

International Telecommunication Union

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050–Q.5069

For further details, please refer to the list of ITU-T Recommendations.

Supplement 71 to ITU-T Q-series Recommendations

Testing methodologies of Internet related performance measurements including e2e bit rate within the fixed and mobile operators' networks

Summary

Supplement 71 to ITU-T Q-series Recommendations describes the testing procedures of data transmission speed within the fixed and mobile operators' networks which can be established at the national or international level, providing customers of the existing public telecom networks the possibility to estimate the access related performance. The proposed methodology is based on the concept of the ITU-T Q.3960 (2016), "Framework of Internet related performance measurements".

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q Suppl. 71	2019-10-25	11	11.1002/1000/14125

Keywords

Internet, measurement of QoS, network performance, QoE, testing.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Supplement	1
4	Abbreviations and acronyms	1
5	Conventions	3
6	Test methodology	3
6.1	General overview	3
6.2	Functional architecture of the measurement system	3
6.3	Workflow	5
6.4	Measurement of Data	12
Appendix I – Collecting additional information from user's hardware and software		14
Appendix II – Measurement of network parameters over NAT		16
II.1	STUN test architecture	16
II.2	TURN test architecture	17
Bibliography		21

Supplement 71 to ITU-T Q-series Recommendations

Testing methodologies of Internet related performance measurements including e2e bit rate within the fixed and mobile operators' networks

1 Scope

This Supplement describes the testing procedures of data transmission speed within the fixed and mobile operators' networks.

The methodology is based on the concept of the ITU-T Q.3960 (2016), "Framework of Internet related performance measurements".

2 References

[ITU-T Q.3960] Recommendation ITU-T Q.3960 (2016), *Framework of Internet related performance measurements*.

[IETF RFC 7594] IETF RFC 7594 (2015), *A Framework for Large-Scale Measurement of Broadband Performance (LMAP)*.
<https://tools.ietf.org/html/rfc7594>

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 data transmission speed [b-ETSI EG 202 057-4]: The data transmission rate that is achieved separately for downloading and uploading specified test files between a remote web site and a user's computer.

3.1.2 network operator [b-ITU-T M.3208.1]: An organization that operates a telecommunications network. A network operator may be a *service provider* and vice versa. A network operator may or may not provide particular telecommunications services.

3.1.3 operator [b-ITU-T M.1400]: An organization responsible for identification and management of telecommunication resources. An operator must be legally recognized by the telecommunication administration of the country, or delegation thereof. An operator may or may not correspond to a trading partner.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AES Advanced Encryption Standard

APN Access Point Name

CGI Cell Global Identification

CI Cell Identity

DMP Destination Measurement Peer

DL Downlink

DTLS	Datagram Transport Layer Security
ECC	Embedded Communication Channel
FE	Functional Entities
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
EPS	Evolved Packet System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
ID	Identification
IP	Internet Protocol
ICMP	Internet Control Message Protocol
IR	Internet Resource
LAI	Location Area Identification
LTE	Long Term Evolution
MA	Measurement Agent
MCC	Mobile Country Code
MCS	Measurement Control Server
ME	Measurement Agent
MNC	Mobile Network Code
MP	Measurement Peer
MQTT	Message Queue Telemetry Transport
NAT	Network Address Translation
NMEA	National Marine Electronics Association
OS	Operating System
PCI	Physical Cell ID
PGW	Packet Data Network Gateway
PLMN	Public Land Mobile Network
RSA	Regenerator Section Adaptation?
RSSI	Received Signal Strength Indication
RTT	Round-Trip Time
SMA	Source Measurement Agent
SSL	Secure Sockets Layer
STUN	Session Traversal Utilities for NAT
SW	Software
TCP	Termination Connection Point
TE	Terminal Equipment

TLS Transport Layer Security

TURN Traversal Using Relays around NAT

UDP User Datagram Protocol

UID Unique Identifier

UIN Unique Identification Numbers

UMTS Universal Mobile Telecommunications System

UL Uplink

UUID Universally Unique Identifier

5 Conventions

None.

6 Test methodology

This clause defines the basic framework of the test methodology, which is the subject of this Supplement, including initial conditions, the phases of the test and testing algorithms. In addition, some guidelines in results processing are introduced.

6.1 General overview

The test methodology aims at delivering an accurate measurement of the maximum bandwidth available over a given internet connection. This is achieved by transferring multiple parallel data streams over separate TCP connections* within a predefined amount of time. The transferred data consist of randomly generated data with high entropy. It is not expected that the (pseudo) random number generator meets cryptographic requirements. However it should effectively avoid data compression during the transmission. In order to increase the probability that the test can be performed even within networks protected by firewalls and proxy servers, the data should be transferred over hypertext transfer protocol (HTTP) or hypertext transfer protocol secure (HTTPS) (i.e., transport layer security (TLS) or secure sockets layer (SSL) connection).

NOTE – The usage of UDP-connections for testing is for further study.

6.2 Functional architecture of the measurement system

6.2.0 Introduction

The measurement system should be composed of the functional entities (FEs) in Figure 1. Note that this functional architecture does not impose any particular implementation constraints and different FEs can be mapped to one or many software/hardware (SW/HW) nodes.

