International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3913

(08/2014)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Testing for next generation networks

Set of parameters for monitoring Internet of things devices

Recommendation ITU-T Q.3913

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

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.3999
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.3649
NGN applications	Q.3700–Q.3849
Testing for next generation networks	**Q.3900–Q.3999**

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

Recommendation ITU-T Q.3913

Set of parameters for monitoring Internet of things devices

Summary

Recommendation ITU-T Q.3913 identifies the set of parameters that indicate the status of devices, including traffic parameters, anomalous behaviour and events parameters, performance parameters and battery parameters. This Recommendation also provides measurement metrics for device monitoring.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3913	2014-08-29	11	11.1002/1000/12219

Keywords

Anomalous behaviour, device, monitoring, performance, traffic.

* 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.3913

Set of parameters for monitoring Internet of things devices

1 Scope

This Recommendation provides measurement metrics for device monitoring and defines the set of parameters that indicate device status, including device traffic, anomalous behaviour, events, performance and power supply. These parameters may be generated by network elements, terminals and access gateways. The definitions provided here are dependent on next generation networks (NGN), which use Internet Protocol (IP) as the bearer protocol. How these parameters are monitored is outside of the scope of 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 Y.2060] Recommendation ITU-T Y.2060 (2012), *Overview of the Internet of things*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 device [ITU-T 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 flow: A flow is defined as a set of IP packets passing an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties. A packet is defined as belonging to a flow if it completely satisfies all the defined properties of the flow.

3.2.2 observation point: The observation point is a location in the network where IP packets can be observed.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

FEC Forwarding Equivalence Class

ICMP Internet Control Message Protocol

IMEI International Mobile Equipment Identity

MEID Mobile Equipment Identifier

MPLS Multi-Protocol Label Switching

QoS Quality of Service

TCP Transmission Control Protocol

UDP User Datagram Protocol

5 Measurement metrics

Devices can be either stand-alone or situated in a local network. Devices in a local network can be monitored using monitors or probes, which are instruments that enable the transmission of monitoring data to a monitoring system in order to determine the status of a local area network and devices.

The monitors or probes can be integral to the devices or can be stand-alone. Probes usually record behaviour or measure the device traffic. This form of measurement is known as passive measurement. These probes often devote significant internal resources to device management. Monitoring the performance of a device uplink is also known as traffic measurement.

To determine the status of a device, monitoring software in the monitor or probe may periodically send a test message from a remote monitoring system. This is known as active measurement. Commonly measured metrics include response time and availability. However, both consistency and reliability metrics are starting to gain popularity.

In addition, these monitors/probes may be used by a network management service provider to access a remote device.

6 Monitoring parameters

Monitoring parameters include:

– Traffic parameters (see clause 6.1)

– Anomalous behaviour and events parameters (see clause 6.2)

– Performance parameters (see clause 6.3)

– Battery parameters (see clause 6.4)

6.1 Traffic parameters

6.1.1 General

Traffic measurement can be applied in usage-based accounting, traffic profiling, traffic engineering, attack/intrusion detection and QoS monitoring. For example, flow-based traffic measurement can be used to help determine device performance or behaviour through the analysis of the measurement parameter values.

6.1.2 Flow-based IP traffic measurements

Flow-based IP traffic measurements can be performed by a router while forwarding traffic, or by a traffic measurement probe attached to a link between the device and the network. A flow record contains measured properties of the flow (e.g., the total number of bytes of all packets of the flow) and usually also contains characteristic properties of the flow (e.g., source IP address).

