|  |
| --- |
| Text Proposal for Accounting and Monitoring |
| Date: 2016-07-25 |
| **Authors:**  |
| Name  | Affiliation  | Phone  | Email  |
| Hao Wang | Fujitsu R&D Center | +86-10-59691000 | wangh@cn.fujitsu.com |
| Su Yi | Fujitsu R&D Center | +86-10-59691000 | yisu@cn.fujitsu.com |
| Xiaojing Fan | Fujitsu R&D Center | +86-10-59691000 | fanxiaojing@cn.fujitsu.com |
| Ryuichi Matsukura | Fujitsu/Fujitsu Laboratory | +81-44-754-2667 | r.matsukura@jp.fujitsu.com |
| **Notice:**This document does not represent the agreed view of the OmniRAN TG It represents only the views of the participants listed in the ‘Authors:’ field above. It is offered as a basis for discussion. It is not binding on the contributor, who reserve the right to add, amend or withdraw material contained herein.  |
| **Copyright policy:**The contributor is familiar with the IEEE-SA Copyright Policy <<http://standards.ieee.org/IPR/copyrightpolicy.html>>.  |
| **Patent policy:** The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://standards.ieee.org/guides/bylaws/sect6-7.html)> and <[http://standards.ieee.org/guides/opman/sect6.html#6.3](http://standards.ieee.org/guides/opman/sect6.html)>. |

Abstract

This document proposes initial text for the function of accounting and monitoring within Functional Design and Decomposition.

7 Functional Decomposition and Design 3

7.7 Accounting and Monitoring 3

7.7.1 Introduction 3

7.7.2 Roles and identifiers 3

7.7.2.1 Network Management Service 3

7.7.2.2 ANC 4

7.7.2.3 NA and BH 4

7.7.2.4 SS 4

7.7.3 Use Cases 4

7.7.3.1 Performance Analysis 4

7.7.3.2 Security Analysis 4

7.7.3.3 Billing 4

7.7.4 Functional Requirements 5

7.7.5 Accounting and monitoring specific attributes 5

7.7.5.1 Node of Attachment 5

7.7.5.2 Backhaul 5

7.7.5.3 Access Network Controller 5

7.7.6 Accounting and monitoring specific basic functions 5

7.7.6.1 Monitoring 5

7.7.6.2 Collection 6

7.7.6.3 Mediation 7

7.7.7 Detailed procedures 8

7.7.7.1 Accounting configuration 8

7.7.7.2 Accounting 9

7.7.8 Mapping to IEEE 802 Technologies 11

7.7.8.1 Overview 11

7.7.8.2 IEEE 802.3 specifics 11

7.7.8.3 IEEE 802.11 specifics 11

7.7.8.4 IEEE 802.16 specifics 11

7.7.8.5 IEEE 802.22 specifics 11

References 12

# Functional Decomposition and Design

## Accounting and Monitoring

### Introduction

The control of network resource utilization is essential for the support of applications with special demands and for the prevention of (malicious or accidental) waste of bandwidth. Accounting intends to provide utilization information and based on which sharing of network resources becomes possible. Besides billing applications, the data about resource usage can also be used as inputs for other applications such as network monitoring and planning, or security analysis. Therefore monitoring usage data of network devices is required by various upper-layer applications.

Accounting describes the process of gathering usage data records at network devices and exporting those records to an accounting server for processing. Then the records are presented to the user or provided to another application, such as performance management, security management, or billing.

Figure 7-7-1 shows the building blocks and their interactions for the purpose of accounting and monitoring. The four blocks are layered according to the processing of the data from the bottom level monitoring via collection and mediation, up to the final applications. The building blocks on different layers in the red block are configured through the policies from the application/management layer. Higher layer policies can be translated into lower layer policies. The configuration parameters are extracted from the policy and passed to the corresponding building block.



Figure 7-7-1: Accounting and monitoring building blocks

### Roles and identifiers

#### Network Management Service

NMS makes use of the functionality provided by ANC, and provides additional functions for management purpose. It represents a human interface to access network operators for manually access the usage data records.

#### ANC

ANC collects data gathered by monitoring on each NE. It also provides mediation functions for the collected data and transfers into well-formatted accounting records which will be provided to SS or NMS upon requests.

#### NA and BH

The observation points are set up on NA and BH capturing data about resource consumption. NA and BH maintain all basic monitoring parameters in MIBs. NA and BH also provide storage for the data before being collected.

#### SS

SS provides user-specific information for accounting service and provides policies for configuring the accounting functions.

### Use Cases

This section describes some accounting and monitoring use cases for deployment. These use cases are not meant to be exhaustive.

#### Performance Analysis

Accounting collection process gathers usage records of network resources, such as interface utilization, traffic per user or per path, and network management traffic. They may include details such as the originator and recipient of a communication.

Granularity of usage records can be for example individual user details for premium customers, normally of service provider’s interest, or a summary per department (access network) per enterprise’s interest.

For example, NMS can monitor one aspect of device performance by polling its accounting records and compare to history data to analyze deviation from normal as well as trending functions.

#### Security Analysis

Monitoring provided by accounting is a relevant building block for security solutions, because security management and incident mitigation depend entirely on information about the network’s state.

An application of security analysis can import the accounting records and analyze different types of protocols, traffic patterns between source and destination.

When attacks are taking place, the records can be used to detect unusual situations or suspicious flows and alarm the network operator, and further to reduce the risk of future attacks.