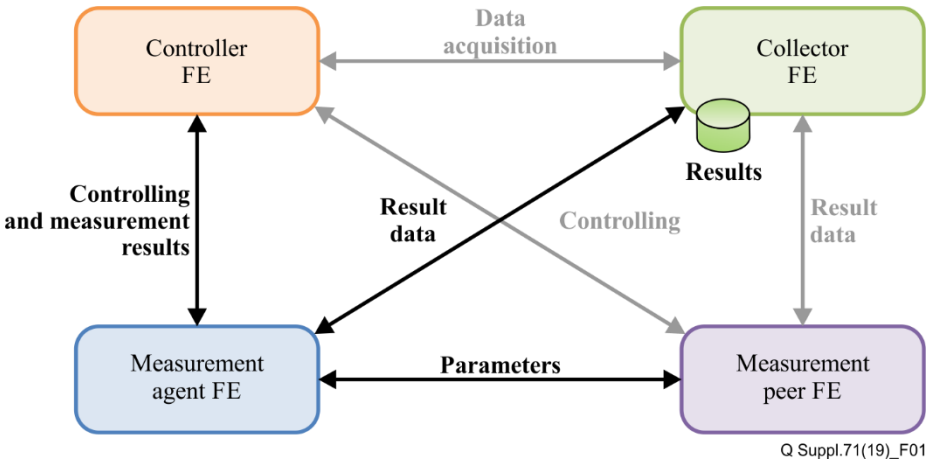

Figure 1 – The functional architecture of the basic measurement system

6.2.1 Controller FE

The Controller is a FE that is able to control the testing mechanisms on a particular measurement agent (MA). The Controller should allow the specification of test scripts defining the measurement workflow (i.e., different stages and testing procedures involved) to later trigger the execution of the relevant test scenarios on that particular MA. The specification process may demand the acquisition of existing data from the Collector.

Furthermore, the Controller provides the user with the measurement environment and tools to execute the test throughout a web page or an HTTP/s access. It should be capable of hosting and serving the required scripts and contents to be used during the test. Additionally, it will provide users with an interface to access measurement results.

6.2.2 Collector FE

The Collector is a FE that gathers, processes and stores measurement results and other statistical data from all MAs connected to the Controller, and from the measurement peers (MPs) in case they are specifically deployed for the specific test scenario. It should be capable of properly handling secured transmission of data.

6.2.3 Measurement Agent FE

The measurement agent is a FE that executes the test scripts defined in the Controller, obtains the test results and uploads the relevant data result to the Collector.

The measurement agent may well admit two different configurations.

Option a) involves a terminal equipment (TE) (including but not limited to computer, smartphone, tablet, etc.) physically controlled and generally owned by the user.

This TE should have an active Internet connection and a web-browser in order to access the website hosted at the Controller, or an app to access the test in case of a portable device.

The TE should also be capable of establishing secure communications to the Collector, for the safe transfer of results and other statistical data.

Option b) involves the same TE and the existence of a MA in the form of a middlebox (probe) or additional hardware integrated in the TE.

– The local measurement peer also requires any hardware and software that enables the remote management and configuration of the device without requiring any specific operation from the customer.

6.2.4 Measurement peer FE

The measurement peer is a FE that is able to respond to testing messages sent from MA and possibly collect measurement data to be uploaded to the Collector. Additionally, it may provide resource usage monitoring capabilities so that the Controller could schedule tests in order to prevent any foreseen interference that could have an impact on the tests results.

6.2.5 Common remarks

All the functional entities should ensure that no interference among concurrent activities affect the test result by proper dimensioning in terms of HW/SW and link capacity. Furthermore, the recipient of the result should be notified of the conditions required to ensure a reliable measurement and the possible measurement errors due to non-conformance with such conditions (including but not limited to cross traffic, background applications, operating system (OS) and applications configuration, etc.).

6.2.6 Security considerations

In the process of data collection, either from the TE and/or the MA (including but not limited to user identity, location, IP address, etc.) different security and confidentiality concerns may occur.. Specific measures to secure each data transfer, authenticate different FEs and anonymize specific collected data are described in [IETF RFC 7594]. In any case, adopted security and privacy threat mitigations shall be deployed according to respective national regulation.

6.3 Workflow

6.3.1 General requirements

The test methodology aims at delivering an accurate measurement of the maximum bandwidth available over a given Internet connection. It may be the case that the maximum data rate per socket connection is limited. Therefore multiple parallel data streams (multiple sockets), running within a given time window should be used.

In order to prevent data compression by the network under test, the transferred data consist of randomly generated data with high entropy. It is recommended to verify that no or only negligible data compression takes place by respective validation tests prior to the actual measurement.

6.3.2 Initial conditions

The test methodology defines a set of variables and constants that need to be assigned prior to the execution of the measurement algorithm or during the test execution. Some of these values are open to selection within a range, according to the specific considerations of each implementation or the current network conditions at the time the test is being executed.

Table 1 – Indicative measurement -parameters

	Parameter	Unit	Range	Default value
n	Number of parallel connections	#	$1 \leq n \leq 10$	n = 3
Tp	Duration of pre-test	s	$0 \leq Tp \leq 5$	Tp = 2 s
Td	Duration of the downlink subtest	s	$5 \leq Td \leq 15$	Td = 7 s
Tu	Duration of the uplink subtest	s	$5 \leq Tu \leq 15$	Td = 7 s
To	Timeout value	s	$5 \leq To \leq 10$	To = 5 s
p	Number of 'pings' during delay subtest	#	$5 \leq p \leq 20$	p = 10
Tl	Maximum elapsed time before the first ping starts	ms	$200 \leq Tl \leq 1\,000$	Tl = 500 ms
z	Reference size of data block (chunk size)	KB	Minimum 1 kbyte	z = 4 KBytes
NOTE – All the values in the table are indicative.				

6.3.3 Measurement procedure

6.3.3.0 Introduction

This clause defines the main phases of the testing procedure, once the measurement agent has obtained the test code from the Controller and the location or locations of the measurement peers.

The MP is determined directly in the Controller by geo-locating the MA and determining its closest access to the Internet. In case of executing the Internet resource (IR) speed test, the measurement peer can be either selected by default or allowing the user to choose a destination within a list of Internet resources.

The following set of graphics state the basic exchange of information between the MA and the selected MP for each of the cases (the same procedure is defined for both the network Internet speed test and the Internet resource speed test).

The test performed according to the methodology follows the procedure outlined below. The test consists of seven phases which are carried out one after each other, i.e., phase *m* starts after phase *m*-1 has finished without any pause in-between. That means that the phases do not overlap.

To ensure comparable data transmission speed test conditions in mobile networks, a pre-load should be initiated. With the pre-load, the mobile networks are set in a defined initial state, i.e., CELL_DCH in the universal mobile telecommunications system (UMTS) and connected in long term evolution (LTE).

