3GPP TR 32.811 V7.0.0 (2007-06)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Telecommunication management;
Itf-N Performance Criteria: Requirements
(Release 7)

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Keywords
UMTS, management, Itf-N performance criteria

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

For the purpose of management interface development, 3GPP has developed an interface concept known as Integration Reference Point (IRP) to promote the wider adoption of standardized management interfaces in telecommunication networks.

The IRP concept and associated methodology employs protocol and technology neutral modelling methods as well as protocol specific solution sets to achieve its goals.

The present document defines Itf-N performance criteria.

1 Scope

The present document provides the overall performance criteria for all Integration Reference Point (IRP) specifications produced by 3GPP.

Relevant IRP overview and high-level definitions are provided in 3GPP TS 32.101 [1], 32.102 [2] and 32.150 [3].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 32.101:"Telecommunication Management, Principles and high level requirements".

[2] 3GPP TS 32.102:"Telecommunication management; Architecture".

[3] 3GPP TS 32.150:"Telecommunication management; Integration Reference Point (IRP) Concept and definitions".

[4] 3GPP TS 32.600:"Telecommunication management; Configuration Management (CM); Concept and high-level requirements".

[5] 3GPP TS 32.111-2:"Telecommunication management; Fault Management (FM); Integration Reference Point (IRP) Information Service (IS)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Information Object Class (IOC): see 3GPP TS 32.101 [1].

IRP: see 3GPP TS 32.101 [1].

Network Element (NE): see 3GPP TS 32.101 [1].

Network Resource (NR): see 3GPP TS 32.101 [1].

Network Resource Model (NRM): see 3GPP TS 32.101 [1].

Operations System (OS): see 3GPP TS 32.101 [1].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

EM Element Manager

MP Measurement Point
PDU Protocol Data Unit

4 System Context

The following general and high-level requirements apply for the present IRP:

A. IRP-related requirements in 3GPP TS 32.101 [1]

B. IRP-related requirements in 3GPP TS 32.102 [2]

C. IRP-related requirements in 3GPP TS 32.600 [4].

Every Interface IRP on the Itf-N interface (e.g. Alarm IRP, Notification IRP, Basic CM IRP, and Bulk CM IRP) is subject to a System Context as described as system context A and context B (3GPP TS 32.150).An NE may be managed via System Context A or B.

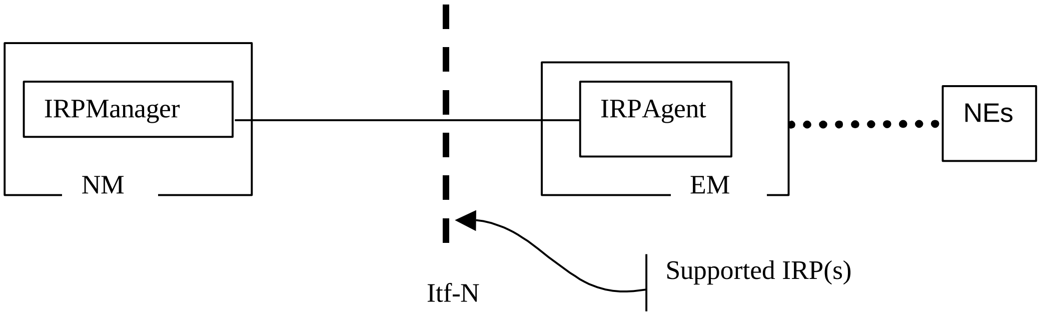

Figure 4.1: System Context A

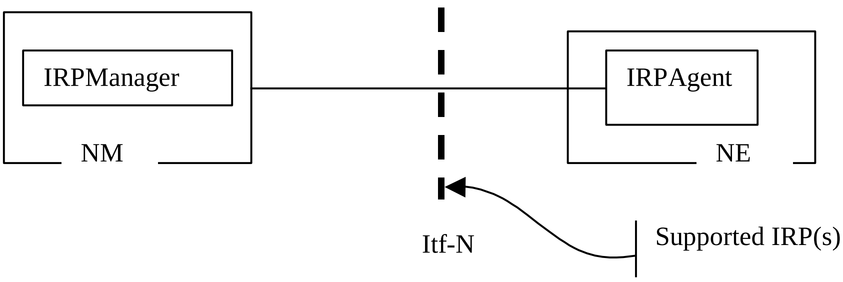

Figure 4.2: System Context B

The following Itf-N performance criteria requirements apply to system context A and or context B. The value definition of the Itf-N performance criteria is outside the scope of this specification.

