# ETSI TS 102 675-1 V1.1.1 (2009-11)

*Technical Specification*

## Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Part 1: Performance Management at the SI-SAP

Reference

DTS/SES-00292

Keywords

architecture, broadband, management, multimedia, satellite

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

***Important notice***

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

# Contents

# Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

# Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Satellite Earth Stations and Systems (SES).

The present document is part 1 of a multi-part deliverable covering Performance Management aspects in "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM)", as identified below:

**Part 1: "Performance Management at the SI-SAP";**

Part 2: "Performance Management Information Base".

# Introduction

The BSM Technical Reports [i.1], [i.2] and [i.3] outlined the general requirements for performance in BSM networks; Technical Specifications [1] and [2] have subsequently defined the BSM Management Functional Architecture and the BSM Performance Parameters respectively. Outside ETSI, ITU and IETF (in the IPPM working group) have also defined a large number of richly parameterized metrics and protocols to deal with Performance Management (PM); these parameters and protocols have been taken into account in defining BSM performance parameters ([2] gives references to ITU and IETF metrics), and to define the PM strategies specified in the present document for BSM networks.

As a result, the focus of the present document is on setting a clear framework of PM for BSM networks and on trying to present all M-plane functions and instruments that can be used to manage the defined performance parameters.

# 1 Scope

The present document defines generic Performance Management in BSM networks based on the management architecture given in [1].

The present document provides a framework for the possible Management-plane (M-plane) performance-related strategies, functions, and protocols that can be used to monitor performance parameters in BSM networks.

Performance Management is here understood to be restricted to BSM network performance measurement and monitoring with all associated supporting functions; this is better explained in clause 4.

# 2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

## 2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI TS 102 672: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Management Functional Architecture".

[2] ETSI TS 102 673: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Performance Parameters".

[3] IETF RFC 1213: "Management Information Base for Network Management of TCP/IP-based internets:MIB-II".

[4] IETF RFC 1445: "Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)".

## 2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.


[i.1] ETSI TR 101 984: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Services and architectures".

[i.2] ETSI TR 101 985: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP over Satellite".

[i.3] ETSI TR 102 157: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP Interworking over satellite; Performance, Availability and Quality of Service".

[i.4] ETSI TS 102 292: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; Functional architecture for IP interworking with BSM networks".

[i.5] ETSI TS 102 464: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Interworking with DiffServ Qos".

[i.6] IETF RFC 3289: "Management Information Base for the Differentiated Services Architecture".

[i.7] IETF RFC 3444: "On the Difference between Information Models and Data Models".

[i.8] ITU-T Recommendation M.3400: "TMN management functions".

[i.9] ITU-T Recommendation P.862 (02/2001): "Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs".

[i.10] IETF RFC 2819: "Remote Network Monitoring Management Information Base".

[i.11] IETF RFC 3577: "Introduction to the RMON Family of MIB Modules".

[i.12] IETF RFC 2722: "Traffic Flow Measurement: Architecture".

[i.13] IETF RFC 2720: "Traffic Flow Measurement: Meter MIB".

[i.14] IETF RFC 3917: "Requirements for IP Flow Information Export (IPFIX)".

[i.15] IETF RFC 5101: "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information".

[i.16] RFC 5102: "Information Model for IP Flow Information Export".

[i.17] IETF RFC 5153: "IPFIX Implementation Guidelines".

[i.18] IETF RFC 5470: "Architecture for IP Flow Information Export".

[i.19] IETF RFC 5476: "Packet Sampling (PSAMP) Protocol Specifications".

[i.20] IETF RFC 5477: "Information Model for Packet Sampling Exports".

[i.21] IETF RFC 4656: "A One-way Active Measurement Protocol (OWAMP)".

[i.22] IETF RFC 1229: "Extensions to the generic-interface MIB".

[i.23] IETF RFC 2206: "RSVP Management Information Base using SMIv2".

[i.24] IETF RFC 2213: "Integrated Services Management Information Base using SMIv2".

[i.25] IETF RFC 2214: "Integrated Services Management Information Base Guaranteed Service Extensions using SMIv2".

[i.26] IETF RFC 2863: "The Interfaces Group MIB".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in [1] and the following apply:

**control plane:** this has a layered structure and performs the call control and connection control functions; it deals with the signalling necessary to set up, supervise and release calls and connections

**management plane:** this provides two types of functions, namely layer management and plane management functions:

- **plane management functions:** performs management functions related to a system as a whole and provides co-ordination between all the planes

NOTE: Plane management has no layered structure.

- **layer management functions:** performs management functions (e.g. meta-signalling) relating to resources and parameters residing in its protocol entities

NOTE: Layer Management handles the operation and maintenance (OAM) of information flows specific to the layer concerned.

**MIB:** (also known as a managed object) one of any number of specific characteristics of a managed device

NOTE: MIBs comprise one or more object instances (identified by their OIDs), which are essentially variables.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in [1] and the following apply:

| | |
|---|---|
| B-NMS | BSM Network Management System |
| BSM | Broadband Satellite Multimedia |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| FTP | File Transfer Protocol |
| HTTP | Hypertext Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| ICPIF | Calculated Planning Impairment Factor |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| IPFIX | IP Flow Information Export |
| IPPM | IP Performance Metrics |
| ITU | International Telecommunications Union |
| MIB | Management Information Base |
| MP | Measurement Point |
| MOS | Mean Opinion Score |
| NAP | Network Access Provider |
| OID | Object Identifier |
| OSS | Operations Support System |
| OWAMP | One-Way Active Measurement Protocol |
| PESQ | Perceptual Evaluation of Speech Quality |
| PM | Performance Management |
| QID | Queue IDentifier |
| QoS | Quality of Service |
| RFC | Request For Comments |
| RMON | Remote Network Monitoring |
| RTFM | Realtime Traffic Flow Measurement |
| SLA | Service Level Agreement |
| SNMP | Simple Network Management Protocol |
| SNO | Satellite Network Operator |

| | |
|---|---|
| ST | Satellite Terminal |
| VoIP | Voice over Internet Protocol |

# 4 Objectives of performance management

Network performance management functionalities are shifting from relatively simple availability measurements to those based on detailed Quality-of-Service (QoS) performance assessment. This is because network element availability is generally high and stable, with hardware or software infrastructure failures occurring infrequently, but at the same time increasing variety of traffic (e.g. voice, video and data), and multi-tiered applications have led to an increase in the volume and complexity of network traffic.

Hence network management is moving from the limited perspective of "device-aware" network management to a focus on service delivery - a "service-aware" perspective that is both more comprehensive and more cost-effective. Being service-aware means that it understands the traffic flowing over the network. Once armed with that understanding, traffic flows can be prioritised and devices configured based on the value and priority of the important traffic.

Whereas this is true as well for satellite as for terrestrial networks, normally the satellite link represents, from the performance management point of view, the weak ring in the end-to-end chain; thus one of the key objectives of Performance Management in satellite networks is ultimately to ensure that Service Level Agreements between the satellite service provider (SNO, NAP, etc.) and other service providers are met. Hence the aspects of Performance Management which are of interest to different actors in the network need to be taken into account here.

The objectives of Performance Management can be divided into the following categories (or function set groups according to ITU classification - see [i.8]):

- Performance Quality Assurance.
- Performance Monitoring.
- Performance Management Control.
- Performance Analysis.

These categories will be briefly explained in the following sub-clauses highlighting those which are relevant for the present document. It should be then clear to the reader that the document deals primarily with Performance Monitoring and Performance Analysis (assessment) in BSM networks.

Network performance assessment is, to a greater of lesser extent, included within Performance Monitoring up to the level of monitoring required. Network performance assessment is based on network traffic measurements, which can be performed in two ways:

- with active measurements, which are performed by injecting traffic with known properties into the network; and/or
- with passive measurements, which consist of monitoring the existing traffic flow(s) at one or more measurement points.

Quality of Service (QoS) is one of the main objectives for network services and is often a main constituent of the SLA of a given NAP. QoS is directly related to network performance. QoS measurement or assessment lies logically above network traffic measurements, and relate to the performance of networking applications; they exploit the measurement data to derive quantitative considerations on the "health" of the network:

- Objective QoS relates to something concrete and quantitative (e.g. packet loss, delay, jitter, connection break length, etc.);
- Subjective QoS corresponds to the service quality from the user perspective (Mean Opinion Score (MOS) tests are often used), subjective QoS can be estimated within certain limits from the basis of objective QoS (e.g. PESQ algorithm [i.9]).

In any case the performance parameters to be considered in BSM networks for performance monitoring and assessment are those described in [2]; they refer to layer-3 (IP-layer) parameters and only indirectly, through the BSM SI-SAP parameters (which are generalized representations of specific SD features), to lower-layer parameters.

## 4.1 Performance Quality Assurance

Performance Quality Assurance supports decision processes that establish, according to current state-of-the-art, SLAs, and customer needs, the quality measures that are appropriate for a correct performance management. It concerns setting the alert thresholds, selecting the types of test to perform, the frequency with which to perform tests, etc.

It is up to the BSM network operator how to deal with these decisions and these functions will not be elaborated further in the present document.