If the downlink and uplink pre-tests procedures are not implemented (phases 2 and 5), the measurement agent shall open an uplink and downlink connection using a number of multiple sockets.

For the latency calculation (IMCP echo request/echo reply method) the echo receiver processing delay shall be taken into account.

The workflow of the measurement system is shown in Figure 2.

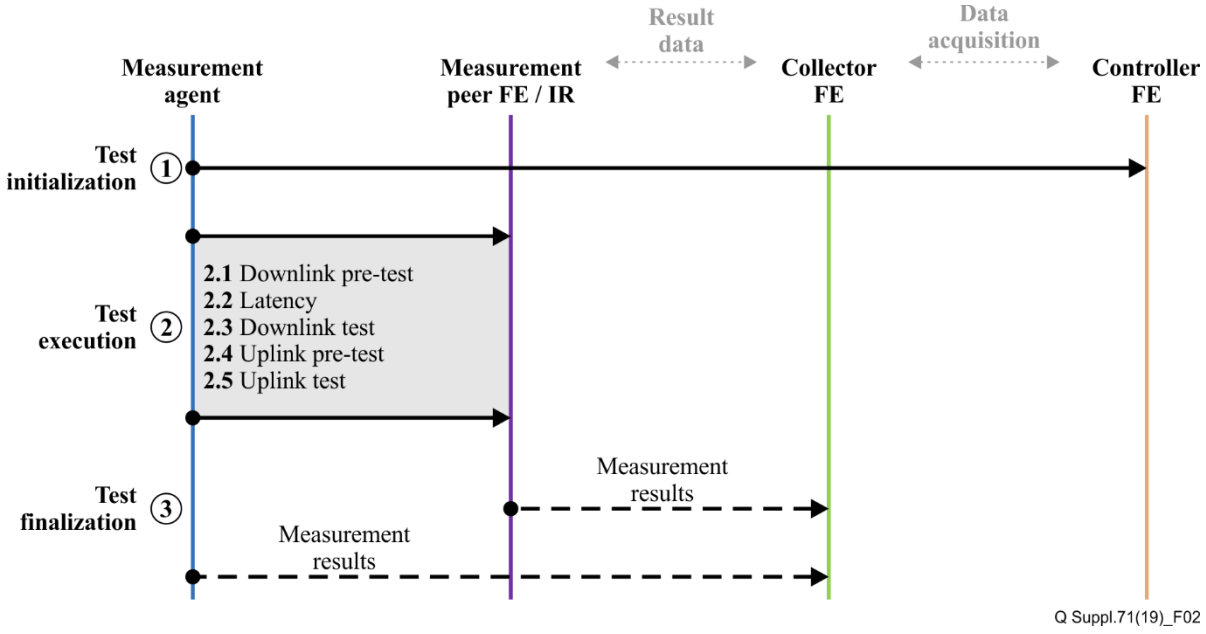

Figure 2 – The workflow of the measurement system

6.3.3.1 Phase 1: Initialization

The measurement agent tries to connect to the Controller, with either option HTTP and/or HTTPS using port 443 over TLS or SSL. In order to pass through certain firewalls, which might block unencrypted data transmissions, HTTPS might be necessary. The data streams themselves are optionally unencrypted. In order to prevent the computational cost of encryption from

deteriorating/depreciating the measurement results, the lowest encryption and authentication parameters should be chosen.

After establishing a proper connection, measurement agent and measurement peer exchange the information, which is required for running the test.

The Controller determines the measurement peer to be used. It then generates a token consisting of the following example components:

- a unique test identification (ID);
- the time at which the measurement is allowed to start;
- the period of time during which access to the measurement peer is allowed (a string representing number of seconds);
- the maximum number of permitted parallel connections from the measurement agent to the measurement peer (a string representing a positive integer).

The Controller then transmits the token as well as all the additional test parameters (e.g., Internet Protocol (IP) address of the measurement peer, public IP address of the measurement agent, number of used multiple socket connections, etc.) to the measurement agent. The token is used for identifying the test session.

6.3.3.2 Phase 2: Downlink pre-test

The downlink pre-test for fixed wired high speed internet connections is optional.

In phase 2, the measurement agent opens n connections to the assigned measurement peer. Within each connection, the measurement agent requests and the measurement peer sends a data block of size z. While the duration of the pre-test has not exceeded Tp, the measurement agent requests a data block of double size compared to the last iteration step. The transfer of the last data block will be finished even if the duration has already exceeded Tp. At the end of the pre-test, all connections are left open optionally for further use.