When the Itf-N performance criteria measurements are being made, it is important that the measurements are measured in exactly the same way. This is important if, for example, an operator is using the Itf-N performance criteria for:

- Vendor selection purposes.
- Detection of `IRPAgent` performance degradation over time.

If these criteria are used for comparison purposes, it is the tester's responsibility to ensure the measurements are made in identical ways for the systems being compared. To achieve statistically reliable results, sufficient number of items should be tested.

Different test environments may have impact on the Itf-N performance test results. For examples of test environment impact, see appendix A.

5 Requirements

5.1 Criteria definition template

Each performance criterion is described using as following template:

a) Concept and description
b) Data type
c) Test method

In any test, it is important to identify two points. One identifies the point, with reference to the context of the system-under-test, at which the test trigger is applied. The other identifies the point where monitoring or measurement is made. We call both these points Measurement Points (MPs).

It is noted that item-c defined above does not describe or specify these MPs since some of these MPs are related to with a particular internal implementations, which are outside the scope of standardization. For example of test MPs, see appendix B.

5.2 Interface IRP data consistency criterion

Data consistency criterion means that data provided over Itf-N shall be consistent with the data stored in the EM without repetition and error. This proposed criterion consists of three criteria . Configuration data consistency, measurement data consistency and alarm data consistency. The defined criteria are only used to evaluate the Itf-N performance not to identify the reason.

5.2.1 IOC instances configuration data consistency criterion

a) NRM IOC instances data consistency criterion means that all the NRM IOC instances' data received by IRP manager over Itf-N (e.g. after one and only one configuration synchronization procedure if necessary) should be consistent with the NRM IOC instances' data stored in EMs and or related NEs. The standardized NRM and vendor extension NRM are in the scope of the tested data.

b) A real value.

c) Compare the NRM IOC instances received over Itf-N with the corresponding IOC instances in the EM and/or related NEs.
Inconsistent IOC attributes within an IOC instance do not lead to inconsistency from this consistency criterion point of view, as long as the IOC instance over Itf-N has the same attribute values as the corresponding EM/NE instance.

IOC instances NRM data consistency=number of tested consistency NRM IOC instances / number of all tested NRM IOC instances *100%.

5.2.2 IOC attributes consistency criterion

a) NRM IOC attribute consistency criterion means all the NRM IOC attributes received over Itf-N by `IRPManager` (e.g. after one and only one configuration synchronization procedure if necessary) should be consistent with the NRM IOC attributes stored in EM and/or related NEs. The standardized NRM attributes and `VSDataContainer` attributes are in the scope of the testing configuration data.

NOTE: Test result in a lab and in a live network maybe different. In a live network, some attributes are dynamical. The Tester needs to prepare appropriate test cases.

b) A real value.

c) IOC attributes data consistency = number of tested consistent IOC attributes / number of all tested NRM IOC attributes.
For this criterion, inconsistent IOC instances are not counted.

5.2.3 Performance Measurement data consistency criterion

a) Performance measurement data consistency criterion means all the measurement data received over Itf-N by `IRPManager` should be consistent with the corresponding measurement data (after calculation if necessary) stored in EM and or related NEs.

b) A real value.

c) Compare the performance measurements value received over Itf-N with the corresponding data in EM and/or related NEs. Usually, tester needs to check the performance measurement result from Itf-N and compare with the original corresponding performance measurements in the EM database and/or related NEs.

Performance data consistency = number of consistency tested performance measurements / number of all tested performance measurements *100%.

5.2.4 Alarm data consistency criterion

a) Alarm data consistency criterion means all the alarm data received by `IRPManager` over Itf-N (after one alarm synchronization procedure if necessary) should be consistent with the alarm data stored in IRP Agent.

b) A real value.

c) Compare the alarm data received over Itf-N with the alarm data stored in IRP Agent Especially, tester should check the additional information parameter defined in `AlarmIRP` to guarantee the related vendor specific alarm type and specific alarm severity are conveyed and keep stable mapping rules to standardized alarm type and alarm severity defined in 3GPP `AlarmIRP`. Otherwise, those alarms shouldn't be tested as inconsistency.

Alarm data consistency = number of tested consistency alarms / number of all tested alarms *100%.

5.3 Interface IRP capacity criteria

5.3.1 Operation response delay criterion

a) Operation response delay criterion means the duration between `IRPManager` invoking an operation via Itf-N and `IRPManager` receiving response of that operation via Itf-N. The operation response delay shall as small as possible. The value of this criterion is based on the specific operation and the data scope involved.

b) An integer value (in milliseconds).

c) Invoke an operation via Itf-N, record the delay of receiving the response over Itf-N.