## 4.2 Performance Monitoring

Performance Monitoring involves the continuous collection of data from the BSM network elements. The basic function of Performance Monitoring is to track system, network or service activities in order to gather the appropriate data for determining performance of the BSM network.

The operation is designed to measure the overall quality of the network connections, using monitored parameters in order to detect service degradation in a timely way. It may also be designed to detect characteristic patterns of impairment before service quality has dropped below an acceptable level.

These are key operations to be considered when defining the M-plane functions in BSM networks; they will be addressed in clauses 6 and 7.

## 4.3 Performance Management Control

Performance Management Control has two main functional areas: on one side it supports the transfer of information to control the monitoring functions within the network; on the other side it includes the application of traffic controls to guarantee a proper network operation in terms of performance.

For the former area, the Performance Management Control deals, for example, with configuration of measurement schedules, sampling intervals, alert thresholds, and other attributes for monitoring and for test traffic, etc. These are also key operations to be considered when defining the M-plane functions in BSM networks; they will be addressed in clauses 6 and 7. The present document will mainly refer to this set of functionalities as "Performance Monitoring Configuration".

The second functional area (enforcement of traffic control policies) may affect the shaping and/or routing of traffic and the processing of flows. It is very much linked to BSM network operator strategies, so it is considered out of the scope of the present document and it will not be elaborated further in the present document.

## 4.4 Performance Analysis

Performance Analysis processes the measurement data and evaluates the performance level of the network and its elements.

This kind of analysis depends on, and it is in fact derived from, the type of measurement performed. It is up to the BSM network operator how to define the necessary analysis to be applied on the performed measurements and this will not be elaborated in details in the present document. Anyway since performance assessment is necessary up to a certain level and it is part of Performance Analysis some considerations will be given in the clauses 6 and 7.

# 5 Information model for performance management

BSM Performance Management takes into account measurements at the IP-layer and at the SI-SAP interface between the BSM and lower layers. Layer-2 issues and layer-2 Measurement Point s (MPs) will not be considered here; so satellites with On-Board Processing (OBP), as layer-2 MPs, will not be considered in the present document.

Considering the BSM management functional architecture in [1], to simplify the discussion in the present document, it is assumed that every BSM ST implements a standard MIB-II [3] and SNMPv2 agent [4] (or later versions). It is further assumed that two types of database (D/B), $D/B_1$ and $D/B_2$ (see also figure 5.1), will be normally used in BSM networks. $D/B_1$ and $D/B_2$ are understood to be combinations of databases (e.g. MIBs), both standard and proprietary ones, as it will be explained in the following.

The internal format of $D/B_1$ and $D/B_2$ is not relevant for the scope of the present document. The present document is only concerned with the type of information transferred between management functions to populate these databases, or in other words the relationships (associations) between these entities and the roles identified in a BSM network.

$D/B_1$ may contain a newly specified BSM-specific MIB, or MIB modules, as defined in part 2 of this multipart deliverable. Part of these MIB modules are based on the BSM SI-SAP performance parameters defined in [2] and or more basic QID elementary attributes identified in the present document. In addition $D/B_1$ may contain other data structures, e.g. technology or vendor specific ones.

$D/B_2$ may also contain a newly specified BSM-specific MIB, or MIB modules, as defined in part 2 of this multipart deliverable. Most likely this database will be based on the BSM IP performance parameters defined in [2]. In addition $D/B_2$ may contain other data structures, at wish of the BSM network operator. $D/B_2$ is in fact the interface between the BSM-internal and external worlds; it will most likely be a combination of data elements or data structures (some standard ones, some proprietary ones, and some BSM-specific ones, as defined in part 2 of this multipart deliverable).

Visibility (read/write access rights) of the databases should be regulated by the BSM network operator; e.g. $D/B_2$ may or may not be made visible to external parties. In any case it should be noted that for specific data elements it may not be possible to prevent external parties from directly polling $D/B_1$.

The set of element management data specified in part 2 of this multipart deliverable may be in the future formally standardized as MIBs; in this case they should be provided by all BSM-compliant systems, so they will thus be accessed by means of standard SNMP through the NMC (see figure 5.1). So service and network performance considerations can be derived from it by aggregation and/or other types of analysis.

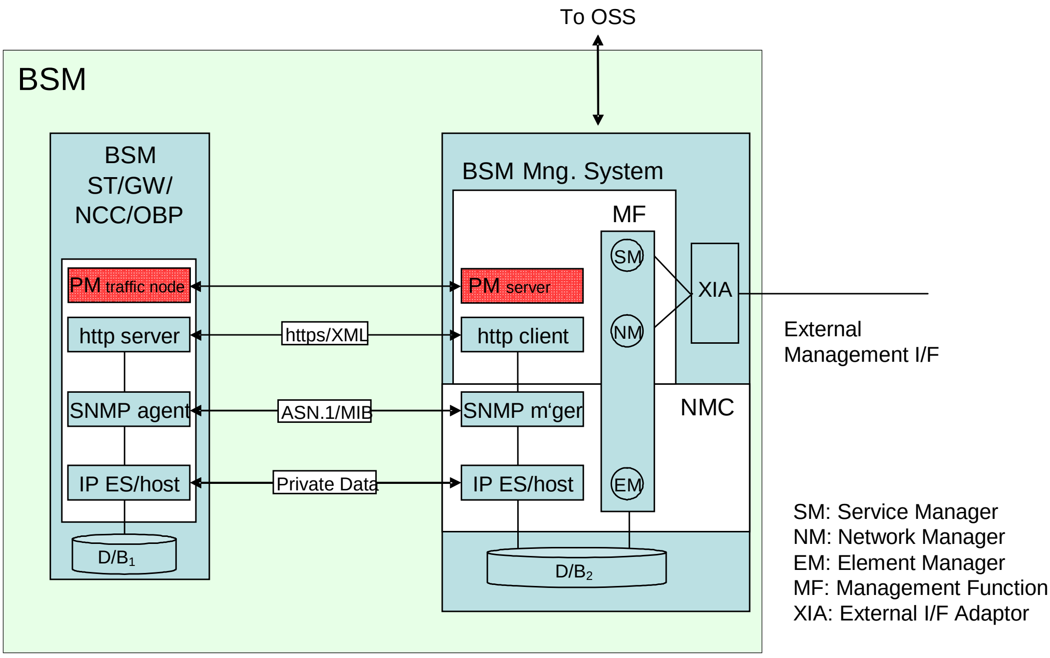


**Figure 5.1: BSM Management Functional Architecture**

The BSM network should also foresee a central PM server which accomplishes its tasks interacting with PM modules (or PM traffic nodes) located in the Satellite Terminals (STs). The server is responsible for selecting measurements to be performed, configuring the PM nodes to perform them, for collecting the data, and for the final performance assessment. The PM server may or may not be involved in the measurement as it is shown in figure 5.2. This centralized architecture, where a central server is responsible for the PM in the network, seems quite suitable to a satellite network.

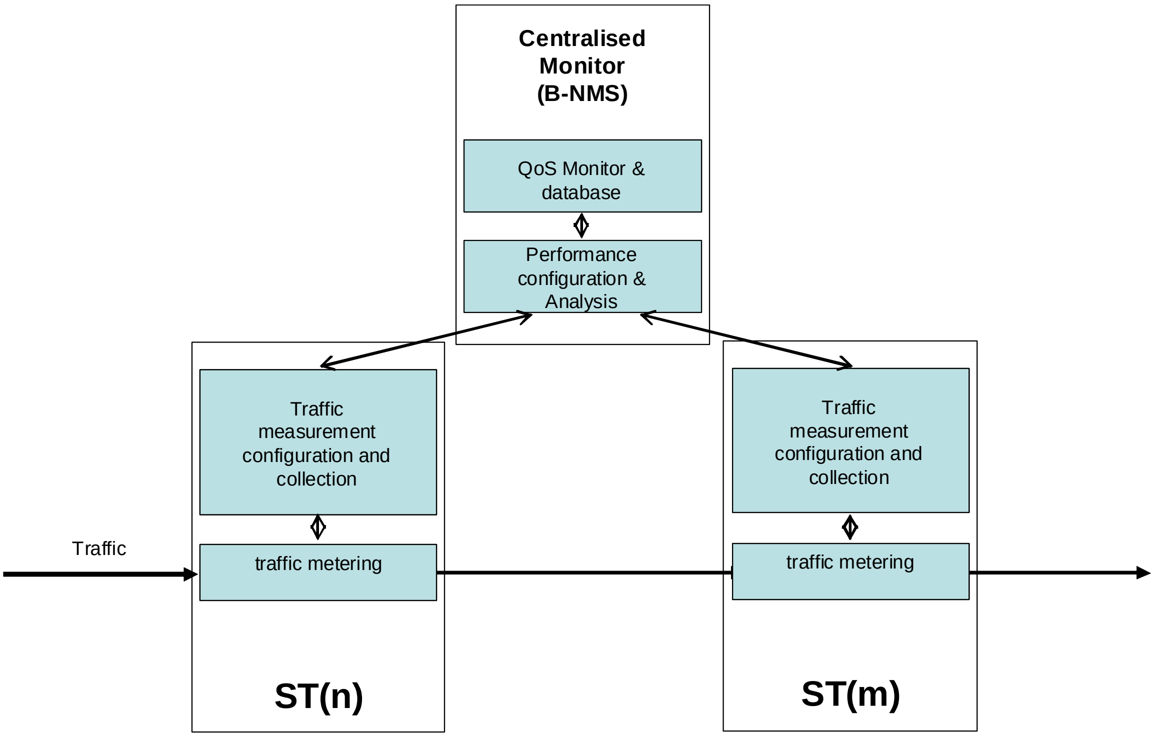


**Figure 5.2: Simplified BSM architecture for performance measurements**

# 6 Hierarchy (actors and roles)

## 6.1 Performance Management Operations

The architecture presented in the previous clause can be considered a centralized architecture, as there is a central PM server, located in the BSM Network Management System (B-NMS), and a number of managed network elements, the PM traffic nodes, located in the STs. So there are two types of entities in a PM BSM architecture, and thus two PM roles. For both of these roles the following four PM operations can be clearly identified:

- selection of the measurements to be performed;
- configuration of the PM nodes which perform them;
- measurements execution and collection of the data;
- final performance assessment.