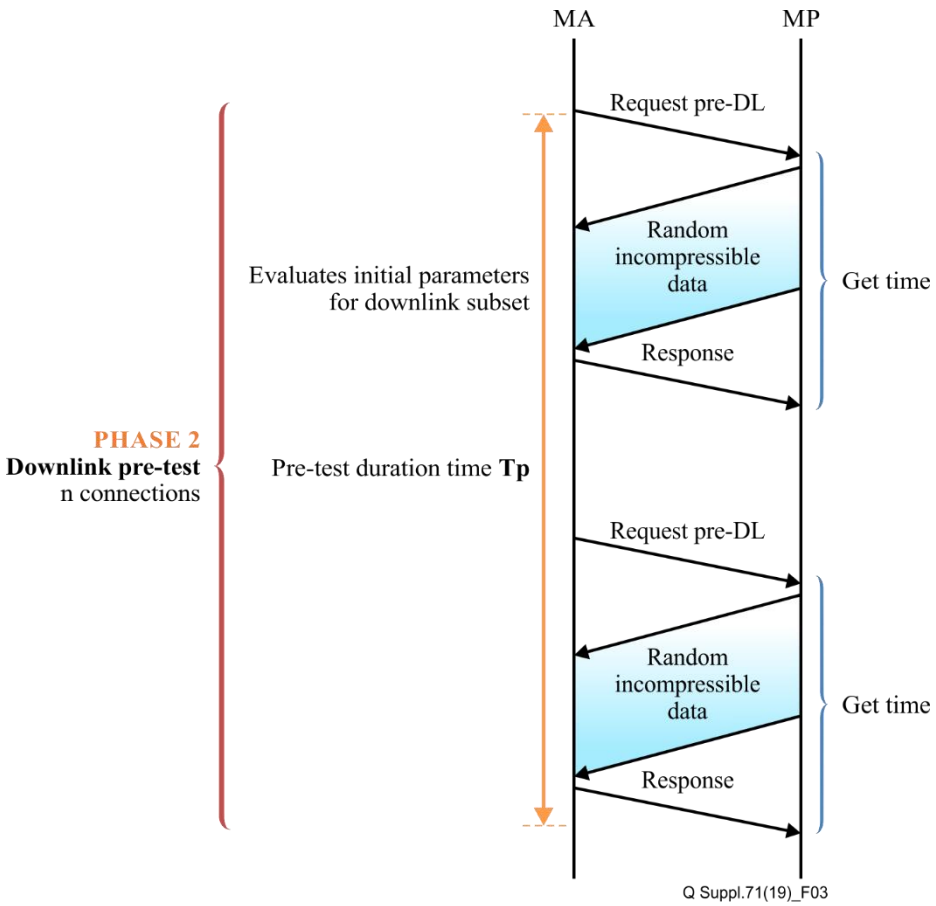

Figure 3 – Sample diagram of phase 2 of measurement algorithm

6.3.3.3 Phase 3: Latency test

During this phase, the measurement agent sends p "pings" in short intervals to the measurement peer to test the latency of the connection. One "ping" consists of the transmission of short strings via one of the connections to the measurement peer, which returns short strings as acknowledgement. The measurement agent measures the time between sending and receiving the return message, while the measurement peer additionally measures the time between sending its return message and the measurement agent's reception response. The measurement agent stores all measurements.

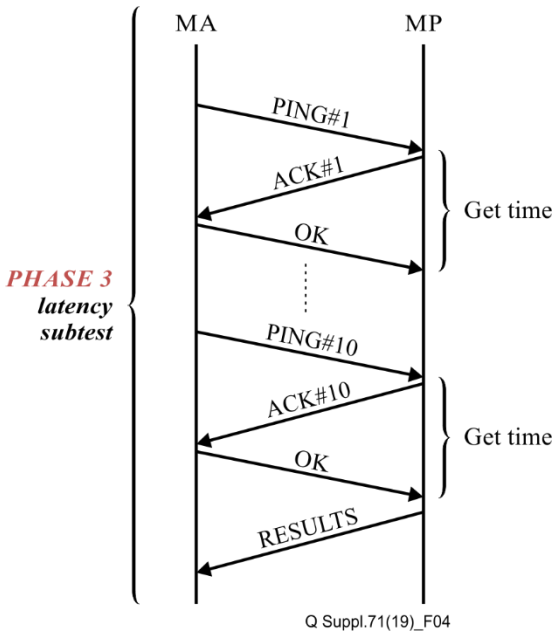

Figure 4 – Sample diagram of phase 3 of measurement algorithm

6.3.3.4 Phase 4: Downlink subtest

Within each of the n connections opened during phase 2, the measurement agent simultaneously requests and the measurement peer continuously sends data streams consisting of fixed-size chunks of size s (randomly pre-generated data with high entropy).

As an option, the Collector can continuously send data streams on n connections consisting of data files from the data-reference system. All transmissions start at the same time, which is denoted as relative time 0. For each connection the measurement agent records the elapsed time and the amount of data received.

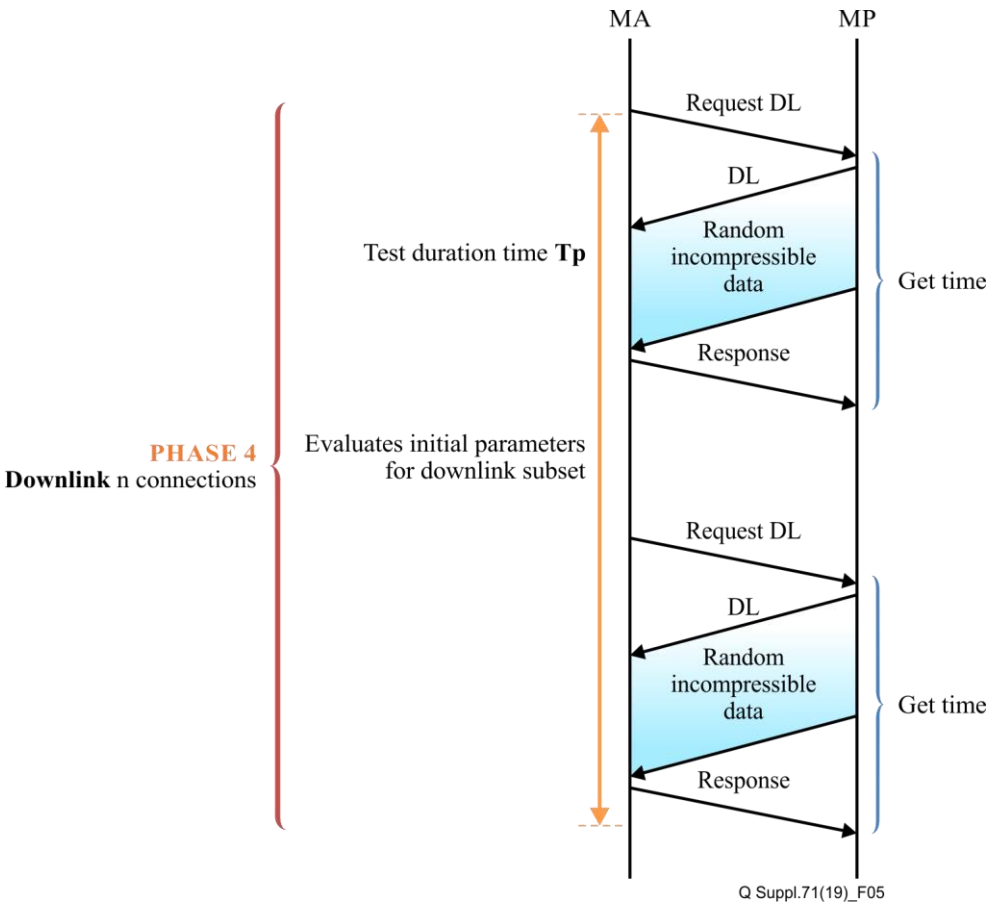

Figure 5 – Sample diagram of phase 4 of measurement algorithm

6.3.3.5 Phase 5: Uplink pre-test

The uplink pre-test for fixed wired high speed internet connections is optional.

