International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3056

(12/2019)

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

Signalling requirements and protocols for the NGN – Network signalling and control functional architecture

Signalling procedures of the probes to be used for remote testing of network parameters

Recommendation ITU-T Q.3056

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
General	Q.3000–Q.3029
Network signalling and control functional architecture	**Q.3030–Q.3099**
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	Q.3600–Q.3616
Service and session control protocols – supplementary services based on SIP-IMS	Q.3617–Q.3639
VoLTE/ViLTE network signalling	Q.3640–Q.3655
NGN applications	Q.3700–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.

Recommendation ITU-T Q.3056

Signalling procedures of the probes to be used for remote testing of network parameters

Summary

Recommendation ITU-T Q.3056 describes architecture and signalling procedures to be used for remote testing of network parameters utilizing probes. These procedures include the execution of testing, testing profile templates, storing of measurement results, and authorized access for users to test results. The procedures also enable a probe to function as a "black box" recording all events on the subscriber side, and suitable for a trusted system in resolving disputes between various information and communication technology (ICT) stakeholders.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3056	2019-12-14	11	11.1002/1000/14142

Keywords

Probe, protocol, remote testing, signalling, test process, test profile.

* 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

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 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/.

Table of Contents

Recommendation ITU-T Q.3056

Signalling procedures of the probes to be used for remote testing of network parameters

1 Scope

This Recommendation defines requirements for high level signalling procedures intended for use in controlling probes used for remote testing of network parameters.

The signalling procedures described in this Recommendation propose secure storage of measurement results and authorized access for users to test results, with no possibility of third parties modifying the structure and content of measurement results.

These procedures enable a probe to function as a "black box" recording all events on the subscriber side, and suitable for a trusted system in resolving disputes between various ICT stakeholders.

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

[ITU-T Y.3011] Recommendation ITU-T Y.3011 (2012), *Framework of network virtualization for future networks*.

[ETSI ES 201 770] ETSI ES 201 770 (2000), *Methods for Testing and Specification (MTS); Test synchronization architectural reference; Test Synchronization Protocol 1 plus (TSP1+) specification*.

[IETF RFC 5389] RFC 5389 (2008), *Session Traversal Utilities for NAT (STUN)*.

[IETF RFC 5766] RFC 5766 (2010), *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)*.

[IETF RFC 5780] RFC 5780 (2010), *NAT Behavior Discovery Using Session Traversal Utilities for NAT (STUN)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 testing [b-ITU-T L.300]: Activities for evaluating faults and the condition of NEs after installation, and for identifying fault locations.

3.1.2 probe [b-ITU-T Y.1545.1]: Is an end-point test tool which uses probing packets to collect measurements.

3.1.3 signalling message [b-ITU-T Q.9]: An assembly of signalling information pertaining to a call, management transaction, etc., comprising also elements for delimitation, sequencing and error control, that is transferred as an entity.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
DCAOS	Data Collection, Analysis and Output Subsystem
ICT	Information and Communication Technology
ISP	Internet Service Provider
MCS	Monitoring Subsystem
NAT	Network Address Translation
NE	Network Element
NFV	Network Virtualization Technologies
P2P	Peer-to-Peer
QoS	Quality of Service
STUN	Session Traversal Utilities for NAT
TURN	Traversal Using Relay NAT
VRM	Virtual Resource Manager

5 Conventions

This Recommendation uses the following conventions:

MDB	Test database
MUID	Unique Test Identifier
PDB	Node database
PUID	Unique Probe Identifier
RTNP	System for remote testing of network and communication service parameters
SMP	Application test node
SMP CI	Interoperation interface with the application test node

6 Introduction

Most operators have private technical solutions for assessing the performance of their networks, and users have no alternative means of justifying any claims regarding appropriate or inadequate provision of communication services.

The solution to this problem involves the creation of an algorithm/protocol that can be used by probes and whose measurements can be trusted by all ICT stakeholders. Using such a trusted protocol will preclude any possibility of operational services of an operator influencing monitoring system readings

and thus ensure for the users the reliability of data on the technical characteristics of the service provided.

7 Architecture of the system

A system for remote testing of network and communication service parameters has client-server architecture and comprises the following elements:

Probe – a client system for monitoring the quality of communication services, comprising the following subsystems:

- Application test node (SMP)
- Application test node interoperation interface (SMP CI).

Server for remote testing of network and communication service parameters (RTNP server), comprising the following subsystems:

- Monitoring subsystem (MCS)
- Data collection, analysis and output system (DCAOS)
- Test database (MDB)
- Node database (PDB)

The architecture of the system is illustrated in Figure 1.