They will be detailed clause 6.2.

## 6.2 PM Roles

The four operations listed above include a series of sub-tasks which should be performed by different entities in the network (either by the PM server, or by the PM traffic nodes, or by both). In this clause we distribute these tasks to the different PM roles in the network and describe the details.

### 6.2.1 PM traffic node (ST)

The following activities may be performed by the PM traffic node (ST) in the four operation areas identified above:

- **Selection of the measurements to be performed:** the ST should decide to perform selected measurements independently only if this is required to populate local databases, or in order to fulfil requirements given by the central PM server (e.g. keep a given parameter up-to-date).
- **Configuration of the PM nodes which perform measurements:** the PM traffic node may be pre-configured with test applications, or may be completely configurable from remote (e.g. by RMON, [i.10]), both these options are possible either for active and for passive measurements.
- **Measurements execution and collection of the data:** normally the ST will populate the database $D/B_1$ with the results of the performed measurements. The ST is involved in the measurement of parameters when (or collection of measurement data):
    - it is the only MP for the parameter, so the parameter is measured locally (e.g. number of active QIDs, see [2]);
    - it is involved in a measurement which takes place between multiple MPs, typically one-way measurements (e.g. one-way delay by means of OWAMP, [i.21]);
    - it is exporting data, which are collected by some other entities in the network, if, for example, IPFIX is used, the ST will run an IPFIX exporter.
- **Final performance assessment:** not relevant for a PM traffic node.

### 6.2.2 PM server (B-NMS)

The following activities may be performed by the central PM server in the four operation areas identified above:

- **Selection of the measurements to be performed:** the PM server selects the metrics to be measured, i.e. the *singleton metrics* (in IETF ippm terminology); it also decides the domain of measurement and the way of sampling metrics:
    - E.g. which STs? Which applications? Which network sections? Observation time, sampling period, etc.;
    - Decides how to derive the *sample metrics* (in IETF ippm terminology).
- **Configuration of the PM nodes which perform measurements:** the PM server takes care of configuring the PM traffic nodes to instruct them on how to measure parameters, either for passive monitoring or for active measurements; if a pre-processing has to be done at the ST (i.e. on some *sample metrics* to derive *statistical metrics*, in IETF ippm terminology) this is also configured by the PM server.
- **Measurements execution and collection of the data:** normally the PM server records the results of measurements (the *sample metrics* in IETF ippm terminology), it processes the collected data for some statistics (the *statistical metrics* in IETF ippm terminology), and writes them in the database $D/B_2$. It is also involved in the measurement of parameters when (or collection of measurement data):
    - it is involved in a measurement which takes place between multiple MPs, typically one-way measurements (e.g. one-way delay by means of OWAMP, [i.21]); it may be frequent to involve the PM server in one-way measurements;
    - it is collecting data, which are exported by some other entities in the network (i.e. the PM traffic nodes), if, for example, IPFIX is used, the PM Server will run an IPFIX collector (see clause 7.2.1.3 and the figure therein).
- **Final performance assessment:** The PM performs all the relevant analysis on the collected data to derive statistics and/or general considerations on the overall network performance, and calculation of SLA compliance; if needed, it also performs some kind of pre-processing before writing the outcomes of this analysis onto the database.

# 7 Management of BSM performance parameters

## 7.1 BSM SI-SAP Performance Parameters

As already mentioned, database $D/B_1$ may be mostly based (even if not only) on the BSM SI-SAP Performance Parameters defined in [2].

The BSM SI-SAP Performance Parameters have the following characteristics:

- They are BSM specific: They are associated to properties of the SI-SAP and in particular they describe specific QIDs features, so they can be defined only for STs which implement the SI-SAP.
- They represent instantaneous values (like MIB parameters) and thus there is no need to track past parameter values to compute one of these metrics.
- They can be measured at each SI-SAP in a BSM network, as a single point of measurement, i.e. at each ST or gateway without involvement of external entities to support the measurement procedure (see [2] for more details).
- They can be stored at each ST (where an SI-SAP is located) quite simply, by just measuring and immediate storing the result of the measurement.

The present document defines performance management in a flexible way so that it can be implemented with a minimum overhead requirement. In particular the latter three properties show that the monitoring of these parameters is quite simple and does not add big complexity in the STs. In addition this shows that the BSM SI-SAP Performance Parameters can be easily mapped to a MIB and be remotely retrieved by means of SNMP.

An ST with sufficient processing power may also generate statistics or tracking of selected parameters over time, as well as other types of processing/aggregation of QID parameters. If the ST is capable of pre-processing, this should be known to the B-NMS in advance in order to enable an efficient exchange of information, and avoid duplicating effort (at the B-NMS there is no need of averaging multiple metrics retrieved from the ST, if an average was already performed at the ST and the average value was transmitted). Pre-processing and statistics can be performed either over time or over multiple QIDs for a given point in time, or over both time and QIDs, as it is shown in the three following examples, which represent the three cases respectively:

1) Average number of open QIDs in the last hour.

2) Average Slack Term *S* over QIDs 1 to 5.

3) Average QID Rate *R* over the last hour for QIDs 6 to 10.

Given the very high number of possible combinations, by pre-calculating statistics of the basic BSM SI-SAP performance parameters, many new "pre-processed" parameters can be created. These special parameters coming from pre-processing and statistics are not standardized in the present document, implementers and operators are left free to define the ones best suited to their management objectives.

### 7.1.1 Retrieving BSM SI-SAP Performance Parameters

Some of the parameters have only meaning locally to the ST, and for this reason a remote server (the B-NMS) has to follow a clear procedure to retrieve them from an ST, in order to guarantee a proper system operation. In particular the QID labels (or simply QIDs) are not sent over the air, and normally the QID value is not known to the B-NMS. So in order to refer to (or to ask for) a specific parameter referred to a certain QID, the B-NMS has first to ask for the QID label.

As described in [2], the BSM SI-SAP performance parameters can be divided in two classes: the SI-SAP-level ones and the QID-level ones. The former ones have generally meaning for each ST, or for each BSM_ID, as they are defined only if the SI-SAP exists, the latter ones have only meaning inside the ST, as they refer to QIDs and to local resources. For this reason the former ones can be directly retrieved by the BSM network (i.e. the B-NMS) by simply addressing the ST; on the other hand in order to retrieve the latter ones the BSM network needs to know the QID they are referred to. So if the B-NMS is trying to get QID-level parameters, it should first retrieve from the ST the list of active QIDs; once the B-NMS is aware of the QIDs available at an ST, it can ask for transmission of the specific QID-level parameter(s). This procedure is depicted in figure 7.1.

From the figure it appears that it may not be easy to understand whether the QID label available at the B-NMS is up-to-date or not: QIDs may change at the ST, be released and be created in the timeframe of minutes, hours, or days. This timeframe may vary depending on the way the BSM network is managed, so the B-NMS should ask for updates of the QIDs list according to these network characteristics. It may be also useful to piggyback the request for a QIDs list update when the B-NMS is asking for other parameters, in order to have at the B-NMS information on the QID list as up-to-date as possible.