In phase 5, the measurement agent opens n connections to the assigned measurement peer. Within each connection, the measurement agent sends a data block of size z (randomly pre-generated data with high entropy). While the duration of the pre-test has not exceeded Tp, the measurement agent sends a data block of double size compared to the last iteration step. The transfer of the last data block will be finished even if the duration has already exceeded Tp. At the end of the pre-test, the connections are left open for further use.

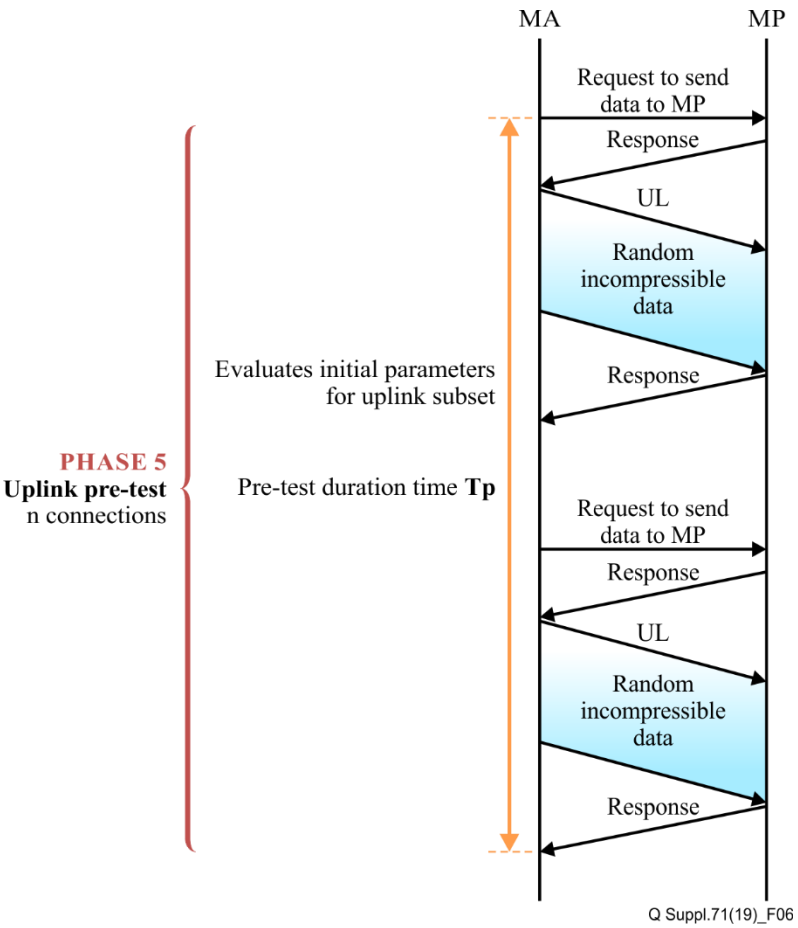

Figure 6 – Sample diagram of phase 5 of measurement algorithm

6.3.3.6 Phase 6: Uplink subtest

Within each of the n connections opened during phase 5, the measurement agent continuously sends data streams. Fixed-size chunks can be used as an option. As an option, the measurement agent can continuously send data streams on n connections consisting of a data file with randomly generated data with high entropy. All transmissions start at the same time, which is denoted as relative time 0. For each connection, the measurement peer gives feedback to the measurement agent by sending the elapsed time and the amount of data received.