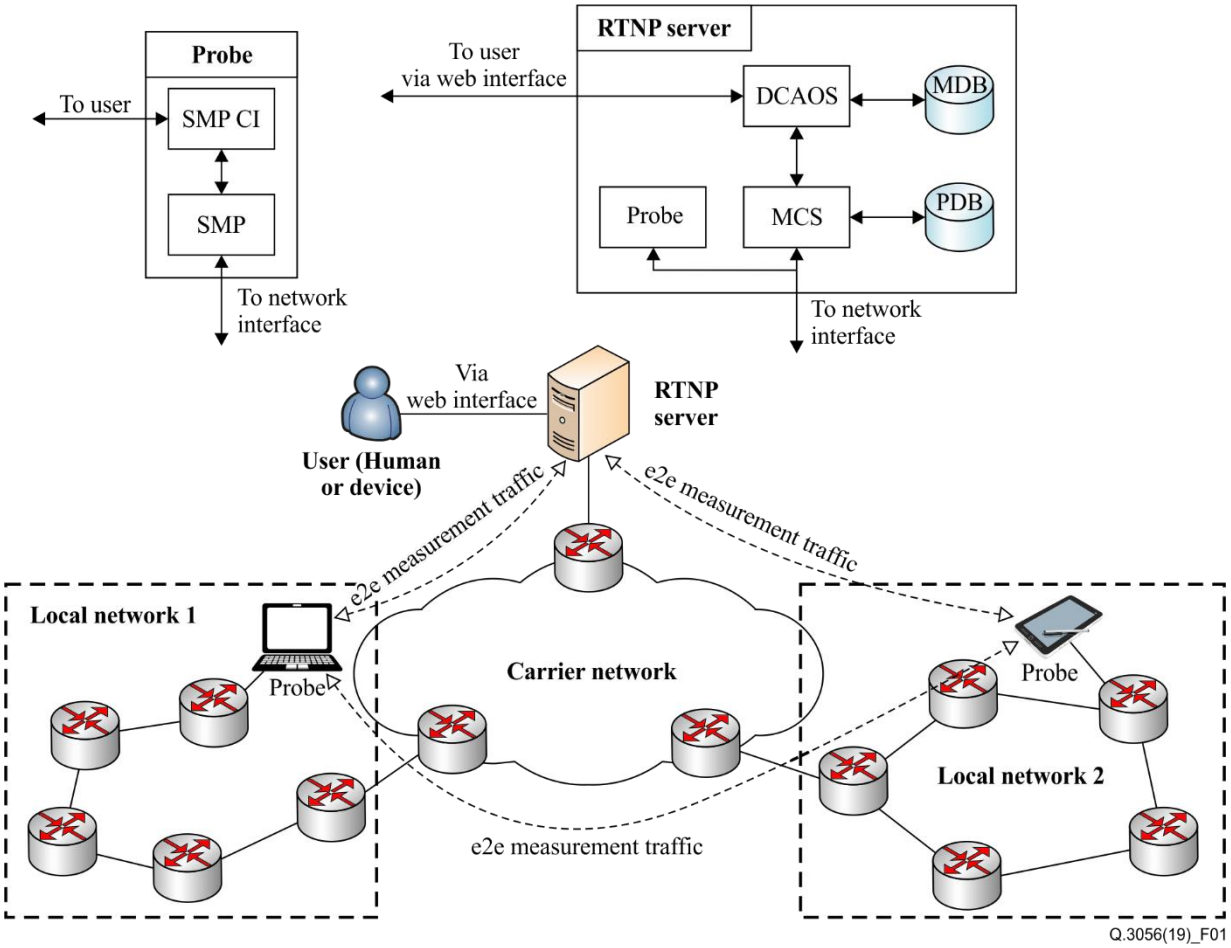

Figure 1 – Architecture of a system for remote testing of network and communication service parameters

Depending on the particular features of the network construction and the tasks, all the elements and subsystems indicated in this clause may be used jointly or separately in differing combinations, including in a single hardware system.

7.1 Probes

A probe is the separate element of the RTNP system. It can be in the form of a hardware and/or software.

Application test node (SMP) – software running in background mode implementing test scenarios, using test configurations obtained from the monitoring subsystem, and carrying out collection, saving and transmission of measurements and forming, on the basis of the test configurations obtained, traffic flows using the selected level 3-7 protocol in accordance with the OSI model.