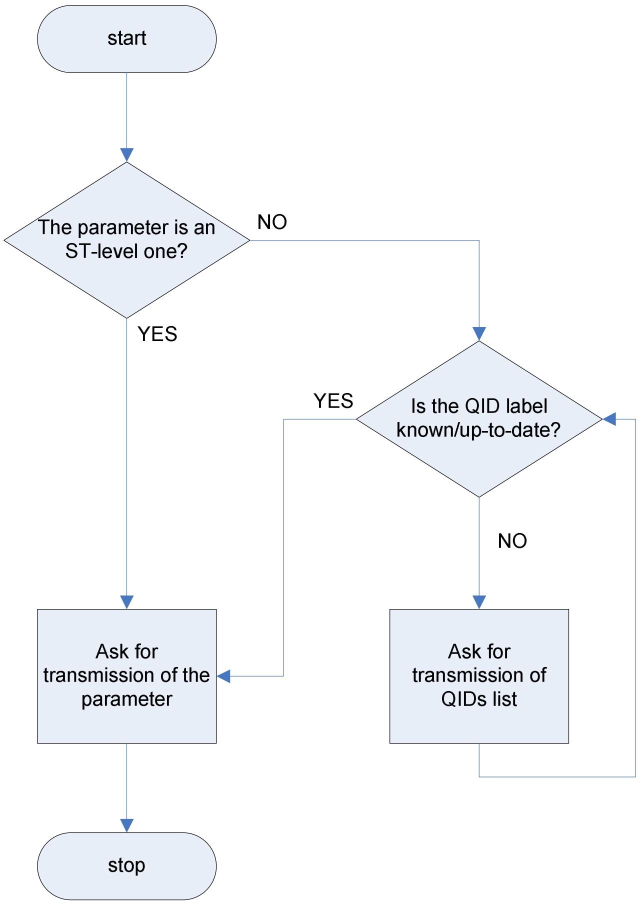


**Figure 7.1: Flow-chart of the BSM SI-SAP performance parameters retrieval procedure at the B-NMS**

## 7.1.2 Calculating BSM SI-SAP Performance Parameters

In this clause clear indications are given on how to calculate BSM SI-SAP Performance Parameters.

### 7.1.2.1 QID-level Performance Parameters

Most of the QID-level parameters described in [2] can be extracted directly from measurements on the QIDs or should be known to the ST by other means, e.g. through other local MIBs or by some intrinsic knowledge. In [2] it is also described how to derive most of these parameters. Where they cannot be measured or extracted directly, a set of QID elementary attributes can be used to derive these SI-SAP parameters. In the present clause the derivation of all SI-SAP QID-level performance parameters is given and the list of the associated QID elementary attributes is derived.

#### 7.1.2.1.1 List of IP flows associated to a QID [IP(QID$_i$)] and List of SD queues associated to a QID [SD(QID$_i$)]

The List of SD queues associated to a QID [SD(QID$_i$)] is a list of SD labels, or technology- and system-dependent codes, which should be known to the NCC, but may not be known to the B-NMS. So the B-NMS may have to communicate with the NCC to interpret these parameters data; this is assumed to be feasible without need of further interface specification in the present document.

On the other hand the List of IP flows associated to a QID [IP(QID$_i$)] may present a set of labels and handles which have only meaning locally to the ST. A way to handle these object is to use existing IETF MIBs, as described in annex B.

Alternatively it might be helpful to specify a set of labels to represent possible IP queues, which should be used in the place of this IP(QID$_i$) list, as explained in the following:

- a label for each DiffServ queue, e.g. according to the DiffServ Code Points (DSCPs) recommended by IETF, as summarized in tables 7.1 and 7.2 (taken from [i.5]);
- separate labels for each IntServ queue.

**Table 7.1: Summary of DiffServ Code Points (DSCPs)**

| | PHBs | DSCPs | | | No. |
|---|---|---|---|---|---|
| **IANA assigned** | BE | 000 | 00 | 0 | 1 |
| | CS | 001-111 | 00 | 0 | 7 |
| | AF | 001-100 | 01-11 | 0 | 12 |
| | EF | 101 | 11 | 0 | 1 |
| **Not assigned** | | 000 | 01-11 | 0 | 3 |
| | | 101 | 01-10 | 0 | 2 |
| | | 110-111 | 01-11 | 0 | 6 |
| **EXP/LU (see note)** | | xxx | x1 | 1 | 16 |
| **EXP/LU (see note)** | | xxx | x0 | 1 | 16 |
| **Total:** | | | | | 64 |
| NOTE: Initially available for experimental or local use, but may be used for future standards action allocations as necessary. | | | | | |

**Table 7.2: Summary of Assured Forwarding DSCPs**

| | AF1x | AF2x | AF3x | AF4x |
|---|---|---|---|---|
| **Low drop precedence (AFx1)** | 001010 | 010010 | 011010 | 100010 |
| **Medium drop precedence (AFx2)** | 001100 | 010100 | 011100 | 100100 |
| **High drop precedence (AFx3)** | 001110 | 010110 | 011110 | 100110 |

No further elementary QID attributes are needed for these SI-SAP parameters.

#### 7.1.2.1.2 Time from [$t_{mod}$] and type of [$m_{QID}$] last QID modification

These two parameters can be derived as described in [2].

No further elementary QID attributes are needed to derive these SI-SAP parameters.

#### 7.1.2.1.3 Transmission Delay [$D_T$]

This parameter can be derived as described in [2]. It may also be that this parameter is known to the ST through other MIBs.

No further elementary QID attributes are needed to derive this SI-SAP parameter.

#### 7.1.2.1.4 Maximum Hardware Delay [$D_{hw}$]

As described in [2], this parameter should be known to the ST, and thus no further elementary QID attributes are needed to derive this SI-SAP parameter.

#### 7.1.2.1.5 Rate [*R*]

This parameter represents the QID service rate, i.e. the total number of bytes of IP datagrams (including headers) transmitted over the satellite interface for a given QID divided by the time interval duration (or equivalently, the number of bytes of IP datagrams transmitted for a given QID per second). In order to calculate it, it is necessary to know the number of bytes transmitted over satellite on a given QID. This can be done by implementing an "octets counter", i.e. a counter which is incremented every time IP packets are sent from the relevant QID. If this counter is named *QidOctetsCounter*, then *R* can be derived as follows:

$$R_T(t_0) = \frac{QidOctetsCounter_{t=T+t_0} - QidOctetsCounter_{t=t_0}}{T}.$$

If a packet counter *QidPktsCounter* is also implemented for each QID, some other statistics may be derived, like the average packet service rate of the QID, i.e. the number of IP datagrams transmitted for a given QID per second over a time window *T* (this is useful if for example the size of the transmitted packet is constant):

$$R_{\mathrm{pkts},T}(t_0) = \frac{QidPktsCounter_{t=T+t_0} - QidPktsCounter_{t=t_0}}{T}.$$

The following two QID elementary attributes are useful to compute the Rate parameter:

- QID octets counter [*QidOctetsCounter*] (counter);
- QID packets counter [*QidPktsCounter*] (counter).

#### 7.1.2.1.6 Slack Term [*S*]

The slack term *S* defines the packet queuing delay associated with a QID, i.e. the time the packet spends in the ST at the outgoing satellite interface waiting for being selected for transmission over a given QID. It is possible to estimate this average queuing delay for a given QID by knowing the queue length at a given time and the QID service rate. Actually we could also define $S_{\mathrm{bytes}}$ as the average queuing delay per byte associated with a QID.

If we let *QidQPktsLen* be the QID queue length in number of packets, and let $R_{\mathrm{pkt}}$ be the average packet service rate of the QID (as calculated in previous clause 7.1.2.1.5), then *S* can be estimated as follows:

$$S(t_0) = \frac{QidQPktsLen_{t=t_0}}{R_{\mathrm{pkts}}(t_0)}.$$

Equivalently, being *QidQOctetsLen* the QID queue length in number of bytes of IP datagrams, and *R* the service rate of the QID (as calculated in previous clause 7.1.2.1.5), $S_{\mathrm{bytes}}$ can be estimated as follows:

$$S_{\mathrm{bytes}}(t_0) = \frac{QidQOctetsLen_{t=t_0}}{R(t_0)}.$$

The following two QID elementary attributes are useful to compute the Slack Term parameter:

- QID queue length in packets [*QidQPktsLen*] (32 bit integer);
- QID queue length in octets [*QidQOctetsLen*] (32 bit integer).

#### 7.1.2.1.7 Traffic Pattern [*r*, *b*, *p*, *m*, *M*]

If the traffic going through the QID is metered by a token bucket model, the parameters of the token bucket shaper adopted can be used to derive the set of values for *r, b, p, m,* and *M* (e.g. by means of a DiffServ MIB, ). In case the traffic is not metered at the transmitting QID, a token bucket model, which bounds the transmitted traffic, may be in any case computed. In this case the following QID elementary attributes may be needed:

- QID octets counter [*QidOctetsCounter*] (counter), this is needed to estimate the parameters *r, b* and *p* of the Traffic Pattern;
- QID queue length [*QidOutQLen*] (32 bit integer), this is needed jointly with *QidOctetsCounter* to estimate the parameters *r*, *b* and *p* of the Traffic Pattern;
- Minimum-size IP packet transmitted [*QidMinPktSize*] (32 bit integer), measured in bytes of IP packet including header, this is needed to estimate the parameter *m* of the Traffic Pattern;
- Maximum-size IP packet transmitted [*QidMaxPktSize*] (32 bit integer), measured in bytes of IP packet including header, this is needed to estimate the parameter *M* of the Traffic Pattern.

### 7.1.2.2 SI-SAP-level Performance Parameters

Most of the SI-SAP-level parameters described in [2] can be extracted directly from measurements on the QIDs or from the QID-level ones. In the present clause the derivation of all these SI-SAP-level performance parameters is given and the list of the associated QID elementary attributes is also derived.