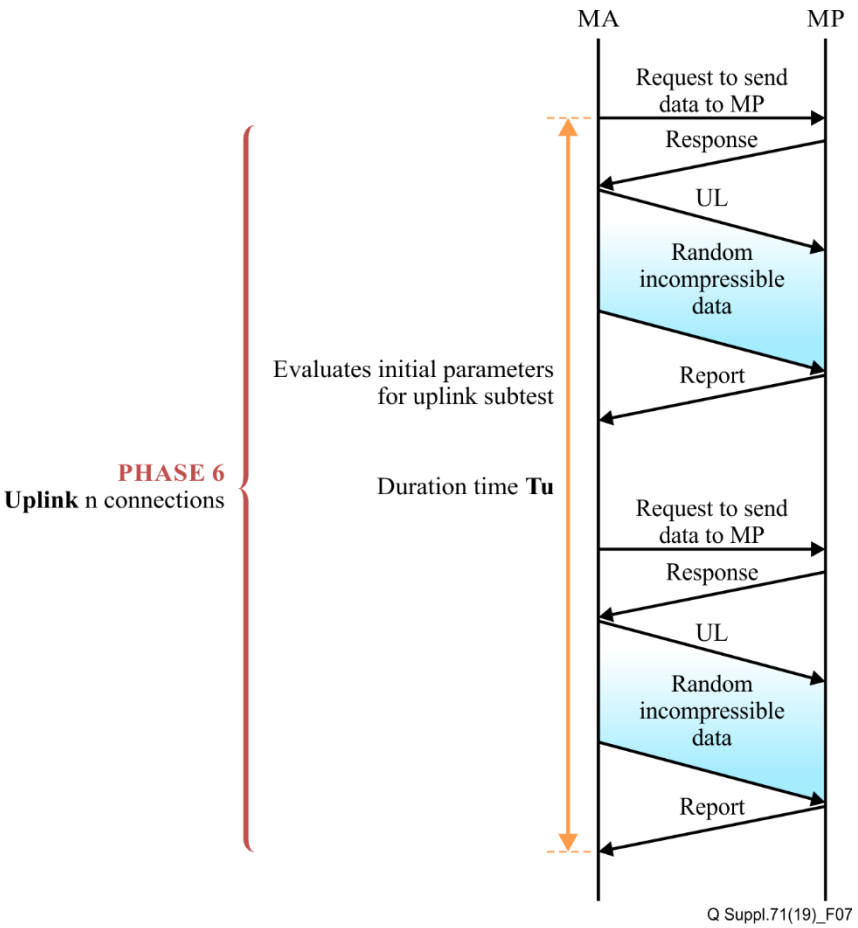

Figure 7 – Sample diagram of phase 6 of measurement algorithm

6.3.3.7 Phase 7: Finalization

After finishing all tests, the measurement agent sends the collected data to the Collector. All results and additional information on the measurement agent are transferred directly to the Collector. Both datasets are then compared by the Collector to check the quality and integrity of the result. All tests, successful or unsuccessful, are stored by the Collector.

6.4 Measurement of Data

According to [IETF RFC 7594] the reporting by the MA shall be encrypted to maintain confidentiality, so that only the authorized Collector can decrypt the results to prevent the leakage of confidential or private information. Reporting shall also be authenticated (to ensure that it comes from a trusted MA and that the MA reports to a genuine Collector) and not vulnerable to tampering (which can be ensured through integrity and replay checks). It shall not be possible to fool an MA by injecting falsified data and the results shall also be stored and processed securely after collection and analysis.

As far as it is available, the following information is stored for each completed test:

- Test UUID;
- Date and time;
- Latency;
- Uplink capacity (data rate);
- Downlink capacity (data rate);
- Number of concurrent connections;
- Client public IP.

- Client phone status and radio technology (e.g., UMTS, LTE, etc.) and quality (e.g., RSSI) Geo-location and tracking accuracy as well as movement during the test (lat, long, timestamp, accuracy, altitude, speed, bearing, location provider).
- The presented values which are measured shall have the minimum, the mean, the median and the max values.

Detailed download and upload procedure					
Duration time (example)	**Test equipment A**		**Network**		**Test equipment B Data reference system BST**
	Phase 1: Initialization	→ ←		→ ←	
2 s	**Phase 2**: Downlink pre-test	←		←	
2,5 s	**Phase 3:** Latency test	→		→	
7 s	**Phase 4:** Downlink				
	Start using multiple socket connection 1	←		←	
	Start using multiple socket connection 2	←		←	
	Start using multiple socket connection 3	←		←	
2 s	**Phase 5:** Uplink pre-test	→		→	
7 s	**Phase 6:** Uplink	→		→	
	Start using multiple socket connection 1	→		→	
	Start using multiple socket connection 2	→		→	
	Start using multiple socket connection 3	→		→	
	Phase 7: Finalization	→ ←		→ ←	

Figure 8 – Detailed download and upload procedure

An example of the detailed description of the communication protocol can be found in clause 8 of [ITU-T Q.3960].

Appendix I

Collecting additional information from user's hardware and software

Collecting data on the user's hardware and software configuration (SO, browser) can be useful not only for statistical result evaluation but also to send warnings to the users about unsuitable configuration if detected or other configuration problems that may lead to unreliable measurements. In contrast, collecting user's information can be a sensitive issue since it could threaten the privacy of the user if some delicate information is collected (i.e., geolocation). A "compromise solution" for this issue should be decided.

The following information could be collected

1) For fixed networks:
   - Test time;
   - Time zone;
   - User IP address;
   - TCP and UDP settings;
   - Operation system version;
   - Web-browser version/User agent (in case web technology is used);
   - Number of parallel connections (downlink and uplink);
   - Duration of pre-test;
   - Duration of the downlink subtest;
   - Duration of the uplink subtest;
   - Timeout value;
   - Number of 'pings' during delay subtest;
   - Maximum elapsed time between ping starts;
   - Reference size of data block (chunk size);
   - Number of received chunks after which the ME answers back to the TE
   - WS advertised during the TCP negotiation phase for the different TCP streams: Regarding the warnings, although n parallel connections will be launched in the test, the measurement peer will calculate whether or not the estimated round-trip time (RTT), OS (TCP flavour + typical Tx/Rx buffer sizes) and measured WS calculated for downlink and uplink speeds are too close (>90%) to the theoretical limitations. It will also determine if it is necessary to notify the user about the unreliability of the test and the need to optimize the configuration for achieving better speeds.

2) For mobile networks (in addition to information for fixed networks):
   - Cell global identification (CGI) [1]
     - The CGI is the concatenation of the location area identification (LAI) and the cell identity (CI)
     - LAI
       - LAI comprises mobile country code (MCC), mobile network code (MNC) and location area code (LAC).
         - MCC identifies the country in which the network public land mobile network (PLMN) is located.
         - MNC is a code identifying the network PLMN in that country.

        - LAC is a fixed length code (of 2 octets) identifying a location area within a PLMN.
    - CI or Physical Cell ID (PCI)
        - Identifies a cell in a certain location area.
- In case the access to GPS data is granted, the collection of National Marine Electronics Association (NMEA) string is preferred.
- Signal strength. Different parameters are accepted:
    - RSSI = Received Signal Strength Indicator
    - RSRP = Reference Signal Received Power
    - RSRQ = Reference Signal Receive Quality
    - SNR = Signal-to-noise ratio
    - SINR = Signal-to-interference-plus-noise ratio
    - RSCP = Received Signal Code Power (only for UMTS).
- Visible neighbouring cell towers, including CIs and signal strength. TBD
- Information regarding the access point name (APN) [1]
    - The APN network identifier defines to which external network the gateway GPRS support node (GGSN) or packet data network gateway (PGW) is connected.
    - The APN operator identifier defines in which PLMN general packet radio service (GPRS) or evolved packet system (EPS) backbone the GGSN/PGW is located.
- Bearer (CDMA, GPRS, EDGE, all 3G variants, LTE, etc.)
- Band in relation to the frequency under use (i.e., 3, 7 or 20 in case of LTE in Europe).