The SMP performs the following functions:

- Receives and transmits information from/to the SMP CI;
- Implements test scenarios in accordance with test configurations obtained from the SMP CI;
- Generates traffic flows based on the test configurations received from the SMP CI.

SMP CI – application that performs the function of interoperation with the application test node. It may be a graphic interface, console interface, network interface, or application interface. The application may perform the functions of one of the aforementioned interfaces or of several simultaneously, depending on the task.

The SMP CI performs the following functions:

- Reception and transmission of information from/to the SMP;
- Entry and output of the initial configuration of the SMP (address of server and port, type of hardware platform, PUID);
- Selection, initial configuration and launch of test scenario;
- Entry and output of current test configuration (test scenarios, PUID, IP-address, SMP port, MUID);
- Sends interim and final test results;
- Updates software of probe.

7.2 The server of the system for remote testing

The server shall be capable of managing the execution of testing sessions. The functionality of the server is delivered by the subsystems as follows.

The monitoring subsystem is a server program that monitors the implementation of test scenarios. It performs the following functions:

- Registers probes in the system, allocating a unique node identifier number (PUID);
- Generates test configurations for the probes including a unique test identification number (MUID);
- Receives test configurations from the probes including their unique test identification numbers (MUID);
- Receives and transmits test configurations from/to the probes;
- Receives and transmits interim and final test information from/to the probes;
- Interoperation with the data collection, analysis and output system;
- Records and reads data probes in/from the node database, using the PUID;
- Constantly monitors QoS for the probes registered in the node database;

– Where it is necessary to implement scenarios based on peer-to-peer (P2P) technologies, performs session traversal utilities for NAT (STUN) server and traversal using relay NAT (TURN) server functions.

Data collection, analysis and output subsystem – a server program subsystem carrying out collection, analysis and output of data obtained from implementing a given test scenario. It performs the following functions:

– Interoperation with the monitoring subsystem;
– Input and output of information on completed tests;
– Analysis of information received on completed tests;
– Output of useful information on completed tests for the user, with the aid of a web interface;
– Recording and reading of test information on/from the test database using the MUID.

Test database – a server program subsystem that carries out recording, reading and storage of data on completed tests using a MUID.

Node database – server program subsystem that carries out recording, reading and storage of data concerning registered probes on a RTNP server, using the PUID.

8 Testing process

A general logic diagram of the testing is presented in Figure 2.

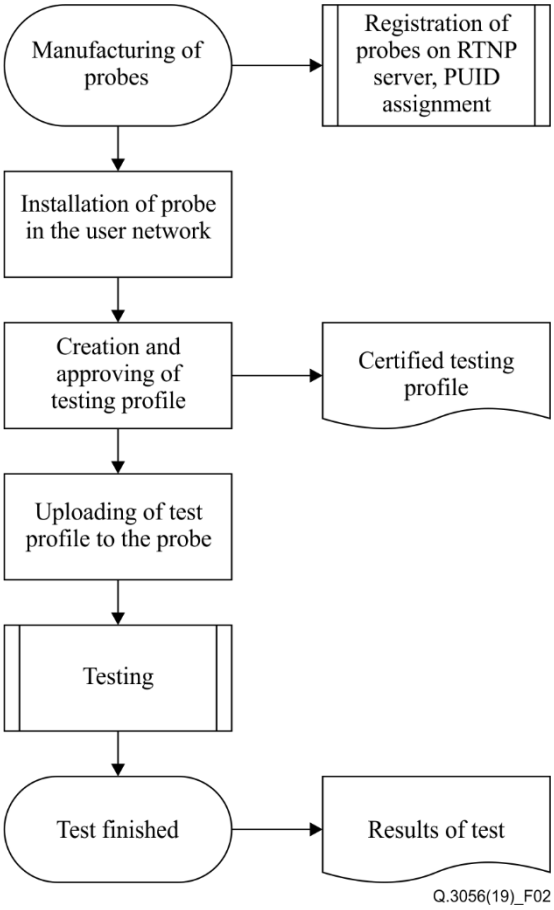

Figure 2 – General logic of the testing using probes

The remote testing relies on a distributed system of verified probes. Each probe includes a built-in hardware unique identifier. The identifier is resistant to tampering by software-based methods.

After the installation of probes in the testing points is completed, the RTNP server provide authentication and authorization of probes for testing. Before running a test, the RTNP server may verify that all test components involved in the test are ready to start.