#### 7.1.2.2.1 Number of active QIDs [$N_{QID}$]

This parameter can be derived as described in [2], and thus no further elementary QID attributes are needed to derive this SI-SAP parameter.

#### 7.1.2.2.2 List of QIDs [$QID_i$]

This parameter can be derived as described in [2], by just monitoring the QIDs currently active in the ST.

No further elementary QID attributes are needed to derive this SI-SAP parameter.

#### 7.1.2.2.3 Available Data Rate [$R_{ava}$]

As described [2], this parameter can be derived from the service Rates of all QIDs (see previous clause 7.1.2.1.5) and from the maximum data rate available to each ST for resource allocation, $R_{max}$; all this information should be known to the ST, and thus no further elementary QID attributes are needed to derive this SI-SAP parameter.

#### 7.1.2.2.4 All-QIDs Transmission Delay [$D_T$]

As described [2], this parameter can be derived from the QID-level values of Transmission Delays, and thus no further elementary QID attributes are needed to derive this SI-SAP parameter.

#### 7.1.2.2.5 All-QIDs Maximum Hardware Delay [$D_{hw}$]

As described [2], this parameter can be derived from the QID-level values of the Maximum Hardware Delays, and thus no further elementary QID attributes are needed to derive this SI-SAP parameter.

#### 7.1.2.2.6 All-QIDs Rate [*R*]

As described [2], this parameter can be derived from the service Rates of all QIDs (see clause 7.1.2.1.5), and thus no further elementary QID attributes are needed to derive this SI-SAP parameter.

#### 7.1.2.2.7 All-QIDs Slack Term [*S*]

As described [2], this parameter can be derived from the QID-level values of the Slack Terms, and thus no further elementary QID attributes are needed to derive this SI-SAP parameter.

#### 7.1.2.3 Summary of QID Elementary Attributes

In summary, as shown in clauses 7.1.2.1 and 7.1.2.2, in order to compute the BSM SI-SAP performance parameters, the following QID elementary attributes are needed at the ST for each QID:

- QID transmitted octets counter [*QidOctetsCounter*] (counter);
- QID transmitted packets counter [*QidPktsCounter*] (counter);
- QID queue length in packets [*QidQPktsLen*] (32 bit integer);
- QID queue length in bytes [*QidQOctetsLen*] (32 bit integer);
- Minimum-size IP packet transmitted [*QidMinPktSize*] (32 bit integer), measured as gauge in bytes of IP packet including header, this is needed to estimate the parameter *m* of the Traffic Pattern;
- Maximum-size IP packet transmitted [*QidMaxPktSize*] (32 bit integer), measured in bytes of IP packet including header, this is needed to estimate the parameter *M* of the Traffic Pattern.

## 7.2 BSM IP performance parameters

As already mentioned, database $D/B_2$ is based on the BSM IP Performance Parameters defined in [2] and recalled in figure 7.2.

The BSM IP Performance Parameters have the following characteristics:

- They were defined considering ITU and IETF IP metrics and thus they are not BSM specific: They are associated to properties of the IP services running on an ST or on a link between two STs.
- They represent instantaneous values, but they become much more useful and meaningful when considered over a time window; thus there is normally a need to track past metric values and to make some kind of (simple) computations when considering these parameters (this will be discussed later in this clause).
- Normally they cannot be measured at a single ST (apart from a few cases, which will be discussed later in this clause), but involve two MPs to be computed.
- Some of them can be stored locally at each ST, some of them are more meaningfully stored in a central PM server (also considering that they cannot be measured locally, but only between two MPs and normally the PM server will be one of the MPs).

Differently from the BSM SI-SAP performance parameters, the latter three properties show that the monitoring of these BSM IP performance parameters cannot be univocally specified. In particular:

- Some of them can be measured locally to the PM traffic nodes (the STs), and some need to be measured between two nodes.
- For some of them it is more meaningful to store them locally, for some of them central storing in the B-NMS is more meaningful and, in some cases, forced, because the measurement only results from processing some data collected at the PM server.

So, for the sake of simplicity, it makes sense to store locally the parameters that can also be measured locally, and to store in the PM server (in the B-NMS) the ones which are measured between two MPs. Figure 7.2 shows this distinction between the two groups of BSM IP performance parameters. Further details about this and on how to measure and store them will be given in clauses 7.2.1 and 7.2.2.

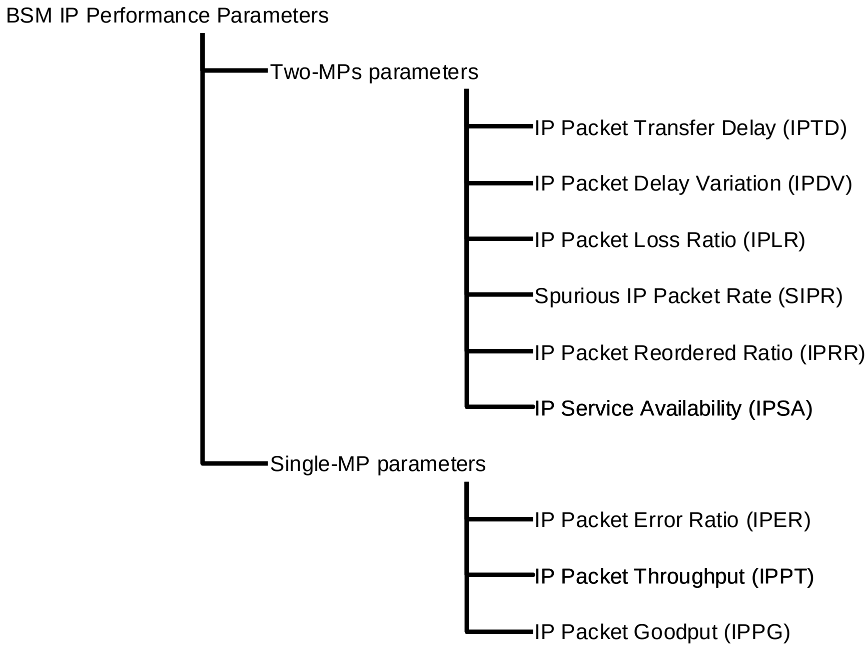


**Figure 7.2: BSM IP Performance Parameters with distinction between parameters with single MP, to be stored in the PM traffic node, and parameters to be measured between two MPs, to be stored in the B-NMS**

### 7.2.1 Tools for Measuring BSM IP performance parameters

Several IETF protocols and architectures have been defined for IP performance parameter collection, such as RMON, RTFM, IPFIX, PSAMP, OWAMP as described below. These techniques can also be used for the BSM IP performance parameters, of course. The present clause describes how these existing IETF protocols should be used in a BSM network.

It is worth mentioning that measuring IP parameters implies some form of sampling, namely selection of the packets to be considered relevant for the measurement, in other words the selection of the population of interest. Sampling of IP performance parameters can be done at different levels:

- Services running in a ST (e.g. QoS classes, types of protocols, destination/source addresses and ports).
- Time: sampling (e.g. Poisson), frequency (e.g. once per minute, or once per day), and duration (start/stop, e.g. constantly, or over limited time windows).
- STs in the network (e.g. all STs or selected groups of STs).
- Links (e.g. uplink, downlink, selected beams).

The selection of these "sampling conditions" is crucial for an overall network-level performance assessment and for this reason it is left to the BSM network operator. The present document is not meant to constraint the selection of these sampling conditions, but it should be noted that these sampling conditions should be clear when measuring, storing and when presenting the BSM IP performance parameters; for this reason this point is further clarified in clause 7.2.2 for each parameter.

#### 7.2.1.1 RMON

The IETF RMON [i.10] concept is designed for more advanced monitoring over a network (compared with basic SNMP which is used more for "device-based" management i.e. go/no-go). Intelligent monitoring functions installed in network equipment (i.e. RMON "probes") consist of RMON software agents which collect information and may then also aggregate and analyse this information e.g. on packets in data flows. A probe places its results in an RMON-associated MIB which can then be accessed by a remote SNMP manager, hence using a "pull" model. The probes can measure and analyse parameters at several protocol layers, from data link to application layers.