The following attributes are required to be reported for each flow:

– the IP version number (this requirement only applies if the observation point is located at a device supporting more than one version of IP)

– the source IP address
– the destination IP address
– the IP protocol type (TCP, UDP, ICMP, etc.)
– the source TCP/UDP port number (if the protocol type is TCP or UDP)
– the destination TCP/UDP port number (if the protocol type is TCP or UDP)
– the packet counter value (If a packet is fragmented, each fragment is counted as an individual packet.)
– the byte counter value (The sum of the total length in bytes of all IP packets belonging to the flow. The total length of a packet covers the IP header and IP payload.)
– the type of service octet (in the case of IPv4) or the traffic class octet (in the case of IPv6)
– the flow label (in the case of IPv6)
– the top multi-protocol label switching (MPLS) label if MPLS is supported at the observation point, or the corresponding forwarding equivalence class (FEC) bound to that label. The FEC is typically defined by an IP prefix
– the timestamp of the first packet of the flow
– the timestamp of the last packet of the flow
– the sampling configuration if sampling is used
– the unique identifier of the observation point

6.2 Anomalous behaviour and events parameters

Monitoring anomalous behaviour or events is an important aspect of security threat detection. A baseline of normal behaviour must be identified over a period of time. Once certain parameters have been defined as normal, any departure from one or more of these parameters is flagged as anomalous. Many anomaly detection algorithms have been proposed that differ in the information used for analysis and in the techniques that are employed to detect deviations from normal behaviour. Examples of anomaly detection methods include statistical methods, rule based methods, profiling methods and model-based approaches.

6.2.1 Abnormal service activity

Abnormal service activity is an activity that is significantly above or below ordinary service activity levels. The ordinary state of service is defined by a set of service rules. Parameters used to determine if the device is in ordinary state of service include:

– Service interval: The service interval should not be significantly above or below the normal interval.
– Data transmitted or received by the device: The amount of data transmitted or received should not be significantly above or below normal levels.
– Date and time: The date or time should not correspond to the device in activity state.

6.2.2 Mismatch between IMEI/MEID and IMSI

If there is a change in the association between the IMEI/MEID of a device and the international mobile subscription identity (IMSI) of the universal integrated circuit card (UICC), the IMEI/MEID of the device will be unmatchable to the IMSI, which means that the device or the UICC could be used unlawfully. The association between the IMEI/MEID and the IMSI can be defined by the user profile.

6.2.3 Loss of connectivity

A device is connected to the network when it is in active state, or if it is in an idle or dormant state and it can go into active state as the result of a specific command. If the connectivity of the device is lost and cannot be activated it means that the device has been either damaged or stolen. The network connectivity of devices should be monitored.

6.2.4 Change of location

A device may change geographical position and/or point of attachment to the network. Such behaviour should be monitored if the point of attachment to the network is predefined by the profile. It is regarded as change of location if the position of the device is outside of the profile defined.

6.2.5 Unusual logon activities

Since a device may regularly sign into an account from a fixed position or according to a schedule, it might at times be obvious that recent activity was unusual. There are a few parameters that can be used to determine if recent activity was unusual:

– Date and time: The date or time should not correspond to the device access logon to the account.

– Location: If the device signs-in from a physical location that differs from where the device is located or if the physical location where the sign-in took place is not recognized, then the activity may be considered as unusual.

– IP address and domain: An IP address or domain that the device has never used to access the network.

6.3 Performance parameters

6.3.1 Delay

Delay is the interval that a data packet takes to go from the origin to the destination and back. In actual measurement, delay is usually indicated as a round-trip time (RTT), which means the round-trip interval between the origin and the destination.

The value of the delay parameter can indicate a change in device state. The main aspects that influence delay are listed as follows:

– Situation of the device and network congestion: If there is no congestion in the network or the device, the value of the delay parameter is relatively small; otherwise, the value of the delay parameter is relatively large

– Link failure: If the delay suddenly increases in the test path, then there was possibly a link failure

– Device performance: If the device being measured is idle, then the response time is short; otherwise the response time is long.

6.3.2 Packet loss rate

Packet loss rate is the rate of lost data packets during delivery from/to the origin to/from the destination in a specific time interval.

Packet loss rate can be expressed by the following formula:

$$LOSS = \frac{N_{lost\_packets}}{N_{all\_packets}} \times 100\%$$

$N_{lost\_packets}$: The total number of data packets lost during the delivery from the origin to the destination.

$N_{all\_packets}$: The total number of data packets during the delivery from the origin to the destination.

6.3.3 Throughput

Throughput is the rate of transmission at which data passes through a device. It is usually measured in bits per second, bytes per second or data packets per second. Throughput is measured by monitoring the transmission of data packets in a specific interval.