NOTE – The concrete approaches used by RTNP server for authentication and authorization of probes are outside the scope of this Recommendation.

The testing process may include active and/or passive modes of probes. In the passive mode, probes measure the network performance parameters with preestablished rate. In this mode the testing process does not considerably affects the ongoing operations in the undertest network. In the active mode, probes mimic the traffic flow of certain application, which may affect the operation characteristic of the network or even interrupt ongoing processes.

At the end of the testing, results are available on the RTNP server. The results are stored according to the policy accepted by the user and accessible via web interface in the RTNP server.

9 Testing profiles

The result of testing may depend on established test parameters. Test parameters are stored in a testing profile. For the correct testing, appropriate testing profile have to be used. Before testing, the profile must be approved and certified by the user and telecommunication provider. The test profile cannot be changed unilaterally. A structure of the test profile depends on the mode of probe.

9.1 Testing profile for passive mode

Testing profile for passive mode include a set of parameters to be monitored during the test, frequency of measurements, and methodology of the measurement. The list of parameters to be monitored may include, but are not limited to:

- Round trip time, ms
- Jitter, ms
- Packet loss ratio, lost packets/received packets
- Internet speed measurement, Mbit/s.

9.2 Testing profiles for active mode

The testing profiles for the active mode in addition to the parameters measured in passive mode include scripts describing traffic model for an application. Using these scripts, probes emulate the work of applications through the use of similar traffic patterns. The main parameters defined by the script are:

- Application layer protocols;
- Ports;
- Traffic distribution between IP addresses;
- Uplink/downlink ratio, Mbit/sec;
- Average packet size, KB;
- Average packet rate, packets/sec.

10 Signalling

This clause contains a set of standard messages used for managing probes by RTNP.

10.1 Test configuration establishment messages

Table 1 contains a set of standard messages used for test configuration establishment.

Table 1 – Test configuration establishment messages

Message	Source	Comment
SIGRTS	RTNP	Request for establishing testing session. This command is used to verify that probes are ready to start testing.
SIGNOT	RTNP	Notification about testing duration. This command configures the time of the test (if connection between server and probe is interrupted, probes still continue testing procedure until testing duration time expired).
SIGTPU	RTNP	Testing profile uploading. Uploading testing profile to the probe and verify its correct implementation.
SIGSTR	RTNP	Start of a test command.
PACK	Probe	Confirmation that command is accepted and successfully implemented.

10.2 Test session notifications

Table 2 contains a set of standard messages used for test session notifications.

Table 2 – Test session notifications

Message	Source	Comment
SIGCRQ	RTNP	Configuration request. Allows the server to check the current probe configuration, including testing profile values.
SIGSU	RTNP	A probe's status update.
SIGTRQ	RTNP	Testing timer status request. Command used to check test time remaining.
PCR	Probe	A probe's configuration report.
PSU	Probe	A probe's status report.
PTS	Probe	Testing time remainder.
PFER	Probe	Error code. (1 – hardware error, 2 – firmware error, 3 – testing profile error, 4 – other).

10.3 Test completion

Table 3 contains a set of standard messages used for test completion.

Table 3 – Test completion

Message	Source	Comment
SIGTI	RTNP	Test interruption command.
PTFR	Probe	Test finished notification and report about test execution.
SIGFIN	RTNP	Server accepted report and terminated test session.

Appendix I

Use cases

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

I.1 Services highly dependent on the quality of the network

A network testing using probes can be used as a tool for the sharing of responsibility among subscriber and telecommunication provider in business cases when the quality of the network is critical. These applications can be divided into two groups. The first group include applications where low quality of network services can lead to criminal liability of the user. Examples of such cases include remote surgery and other applications causing damage and threat to the life and health of people. The use of an independent assessment of network using probes would help to determine failures in the application due to the unsatisfactory quality of the network.

The second group includes cases where, as a result of unsatisfactory performance of telecommunication services, the user suffers financial and reputational losses. Examples of such applications are remote cash terminals, ATMs and remote video surveillance. In these cases, the data of independent testing of the network with the use of probes can be used as a basis for claims to the telecommunication provider if there are conditions in the contract for the provision of services on the quality of the network (for example, the availability factor).

I.2 Testing of network with NFV

Network virtualization technologies (NFV) has the ability to create logically isolated areas of the network, providing users with virtual resources (telecommunications channels, storage, computing power, etc.) using shared physical resources. It is possible that the total maximum demand for resources of virtual services will exceed the available physical resources. In this situation, in order to provide quality parameters agreed with the user, the Internet service provider (ISP) may need to use additional resources (communication channels), including their rent from third parties. To manage this process, it is required to obtain objective information about existing and leased physical resources which can be used as the architecture of the monitoring and remote testing based on probes.