Operation response delay criterion = (the time of the corresponding response from the Itf-N) - (the time of the invoking tested Itf-N InterfaceIRP operation).

5.3.2 Alarm report delay criterion without filter

a) Alarm report delay criterion means the duration between the alarm eventTime ([5]) and the time alarm that is sent on Itf-N. The `IRPAgent` is recommended to limit the alarm duration time in EM before it is sent out on Itf-N. The intention of this criterion is to test the `AlarmIRP` performance without filter. The method to set Itf-N eventTime by vendors maybe different which may have impact on the test result.

b) An integer value (in milliseconds).

c) Record the time the alarm is sent out on Itf-N and the eventTime included in alarm information ([5]).

Alarm report delay criterion = (the time that alarm is sent out on Itf-N) - (the alarm notification's eventTime).

Note: Depending on where the alarm triggering event time is measured, the measured delay time may include delay inside the EM and thus much more than the Itf-N delay.

5.3.3 Alarm report delay criterion with filter

a) Alarm report delay criterion means the duration between alarm eventTime([5]) and the time that alarm is sent out on Itf-N. The `IRPAgent` is recommended to limit the alarm duration time in EM before it is sent out on Itf-N. The filter set in `AlarmIRP` in the EM may have impact on the performance of `AlarmIRP`. The intention of this criterion is to test the `AlarmIRP` performance with filter.

b) An integer value (in milliseconds).

c) Set alarm filter in `AlarmIRP`.

Record the time the alarm is sent out on Itf-N and the eventTime included in alarm information ([5]).

Alarm report delay criterion= (the time that alarm is sent out on Itf-N)-(the alarm of notification's eventTime).

Note: Depending on where the alarm triggering event time is measured, the measured delay time may include delay inside the EM and thus much more than the Itf-N delay.

5.3.4 Configuration data synchronization delay criterion without filter

a) Configuration data synchronization delay criterion means the maximum time delay for `IRPManager` to synchronize configuration data over Itf-N. The value of this criterion is based on the specific data scope involved. This intention of criteria is to test the interfaceIRP's synchronization capability without filter.

b) An integer value (in milliseconds).

c) Send a synchronization command without filter to `IRPAgent` and receive the synchronized configuration data via Itf-N, record the synchronization procedure time.

5.3.5 Configuration data synchronization delay criterion with filter

a) Configuration data synchronization delay criterion means the maximum time delay for the `IRPManager` to synchronize configuration data through Itf-N. The value of this criterion is based on the specific data scope involved. This intention of criteria is to test the InterfaceIRP's synchronization capability with filter.

b) An integer value (in milliseconds).

c) Send a synchronization command with filter to `IRPAgent` and receive the synchronized configuration data via Itf-N, and then record the synchronization procedure time.

5.3.6 Alarm data synchronization delay criterion without filter

a) Alarm data synchronization delay criterion means the maximum time delay for the `IRPManager` to synchronize current alarm information through Itf-N. This intention of criteria is to test the `AlarmIRP's` synchronization capability without filter.

b) An integer value(in milliseconds).

c) Send an alarm synchronization command to `IRPAgent` and receive the synchronized alarm data via Itf-N, and then record the synchronization procedure time.

5.3.7 Alarm data synchronization delay criterion with filter

a) Alarm data synchronization delay criterion means the maximum time delay for the `IRPManager` to synchronize current alarm information through Itf-N. This intention of criteria is to test the `AlarmIRP's` synchronization capability with filter.

b) An integer value(in milliseconds).

c) Send an alarm synchronization command with filter to IRPAgent and receive the synchronized alarm data over Itf-N, and then record the synchronization procedure time.

5.3.8 Performance measurement data collection delay criterion

a) Performance measurement data collection delay criterion means the duration between the demanded reporting time and actual time when IRPManager receives related performance measurement data via Itf-N.

b) An integer value(in milliseconds).

c) Performance measurement data collection delay = (The time when the performance measurements should be received by IRPManager) - (the time when they are actually received by IRPManager).

5.4 Interface Reliability criteria

5.4.1 Mean Time To Repair (MTTR)

a) Here, MTTR criterion means the mean value of Itf-N fault (when the Itf-N is in an unavailable state) recovery time.

b) An integer value (in milliseconds)

c) The total corrective maintenance time divided by the total number of corrective maintenance actions (i.e. the number of unavailability periods of Itf-N) during a given period of time. (See ATIS definition http://www.atis.org/tg2k/_mean_time_to_repair.html). MTTR = $(T_1+T_2+\ldots+T_k)/k$, where T_i = the time period for a single corrective maintenance action.