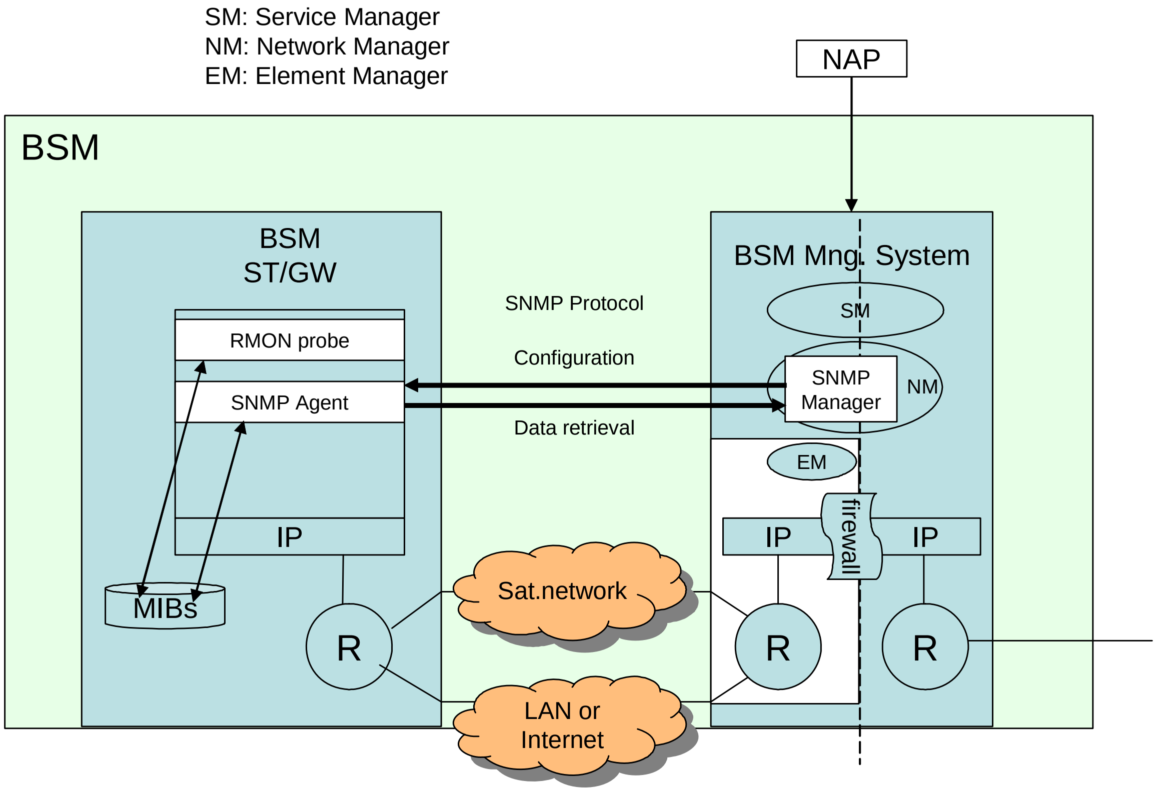


**Figure 7.3: BSM RMON Architecture**

Although RMON agent configuration and data collection use SNMP, RMON is designed to operate differently than other SNMP-based systems. In RMON, agents in network elements shoulder more of the management burden, and thus require more resources. For this reason devices sometimes implement only a subset of the RMON MIB groups e.g. only statistics, history, alarms, and events. The capabilities and configuration of probes are controlled and monitored by reading and writing to OIDs in each of the MIBs.

IETF MIBs [i.11] defined for RMON, in addition to the RMON-1 and RMON-2 MIBs, and relevant to BSM, include the following:

- Remote Network Monitoring MIB Extensions for Switched Networks (SMON MIB).
- RMON MIB Extensions for Interface Parameters Monitoring (IFTOPN).
- RMON Extensions for Differentiated Services (DSMON MIB).
- RMON for High Capacity Networks (HCRMON MIB).
- Application Performance Measurement MIB (APM MIB).
- Transport Performance Metrics MIB (TPM MIB).
- Synthetic Sources for Performance Monitoring MIB (SSPM MIB).
- RMON MIB Extensions for High Capacity Alarms.
- Real-Time Application Quality of Service Monitoring (RAQMON) MIB.

Note that the SSPM MIB covers the artificial generation of a) application-level, b) transport- level, and c) link-level traffic for the purpose of monitoring system performance. The SSPM MIB provides the ability to configure and control the generation of this synthetic traffic.

The RMON-1 OIDs are aimed at link-layer parameters while RMON-2 OIDs extend these to higher layers. The parameters treated are, for RMON-1:

1) Statistics: real-time LAN statistics e.g. utilization, collisions, CRC errors.
2) History: history of selected statistics.
3) Alarm: definitions for RMON SNMP traps to be sent when statistics exceed defined thresholds.
4) Hosts: host specific LAN statistics e.g. bytes sent/received, frames sent/received.
5) Hosts top N: record of N most active connections over a given time period.
6) Matrix: the sent-received traffic matrix between systems.
7) Filter: defines packet data patterns of interest e.g. MAC address or TCP port.
8) Capture: collect and forward packets matching the Filter.
9) Event: send alerts (SNMP traps) for the Alarm group.
10) Token Ring: extensions specific to Token Ring.

For RMON-2:

1) Protocol Directory: list of protocols the probe can monitor.
2) Protocol Distribution: traffic statistics for each protocol.
3) Address Map: maps network-layer (IP) to MAC-layer addresses.
4) Network-Layer Host: layer 3 traffic statistics, per each host.
5) Network-Layer Matrix: layer 3 traffic statistics, per source/destination pairs of hosts.
6) Application-Layer Host: traffic statistics by application protocol, per host.
7) Application-Layer Matrix: traffic statistics by application protocol, per source/destination pairs of hosts.
8) User History: periodic samples of user-specified variables.
9) Probe Configuration: remote configuration of probes.
10) RMON Conformance: requirements for RMON2 MIB conformance.

#### 7.2.1.2 RTFM

The Realtime Traffic Flow Measurement (RTFM) architecture [i.12] provides a general framework for describing and measuring network traffic flows. Flows are defined in terms of their Address Attribute values and measured by a "Traffic Meter".

RTFM defines flows as bidirectional (unlike e.g. IPFIX). An RTFM meter matches packets from B to A and A to B as separate parts of a single Flow, and it maintains two sets of packet and byte counters, one for each direction.

An RTFM meter reader "pulls" data from a meter by using SNMP. Remote configuration is the only way to configure a meter. This is done by using SNMP and a specific Meter MIB [i.13].

#### 7.2.1.3 IPFIX

IPFIX ([i.15] to [i.18]) is aimed specifically at measuring and sending IP flow records over a network. This is done by metering in network elements (in this case STs) and the subsequent information export by devices installed in them. IPFIX devices export data using the IPFIX protocol. The devices employ a "push" model, and decide when and whether to export an expired Flow, or for long-lasting flows the Exporting Process should export the Flow Records on a regular basis or based on some export policy. An IPFIX Exporting Process is configured to export records to a specified list of IPFIX Collecting Processes.

An IPFIX collector would typically be installed in the B-NMS and would be responsible for correlation of flow records.

IPFIX defines Information Elements (rather than a MIB) for describing unidirectional flow properties.

IPFIX does not provide for remote configuration of an IPFIX device, and so implementers must provide their own way to do this, e.g. one could consider extending the PSAMP MIB to also allow configuration of IPFIX processes (see clause 7.2.1.4).

Some performance metrics require the correlation of data from multiple observation points (e.g. Delay). For this, the clocks of the involved metering processes must be synchronised. Furthermore, the collector must recognise that the same packet was observed at different observation points.

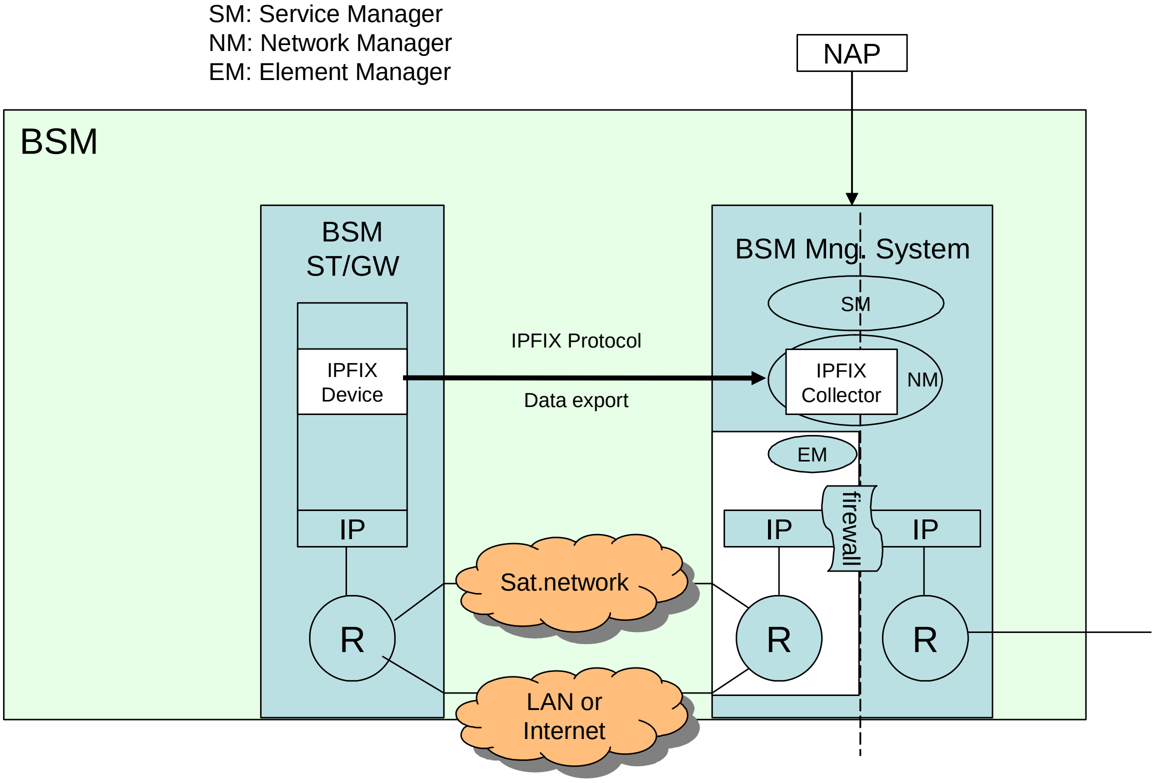


**Figure 7.4: BSM IPFIX-based parameter collection Architecture**

## 7.2.1.4 PSAMP

The Packet Sampling (PSAMP) Protocol [i.19] defines packet selection methods, their configuration at probes, and the reporting of packet information. PSAMP uses IPFIX as a basis for exporting packet information. [i.20] describes further Information Elements for exporting packet information and reporting configuration information.