[1] ETSI, Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 version 10.5.0 Release 10)

Appendix II

Measurement of network parameters over NAT

This appendix describes the case when the measurement peers are behind a NAT, including the following procedures:

- The "Session Traversal Utilities for NAT" (STUN)
- NAT behavior discovery using session traversal utilities for NAT (STUN)
- Traversal using relays around NAT (TURN)
- Relay extensions to session traversal utilities for NAT (STUN)

The STUN procedure can be used if the performance measurements are based on the UDP transport protocol. The TURN procedure can be used if the performance measurements are based on TCP transport protocol.

II.1 STUN test architecture

The architecture is based on the STUN procedure which is shown in Figure II.1.

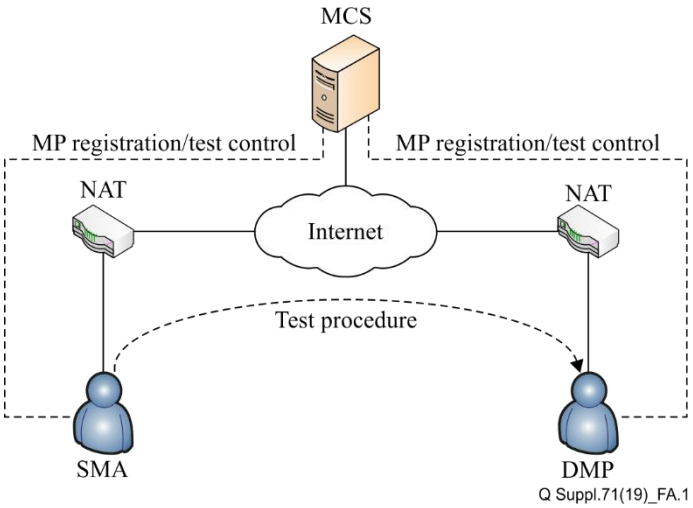

Figure II.1 – Testing architecture based on the STUN procedure

This architecture includes several types of devices:

1) Measurement control server (MCS) is a device based on the functional elements Controller FE and Collector FE indicated above in the main body of this Supplement. The MCS performs the functions of the testing control server. It also includes the database of the performed tests and the STUN server. MCS is responsible for:
   - Registration of SMA and DMP devices on the server using the unique identification numbers (UID);
   - Functioning as the STUN server, including mapping of the UID DMP, SMA, external IP address and NAT port corresponding to this DMP and SMA;
   - Generates test configurations for DMP and SMA;
   - Monitors the testing procedure;
   - Keeps information about testing;
   - Returns the test results to SMA.

2) The measurement peer (MP) is a device that has the role of an SMA or the DMP. This device does not have a public IP address and can operate behind one or multiple NATs. During the initialization phase, the device should establish a connection with the MCS. In the response message, the device receives a unique identification number (UID), its own IP address and the port allocated by NAT. With this identification number, the device can perform the specified test scenarios.

3) The source measurement agent (SMA) is a measurement peer (MP) which is based on the measurement agent FE specified above. This device initiates the testing procedure using the configuration obtained from the measurement control server (MCS). After registration on the MCS, SMA should receive the UID of the relevant destination measurement peer (DMP), the IP address and the NAT port of the called DMP. Afterwards, the SMA can perform the test scripts directly (SMA – DMP), bypassing NAT. After the testing is complete, the test results (data) are sent to the MCS.

4) The DMP is based on the functional element measurement peer FE defined above. After registration on the MCS, DMP is waiting for a test configuration, UID SMA, IP address and NAT port to which the SMA is connected to from the MCS. The testing is carried out directly (DMP – SMA), bypassing the NAT. After the testing is complete, the test results (data) are sent to the MCS.

The STUN procedure is based on the application layer protocol which uses the transport protocol UDP to bypass the NAT using a logical point-to-point connection (SMA-DMP).

II.2 TURN test architecture

The architecture is based on the TURN procedure and is shown in Figure II.2.

1) Measurement control server (MCS) is a device based on the functional elements Controller FE and Collector FE as indicated in this Supplement. The MCS is to perform the functions of the testing control server. It also includes the database of the performed tests and the TURN server.

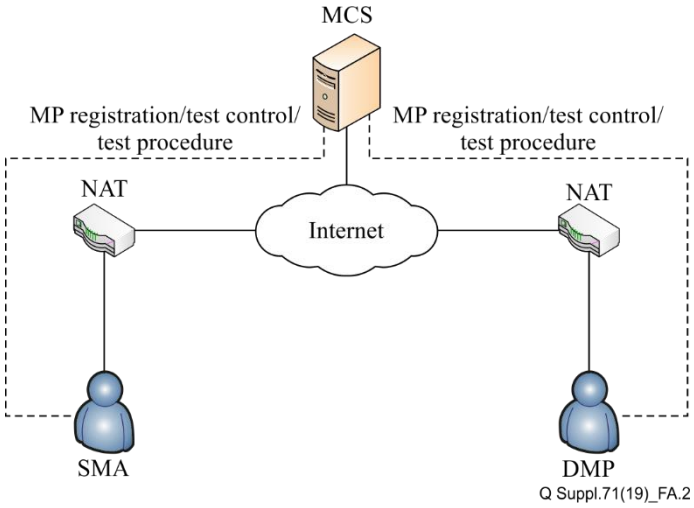

Figure II.2 – Testing architecture based on the TURN procedure

The common procedures are similar to the STUN architecture defined above.

The TURN procedures are based on application layer protocols that use the TCP and UDP transport protocols to bypass NAT, using the MCS TURN server as an intermediate node (SMA – MCS – DMP). This procedure is not recommended for tests based on the UDP application layer protocols.