5.4.2 Number of supported IRPManagers

a) Number of supported IRPManagers criterion means the maximum number of IRPManager that could access IRPAgent at the same time. It is required that the implemented YyyIRP should have the capability to allow multiple IPPManagers to access Itf-N at the same time.

b) An integer value

c) Determine the number of IRPManagers that can access the IRPAgent at same time.

5.4.3 Mean Time Between Failure (MTBF)

a) MTBF is defined as the average time a component works without failure. MTBF ratings are measured in hours and indicate the sturdiness of the equipment, e.g. hard disk drives and printers.

b) An integer value (in hours).

c) Over a long performance measurement period, the measurement period divided by the number of failures (i.e. the number of unavailability periods of Itf-N) that have occurred during the measurement period. (See ATIS definition http://www.atis.org/tg2k/_mean_time_between_failures.html)

5.4.4 Error data tolerance ability criterion

a) Error data tolerance ability criterion is used to evaluate tolerance ability of Itf-N when it receives the illegal data from the IRPManager. The IRPAgent should recognize the illegal data from IRPManager and give a report or notification. The IRPAgent should not fail due to illegal data from IRPManager.

b) Inapplicable

Send illegal data and check the response and the behaviour of the IRPAgent

Annex A:
Example of Test Environment

Figure A.1 illustrates the typical architecture of an `IRPManager` to `IRPAgent` to NE architectural set up.

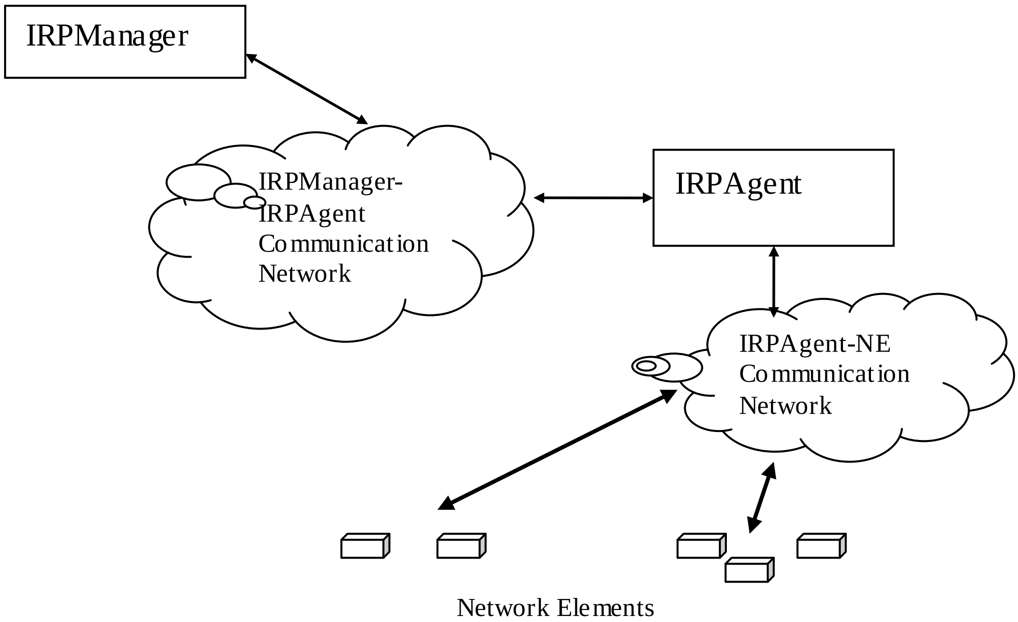

Figure A.1 : Test Environment

Figure A.1 shows two kinds of communication network (i.e. `IRPManager`-`IRPAgent` communication network and `IRPAgent`-NE communications network) and three kinds of system, i.e. Network Management System, Element Management System and Network Elements.

Regarding the communication network, the following are examples of considerations that need to be factored into test criteria.

a) The communications infrastructure between `IRPManager` and `IRPAgent` may have impact on the test result. It is possible for this common infrastructure to be used for other (than testing) purposes, e.g. LANs for additional operator terminals.Possibly other OSSs and management systems are sharing the communications infrastructure i.e. performing tasks unrelated to subject testing.

b) The two communciations infrastructure may be supported by Bridges/routers, some of these may be provided with inbuilt security mechanisms, such as IPSEC, fire-walls, discriminating routers which perform functions based on particular addresses.All of these have an impact on communciations performance throughput, i.e. different communications infrastructures of different security configuration settings will cause test result differences.