The main difference between IPFIX and PSAMP is that IPFIX addresses the export of Flow Records, whereas PSAMP addresses the export of packet records. Furthermore, PSAMP explicitly addresses remote configuration and defines a MIB for the configuration of packet selection processes.

NOTE: At the time the present document is being written; the PSAMP MIB is under preparation in the IPFIX IETF working group.

## 7.2.1.5 OWAMP

The One-Way Active Measurement Protocol (OWAMP) [i.21] measures unidirectional characteristics such as one-way delay and one-way loss. High-precision measurement of these one-way IP performance metrics became possible with wider availability of good time sources (such as GPS and CDMA). OWAMP enables the interoperability of these measurements.

The OWAMP specification consists of two inter-related protocols: OWAMP-Control and OWAMP-Test. OWAMP-Control is used to initiate, start, and stop test sessions and to fetch their results, whereas OWAMP-Test is used to exchange test packets between two measurement nodes.

OWAMP generates test traffic as a stream of UDP packets.

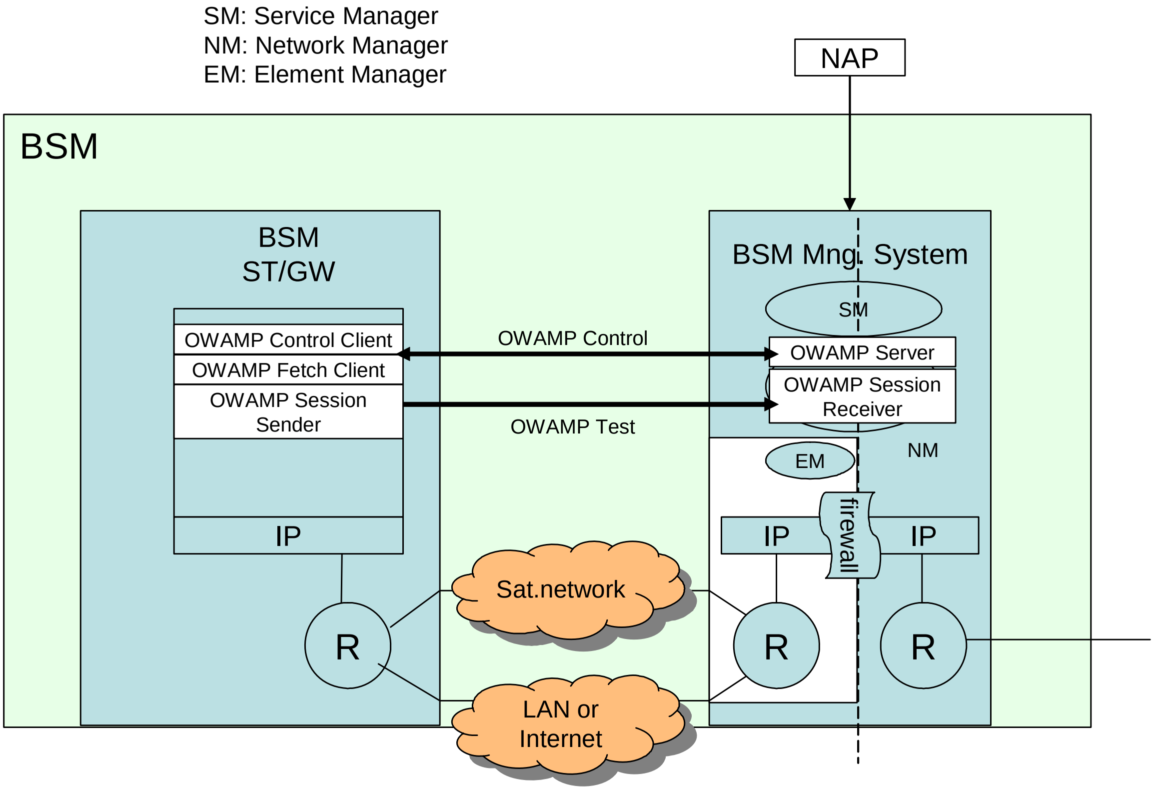


**Figure 7.5: BSM OWAMP-based Architecture**

Functions in the above diagram are:

Session-Sender: the sending endpoint of an OWAMP-Test session;

Session-Receiver: the receiving endpoint of an OWAMP-Test session;

Server: an end system that manages one or more OWAMP-Test sessions, is capable of configuring per-session state in session endpoints, and is capable of returning the results of a test session;

Control-Client: an end system that initiates requests for OWAMP-Test sessions, triggers the start of a set of sessions, and may trigger their termination; and

Fetch-Client: an end system that initiates requests to fetch the results of completed OWAMP-Test sessions.

## 7.2.2 Calculating BSM IP performance parameters

In this clause some guidelines are given on how to calculate BSM IP Performance Parameters.

### 7.2.2.1 Two-Measurement-Points BSM IP Performance Parameters

The BSM IP Performance Parameters considered in this clause are normally measured between two MPs, so it is recommended (even if not mandatory) to store them in a central PM server.

#### 7.2.2.1.1 IP Packet Transfer Delay (IPTD) and Delay Variation (IPDV)

Measurements of these parameters can be done directly (with OWAMP) or by collecting data at the PM server (with RMON, RTFM, IPFIX) and processing them. In case the measurement is performed on one-way the time sources at the nodes need to be precisely synchronized (e.g. by means GPS) in order to provide reliable measurements. The post-processing at the PM server also gives the possibility to elaborate statistics of the collected data, e.g. to derive the mean IPTD over a time window.

NOTE: These parameters (IPTD and IPDV) may also be estimated locally at the PM traffic nodes by measuring with probes the round-trip time (RTT) delay over a given satellite link (see annex A). In this case they could be stored locally. Anyway in this case the estimation is clearly less accurate and depends on several factors (UDP echo or ICMP echo, processing time at the remote node, etc.), for this reason it is suggested to adopt these RTT methods to update the Transmission Delay, $D_T$, parameter of the BSM SI-SAP performance parameters set (see clause 7.1).

RMON-1, PSAMP, and RTFM Meter MIBs can be used to keep track of the "sampling conditions" under which the measurement was performed.

#### 7.2.2.1.2 IP Packet Loss Ratio (IPLR)

Measurements can be done directly (with OWAMP) or by collecting data at the PM server (with RMON, RTFM, IPFIX) and processing them. Accurate time synchronization of the PM traffic nodes performing the measurement is not needed. Also here the post-processing at the PM server gives the possibility to elaborate statistics of the collected data, e.g. to derive the average IPLR over a specific time window.

NOTE: Even if possible, it is suggested to avoid estimating this parameter by round-trip measurements.

RMON-1, PSAMP, and RTFM Meter MIBs can be used to keep track of the "sampling conditions" under which the measurement was performed.

#### 7.2.2.1.3 Spurious IP Packet Rate (SIPR)

Measurements can be done directly (with OWAMP) or by collecting data at the PM server (with RMON, RTFM, IPFIX) and processing them. Accurate time synchronization of the PM traffic nodes performing the measurement is not needed. Also here the post-processing at the PM server gives the possibility to elaborate statistics over long time windows.

NOTE: It is not possible to estimate this parameter by round-trip measurements.

RMON-1, PSAMP, and RTFM Meter MIBs can be used to keep track of the "sampling conditions" under which the measurement was performed.

#### 7.2.2.1.4 IP Packet Reordered Ratio (IPRR)

Measurements can be done directly (with OWAMP) or by collecting data at the PM server (with RMON, RTFM, IPFIX) and processing them. Accurate time synchronization of the PM traffic nodes performing the measurement is not needed. Also here the post-processing at the PM server gives the possibility to elaborate statistics.

NOTE: Even if possible, it is suggest to avoid estimating this parameter by round-trip measurements.

RMON-1, PSAMP, and RTFM Meter MIBs can be used to keep track of the "sampling conditions" under which the measurement was performed.

#### 7.2.2.1.5 IP Service Availability (IPSA)

The way to derive this parameter is strictly linked to the way IPLR is estimated, and since IPLR should be measured between two MPs and stored on the PM server, the same applies to IPSA. Anyway it is difficult to estimate IPSA without a post-processing at the PM server. The IPSA is defined as the percentage of time intervals $T_{av}$, for which IPLR exceeds a threshold $c$, when measured over a minimum number of packets $M_{av}$ and over a minimum interval of time $T_{av}$. So the estimation of IPSA should be done by collecting data at the PM server (with RMON, RTFM, IPFIX) and processing them according to the given definition.