Thus, the ISP can get information about the actual quality of service (QoS) parameters as well as physical resources that are allocated between virtual resources. The example of interaction of elements is shown in Figure I.1.

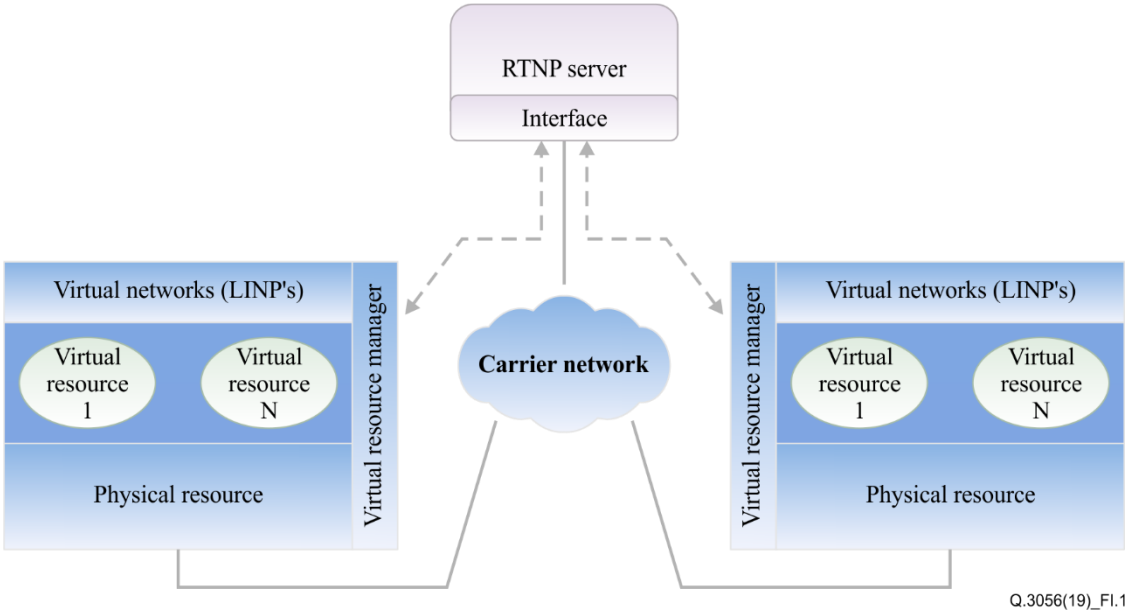

Figure I.1 – The principle of NFV and RTNP interaction

- Physical resource is specified in [ITU-T Y.3011].
- Logical resource is specified in [ITU-T Y.3011].
- Virtual resource manager (VRM) is responsible for management/redistribution of physical resources between virtual resources. The communication procedure with VRM highly depends on the manufacturer.
- Interface – a software interface (REST or other) to interact with the server RTNP.
- The solid black line is the physical line connection.
- Dotted line shows the interaction between VRN and RTNP server using the application programming interface (API).

NOTE – Probe can also be placed as a virtual entity on one of the physical resources, it gives flexibility and convenience in deploying the test system, as well as dynamic distribution/redistribution of probes in the communication network.

I.3 Testing the readiness of the corporate network to deploy new services with the required level of availability and quality

An approach can be suggested to test network availability when deploying new services. It can be implemented on both corporate and ISP networks.

In a case of corporate networks, it is necessary to check network capabilities before deployment of new applications, such as Skype for business, online production management systems, or more demanding applications, such as telemedicine services (remote surgery).

ISP network testing will help to identify possible problems in the implementation of demanding services, such as multimedia for virtual reality applications or real time applications.

In these cases, the purpose of testing is to predict possible problems in the functioning of the services, identifying weaknesses in the network before the deployment of the service. The results will give a clear understanding of the necessary investments to achieve the required QoS before deployment of new services.

Bibliography

[b-ITU-T L.300] Recommendation ITU-T L.300/L.25 (2015), *Optical fibre cable network.*

[b-ITU-T Y.1545.1] Recommendation ITU-T Y.1545.1 (2017), *Framework for monitoring the quality of service of IP network services*.

[b-ITU-T Q.9] Recommendation ITU-T Q.9 (1988), *Vocabulary of switching and signalling terms*.

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