As an example, when the throughput is measured in data packets per second it can be expressed by the following formula:

$$Throughput = \frac{b}{T}$$

T: Measurement time interval.

b: The total number of data packets passing through the observation point in time T.

When measuring throughput, the time interval must be selected with care. A time interval that is too long may make burst traffic appear smooth, while a time interval that is too short may exaggerate burst traffic.

6.3.4 Link utilization

Link utilization refers to the extent to which a device actually uses its link throughput in a specific time interval.

When calculating link utilization the unit of throughput and link utilization should stay the same.

Link utilization can be expressed by the following formula:

$$\mathrm{U} = \frac{\mathrm{Throughput}}{R}$$

Throughput: The link throughput in the specific interval.

R: The total bandwidth of link.

U: Link utilization.

A change in link utilization indicates the congestion trend of a device. If the link utilization is too high, the device connected by the link may be susceptible to congestion, which may lead to poor performance.

6.3.5 Availability

Availability is the percentage of the time period in which a device has a normal operation status within a specific interval.

The calculation of availability can be expressed by the following formula:

$$\mathrm{A} = \frac{t}{T}$$

t: The uptime or time period in which the device is in normal operation.

T: The total time.

A: Availability.

When performing a specific measurement of availability, two types of availability should be considered:

– Service availability: The ability of a specific service to be operated normally.

– Node availability: The ability of a device to provide services.

6.4 Battery parameters

A device may use a battery as a power supply when the device is mobile, in open country or when the mains power supply is out of service. Some battery parameters should be monitored to indicate the battery state, longevity and capacity so that the operator is informed of the current or future sate of the device.

6.4.1 Temperature

Temperature is a numerical measurement of how hot or cold something (a device) is. Operating at extremes of cold and heat not only has a profound effect on the battery capacity and longevity, but also reduces charge acceptance. For example, colder operating temperatures will yield slightly increased longevity, but will lower the capacity of the lead acid cells. Higher temperatures yield increased battery capacity but have a detrimental effect on longevity.

Temperature is measured in degrees centigrade or in degrees Fahrenheit.

6.4.2 Voltage

Voltage is the difference in electric potential between two points; it signifies the amount of power in an electric current. A voltage may represent either a source of energy (electromotive force), or it may represent lost, used or stored energy. A voltage measurement indicates if the power source is in ordinary service state or not.

Voltage is measured in volts.

6.4.3 Discharge current

Discharge current is a measurement of the flow of electricity that a battery releases from stored energy or electric charge through a device or circuit. Combined with the remaining capacity of the battery, the discharge current measurement can be used to estimate the remaining lifetime of the battery.

Discharge current is measured in amperes.

6.4.4 Charging current

Charging current is a measurement of the flow of electricity that a battery will store as energy. Charging current can be used to estimate the time the battery will require to be fully charged.

Charging current is measured in amperes.

6.4.5 Remaining capacity of the battery

Battery capacity is a measurement of the electric charge a battery can deliver at the rated voltage. The remaining capacity of a battery indicates how long the device will work without mains electricity supply. A low remaining capacity or depth of discharge (DOD) affects the life of the battery. A remaining capacity lower than approximately 20% can be expected to shorten battery life. Telecom operators must be able to estimate the remaining capacity of a battery in the event of a mains electricity supply failure.

Remaining battery capacity is measured in ampere-hours or milliampere-hours.

Bibliography

[b-ITU-T Y.2061] Recommendation ITU-T Y.2061 (2012), *Requirements for support of machine-oriented communication applications in the next generation network environment*.

[b-ETSI TR 103 167] ETSI TR 103 167 V1.1.1 (2011), *Machine-to-Machine Communications (M2M);Threat analysis and counter-measures to M2M service layer*.

[b-ETSI TS 102 689] ETSI TS 102 689 V2.1.1 (2013), *Machine-to-Machine communications (M2M);M2M service requirements*.

[b-3GPP TS 22.368] 3GPP TS 22.368 V 12.2.0 (2013), *Service requirements for Machine-Type Communications (MTC)*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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	Terminals and subjective and objective assessment methods
Series Q	**Switching and signalling**
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014