Testing procedures

The procedure for testing throughput to a remote device connected to the Internet affects the following network parameters:

- Uplink data transmission throughput;
- Downlink data transmission throughput;
- Latency.

In order to test the above listed network parameters, the following types of tests should be executed:

- Uplink pre-test;
- Uplink test;
- Downlink pre-test;
- Downlink test;
- Latency test.

The scenario of the functioning of the measurement system based on the STUN procedure is shown in Figure II.3.

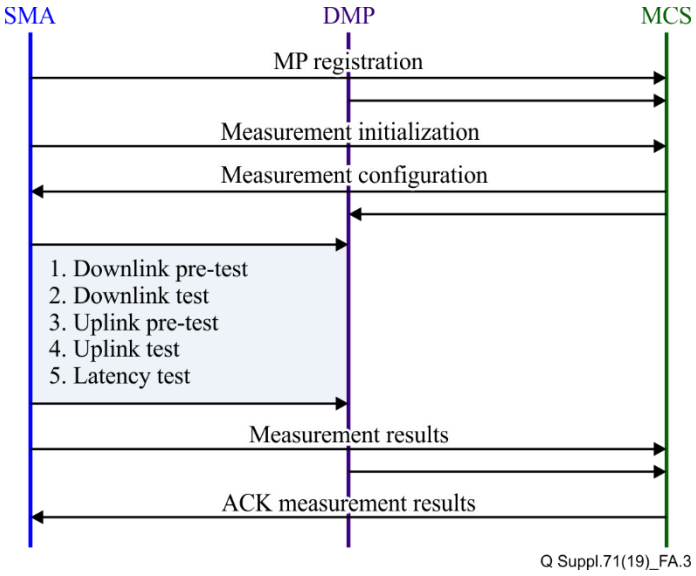

Figure II.3 – The workflow of the STUN-based testing system

The scenarios based on the TURN procedure is shown in Figure II.4.

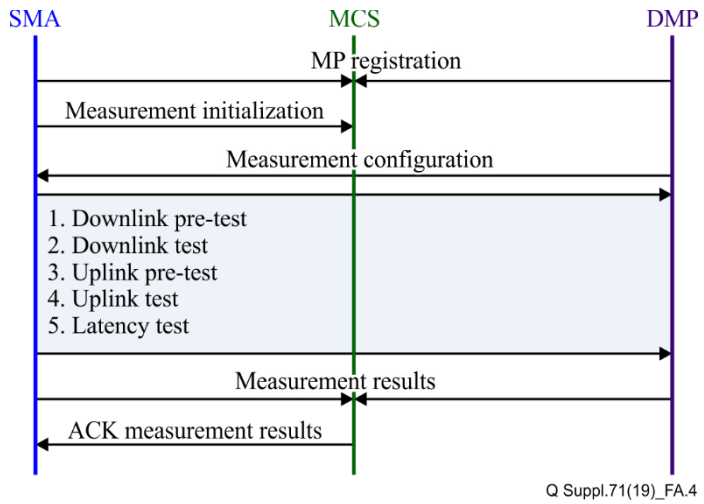

Figure II.4 – The workflow of the TURN-based testing system

Measurement data

It is assumed that the nodes are exchanging the information in the JSON data format.

When a node is registered on measurement control system, each node sends the following information:

- Message type (setup);
- Write window throughput for measurement peer;
- Read window throughput for measurement peer;
- Measurement peer address;
- Measurement peer port.

After registering the node, measurement control system returns the following information to the node:

- Message type (setupACK);
- Measurement peer address;
- Measurement peer port;
- Measurement peer UID.

When measurement is initialized, the following information is passed to the measurement server from source measurement peer:

- Test type;
- Message type;
- Timeout;
- Test duration;
- Write window throughput for source peer;
- Read window throughput for source peer;
- Threads quantity;
- Package quantity – for latency tests and as an alternative to the parameter test duration (optional);
- Size of the test message body – for uplink and downlink throughput tests (optional);
- Used encryption: SSL/TLS, DTLS, NONE;
- Encryption/ decryption method: RSA, NTRUEncrypt, ECC, AES etc.;
- Destination peer UID;

- Measurement peer UID.

As far as it is available, the following information is stored for each completed test e.g.:

- Test UUID;
- Destination peer UID;
- Source peer UID;
- Test type;
- Message type;
- Threads quantity;
- Date and time;
- Latency;
- Uplink data transmission throughput;
- Downlink data transmission throughput;
- Package loose indicator;
- Measurement protocol: HTTP, HTTPS, CoAP, MQTT, FTP etc.;
- Used encryption: SSL/TLS, DTLS, NONE;
- Encryption/decryption method: RSA, NTRUEncrypt, ECC, AES etc.;
- Destination peer address;
- Destination peer port;
- Source peer address;
- Source peer port;
- Number of concurrent connections measurement agent public IP (Optional);
- Measurement agent phone status and radio technology (e.g., UMTS, LTE, etc.) and quality (eg., RSSI). (Optional for radio-frequency networks);
- Geo-location and tracking accuracy as well as movement during the test (latitude, longitude, altitude, timestamp, speed, bearing, location provider, information to assess GPS accuracy, etc.). (Optional).

Bibliography

[b-ITU-T M.1400] Recommendation ITU-T M.1400 (2015), *Designations for interconnections among operators' networks*.

[b-ITU-T M.3208.1] Recommendation ITU-T M.3208.1 (1997), *TMN management services for dedicated and reconfigurable circuits network: Leased circuit services*.

[b-ITU-T M.3320] Recommendation ITU-T M.3320 (1997), *Management requirements framework for the TMN X-Interface*.

[b-ETSI EG 202 057-4] ETSI Guide 202 057-4 (2008), *Speech processing, transmission and Quality aspects (STQ); User related QoS parameter definitions and measurements; Part 4. V1.2.1*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling, and associated measurements and tests**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020