Accurate time synchronization of the PM traffic nodes performing the measurement is not needed.

NOTE: Even if possible (as for the IPLR), it is suggested to avoid estimating this parameter by round-trip measurements.

RMON-1, PSAMP, and RTFM Meter MIBs can be used to keep track of the "sampling conditions" under which the measurement was performed.

#### 7.2.2.2 Single-Measurement-Point BSM IP Performance Parameters

The BSM IP Performance Parameters considered in this clause are normally measured at a single MP, so they can be stored locally to the ST.

##### 7.2.2.2.1 IP Packet Error Ratio (IPER)

Measurements can be done by simply analysing the appropriate OIDs in the standard MIB-II at the ST, and applying simple processing to the relevant counters (e.g. *ipInHdrErrors*, *ifInErrors*, *ipInReceives*). For example the IPER calculated for all incoming IP packets, over a time window $T$ starting at $t_0$ can be calculated as:

$$\mathrm{IPER}_T(t_0) = \frac{ipInHdrErrors_{t=T+t_0} - ipInHdrErrors_{t=t_0}}{ipInReceives_{t=T+t_0} - ipInReceives_{t=t_0}}.$$

The flexibility in measuring this over a given population of interest is constraint by the counters available in the MIB-II.

This parameter can clearly represent an instantaneous value of the IPER metric when the time window selected is very short, but it can also be computed over a longer. In order to keep track of the "sampling conditions" under which this local measurement was performed, it is suggested to record the way the metric was computed, i.e. the OIDs used and at what time they were sampled.

##### 7.2.2.2.2 IP Packet Throughput (IPPT) and Goodput (IPPG)

The way to measure them is similar to the way proposed for IPER, but in this case since MIB-II does not define OIDs with the size in bytes of transmitted/received packets, the measurement should rely on other MIBs (e.g. the ones provided by the terminal manufacturer) local to the ST. If in these MIBs such OIDs are defined, the IPPT and IPPG can be measured by simply analysing the appropriate OIDs at the ST and manipulating appropriately the counters.

In this case the flexibility in measuring this over a given population of interest is constraint by the counters available in the used MIBs.

Also in this case this parameter can clearly represent an instantaneous value of the IPPT or IPPG metrics, when the time window selected is very short, but it can also be computed over a longer time scale. In order to keep track of the "sampling conditions" under which this local measurement was performed, it is suggested to record the way the metric was computed, i.e. the OIDs used and at what time they were sampled.

# Annex A (informative): Examples of Performance Management tests

The data in the samples for the set of metrics described in this annex can come from the following sources: one-way active measurement, round-trip measurement, and passive measurement. There infrequently is a choice between active and passive measurement, as typically, only one is available; consequently, no preference is given to one over the other. In cases where clocks can be expected to be synchronized, in general, one-way measurements are preferred over round-trip measurements (as one-way measurements are more informative). When one-way measurements cannot be obtained, or when clocks cannot be expected to be synchronized, round-trip measurement may be used.

# A.1 Active measurements

A possible way of monitoring BSM performance is by sending synthetic transactions between two STs or between an ST and other device (e.g. server). One ST acts as the "sender" of the test data, and the other acts as the "responder." The sender can be configured to send different types of synthetic transactions based on port, packet size, type of service, and even more advanced characteristics, as is the case with Voice over Internet Protocol (VoIP) tests.

Table A.1 lists some of the potential test types; most of them may also be performed as passive measurements, by simply monitoring existing traffic flow(s) or existing exchange of packets.

**Table A.1: Examples of potential performance management tests**

| Test Name | Measurement Capability | Example Use |
|---|---|---|
| UDP Jitter | Round-trip delay, one-way delay, one-way jitter, one-way packet loss (see note) | Validating and monitoring delay for latency-sensitive UDP applications |
| UDP Echo | Round-trip delay | Validating and monitoring delay for specific UDP applications |
| UDP Jitter for VoIP | Round-trip delay, one-way delay, one-way jitter, one-way packet loss, VoIP codec simulation: G.711 u-law, G.711 a-law, and G.729aMOS, and ICPIF voice quality scoring capability (see note) | Validating and monitoring VoIP environments, especially prior to rolling out VoIP or investing in VoIP infrastructure |
| TCP Connect | Connection time | Validating and monitoring delay for connection establishment on TCP applications |
| Domain Name System (DNS) | DNS lookup time | Validating and monitoring DNS resolution times across the network |
| Dynamic Host Configuration Protocol (DHCP) | Round-trip time to get an IP address | Validating and monitoring DHCP lookup times across the network |
| FTP | Round-trip time to transfer a file | Validating and monitoring file transfer times using the FTP protocol across the network |
| HTTP | Round-trip time to get a Web page | Validating and monitoring Web transactions across the network |
| Internet Control Message Protocol (ICMP) Echo | Round-trip delay | Validating and monitoring delay for ping response times over the ICMP protocol |
| ICMP Path Echo | Round-trip delay for the full path | Validating and monitoring service provider latency SLAs at all levels of service |
| ICMP Path Jitter | Round-trip delay, jitter, and packet loss for the full path | Validating and monitoring service provider latency and delivery SLAs at all levels of service |
| NOTE: One-way delay requires time synchronization between the source and target STs. | | |

Typical duration of these measurement intervals is 10 seconds. Typical default sending schedule is a Poisson stream. Typical default sending rate is 10 packets/second on average. A one-way (or round-trip) active measurement can be characterized by the source IP address, the destination IP address, the time when measurement was taken, and the type of packets (e.g. UDP with given port numbers and a given DSCP) used in the measurement. For the time, the start and end of the measurement interval need be reported.

# A.2 Passive measurement

Passive measurement use whatever data it is natural to use (e.g. IP telephony application). An analysis of performance of a link might use all the packets that traversed the link in the measurement interval. An analysis of performance of a service provider's network (satellite hub) might use all the packets that traversed the network in the measurement interval. An analysis of performance of a specific service from the point of view of a given site (satellite terminal) might use an appropriate filter to select only the relevant packets. The same typical default duration applies to passive measurement as to active measurement.

When the passive measurement data is reported in real time, or based on user demand, a sliding window should be used as a measurement period, so that recent data become more quickly reflected. For historical reporting purposes, a fixed interval may be preferable.

# Annex B (informative): IETF MIBs and BSM Performance Objects

The Internet Standard MIB (MIB-II) contains a group of management objects pertaining to a network device's generic network interface(s). These objects are generic in the sense that they apply to all network interfaces, irrespective of the type of communication media and protocols used on such interfaces. These objects are not sufficient and additional MIB objects specific to particular media and lower-level (subnetwork-layer and below) protocol stacks have been defined. Such objects are defined as extensions to the generic interface group, rather than defined in multiple specific-interface-type MIBs.

Some IETF MIBs already define many performance parameters at interfaces to IP hosts. Some of the most relevant MIBs related to performance at IP level and at sub-network interfaces are:

- RFC 1213 [3]: Management Information Base for Network Management of TCP/IP-based internets: MIB-II.
- RFC 1229 [i.22]: Extensions to the Generic-Interface MIB.
- RFC 2206 [i.23]: RSVP Management Information Base using SMIv2.
- RFC 2213 [i.24]: Integrated Services Management Information Base using SMIv2.
- RFC 2214 [i.25]: Integrated Services Management Information Base Guaranteed Service Extensions using SMIv2.
- RFC 2863 [i.26]: The Interfaces Group MIB.
- RFC 3289 [i.6]: Management Information Base for the Differentiated Services Architecture.

The BSM may use some or all of these MIBs for performance management, but a BSM Performance MIB will need additional interface-specific objects to be defined.

As an example, the IETF IntServ FlowEntry parameters could apply to the BSM SI-SAP by defining the SI-SAP as the relevant interface for these parameters.

The following IntServ FlowEntry parameters describe the use of a given interface by a given flow:

- intSrvFlowType;
- intSrvFlowOwner;
- intSrvFlowDestAddr;
- intSrvFlowSenderAddr;
- intSrvFlowDestAddrLength;
- intSrvFlowSenderAddrLength;
- intSrvFlowProtocol;
- intSrvFlowDestPort;
- intSrvFlowPort;
- intSrvFlowFlowId;
- intSrvFlowInterface;
- intSrvFlowIfAddr;
- intSrvFlowRate;
- intSrvFlowBurst;

- intSrvFlowWeight;
- intSrvFlowQueue;
- intSrvFlowMinTU;
- intSrvFlowMaxTU;
- intSrvFlowBestEffort;
- intSrvFlowPoliced;
- intSrvFlowDiscard;
- intSrvFlowService;
- intSrvFlowOrder;
- intSrvFlowStatus.

The counter "intSrvFlowPoliced" starts counting at the installation of the flow.

As described in clause 7, the BSM has a number of SI-SAP specific attributes which are defined for QIDs.

# History

| Document history | | |
|---|---|---|
| V1.1.1 | November 2009 | Publication |
| | | |
| | | |
| | | |
| | | |