c) The performacne of the communications infrastructure, at the time of and for the duration of the tests is also of concern.
Measurements would be invalid if there are a high number of rejected or re attempted PDUs. These errors can be encountered when for example a termination impedence on an ethernet cable is missing or incorrect. The effects may not be noticed when small number of data exchanges occurs with of small message length.The actual "noral" loading of the network is also important as should the utilization of the communcations system, (which uses any form of CSM/CD (Carrier Sense Multiple Access/Collision Detect) mechanism) will experience an almost exponential delivery propagation time when the network load crosses more than 60% utilization. The effects are compounded when a loaded network, starts to experiences errors, which causes the retransmission of protocol data unites. This can cause the network to enter a point of instability.

d) The communications networks may also span long distances using optical or microwave links. The characteristics, e.g. grade of service, of these networks should also be considered, particularly if any aspect is supported by leased lines from 3rd parties.

Regarding the system, the following are examples of considerations that need to be factored into test criteria.

e) Is the system resources used solely for the test?
It is possible for these system resources to be used for other (than testing) purposes, e.g. running system back up tasks. Possibly other OSSs and management applications are sharing the system resources, i.e. performing tasks unrelated to subject testing.

f) The systems may have inbuilt security and reliability mechanisms, such as internal logging of messages, shadowed or mirrored disk. All of these have an impact on system performance throughput, i.e. different systems of different security/reliability configuration settings will cause test result differences.

g) The performacne of the system, at the time of the tests is also of concern. For example, measurements would be invalid if there are a high number of rejected or reattempted disk writes. These errors can be encountered when for example a particular sector of disk is operating at marginal level.

The system may comprise of components connected via various communication technologies (e.g. an inter-processor bus). The characteristics of these communication technologies should also be considered.

Annex B:
Example of Measurement Point

Using a generic system-under-test configuration, the following figure identifies some useful MPs. Vendors can define other relevant MPs for satisfying some test criteria. In those cases, vendor would refine the system-under-test context in order to reveal a new set of MPs not defined here.

It is noted that this specification does not specify how the measurements can be obtained at various MPs. For example, the specification does not specify if a non-intrusive tool (such as use of an external protocol monitor tool) is used at MP-E or if an intrusive tool (such as a program running inside `IRPManager`) to monitor events that occur at MP-E.

Likewise, this specification does not specify how the non-persistent data or persistent data can be viewed/ observed. For example, the specification does not specify if a GUI is installed at MP-F where a human can view the events that occur at MP-F or if a program is installed at MP-F where it logged the events (with proper time-stamps) that occur at MP-F.

Note that the use of persistent data is strictly an implementation issue and may relate to cost and reliability of the system under test and therefore, in general, not a subject of standardization. However, we explicitly define MPs for non-persistent data and for persistent data (see MP-F and MP-G) because measurement results using these MPs can differ significantly.

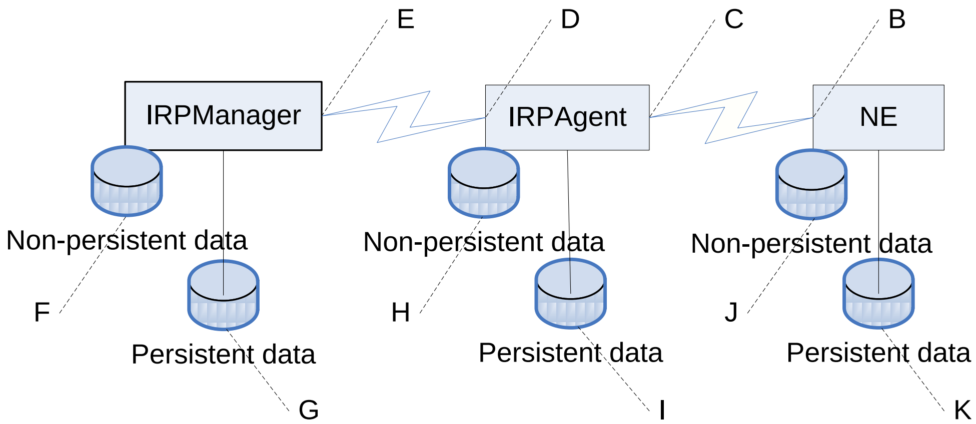

Figure B.1: System-Under-Test context and MPs

Annex C:
Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Cat**	**Old**	**New**
Dec 2006	SA_34	SP-060737	--	--	Submitted to SA#34 for Information	--	1.0.0	
May 2007	SA_36	SP-070291	--	--	Submitted to SA#36 for Approval	--	2.0.0	7.0.0