#### Billing

Accounting describes the process of measuring and collecting network usage parameters from network devices or application servers, and billing is an application that makes use of these well-formatted usage records.

A raw data collection cannot be sent to the user as an invoice. Instead, raw data needs aggregation, mediation, and de-duplication to be applied first to transform data into useful information for the customers. For a billing solution, the following steps are necessary after accounting:

* Charging derives non-monetary costs for accounting data sets based on service and customer specific tariff parameters. Different cost metrics may be applied to the same accounting records even in parallel. Charging policies define the tariffs and parameters which are applied.
* Billing translates costs calculated by the charging into monetary units and generates a final bill for the customer. Billing policies define among others the type (e.g. invoice, credit card), the form of the bill (e.g. itemized or not, etc.) and the time for billing (e.g. weekly, monthly, etc.).

### Functional Requirements

* Applying accounting policies and configuring parameters and processing accordingly should be supported.
* Monitoring of resource usage data records should be supported.
* Generating usage data records that log the user’s activities should be supported.
* Monitoring data storage and data collection should be supported.
* Data filtering, sampling, aggregation, correlation, de-duplication and mediation should be supported in order to transfer the usage data records into well-formatted accounting records.

### Accounting and monitoring specific attributes

#### Node of Attachment

* R1/R3 monitoring data
	+ E.g. transmitted/received volume, throughput, path utilization, QoS parameters, etc.

#### Backhaul

* R3/R6 monitoring data
	+ E.g. transmitted/received volume, throughput, path utilization, QoS parameters, etc.

#### Access Network Controller

* R5/R7 collected data
	+ E.g. network usage per user/group/department, traffic per server/service, etc.
* R4 accounting policies, monitoring configurations
	+ E.g. rules for generation, transport, and storage of accounting data, collection model (push or pull), filtering criteria, sampling method (deterministic or random), monitoring scope, type, schedule, granularity, etc.
	+ Accounting data
	+ User-specific information
* R11 accounting data

### Accounting and monitoring specific basic functions

#### Monitoring

Monitoring is the process of gathering and optionally preprocessing usage data records at devices in the network. These devices can be either network elements with integrated monitoring functionality or a dedicated measurement device (“black box”) that is specifically designed as a monitor.

Monitoring is also referred to as metering collecting observed traffic. This form of monitoring does not affect the user traffic, because it listens to only the packets that pass the meter/observation point.

The monitoring process can be configured by applying monitoring policies. For configuration of the monitoring, the following issues must be addressed: trigger condition for monitoring, monitoring scope (e.g. all data or selected data), type (i.e. which data or information elements are to be collected for a specific device or system, which service events, signaling, or user traffic to monitor), granularity (measurement intervals etc.), and schedule (specifying the time frames during which the measurement job will be active).

Monitoring may supply the following information to be collected for further processing:

* network parameters, e.g. link performance monitoring;
* service parameters, e.g. transmitted volume, throughput, path utilization, QoS parameters, etc.

In general, ANC sends a monitoring request indicating the monitoring policies to the entities in the access network. Upon receiving the request, NE starts the monitoring process.

Each monitoring job running on an NE produces scheduled monitoring reports (measurement records) at the end of each granularity period, and contains the information as requested by the ANC. This information consists of:

* an identification of the monitoring job that generated the report;
* an identification of the involved monitoring type(s) and the measured network resource(s) (e.g. NA);
* a time stamp, referring to the end of the granularity period;
* for each monitoring type, the result value(s) and an indication of the validity of the result value(s);
* an indication if the monitoring is not complete, and the reason why the monitoring could not be completed.

#### Collection

The data gathered by the monitoring has to be collected at the collection server for further processing.

Collection policies define how collection is done and what to collect. Collection server in ANC applies collection rules provided by the SS and configures the collection process to, e.g.

* guarantee the delivery of critical accounting;
* avoid the accounting reports to congest the network and affect the user traffic;
* balance the accounting accuracy and network load;
* monitor the retrieved records for completeness and identify lost accounting records.

Collection methods are classified as push model and pull model.

* In push model, monitoring data are not stored at the devices or are kept there for a short time until being pushed toward a collection server (ANC) at the end of the granularity period. The exporting is event triggered.
* In pull model, the monitoring data are stored in device (like counters in MIB) and assembled for collection. The device constantly updates the counters while the external instance like ANC is responsible for regular collection. The exporting frequency can be configured at ANC.

Simply put, in push model, collection is initiated by NE itself, while in pull model, collection is initiated by ANC. The collection server checks the completeness and then starts the mediation process.

#### Mediation

Mediation means processing on the collected data records, including the following sub-functions:

* Filtering

In most cases the large amount of captured data makes filtering and/or aggregation after the metering necessary. This is because some technologies such as SNMP interface counters do not offer a filter concept at the meter. Some devices do not support complex filtering because the implementation of process-intensive filters at the network element has a performance impact. In these cases of static meters, all traffics are measured with a fixed granularity, not distinguishing if a subsequent charging process needs the specific meter data or not. Therefore filtering is needed at the mediation device to reduce the volume of data.

* Threshold monitoring

A prerequisite for monitoring thresholds is a baseline of the network performance under normal circumstances. When the mediation device monitors a sudden change in the traffic patterns, it should be brought to the administrator's attention immediately.

Threshold monitoring is an optional task for the mediation device. For example for security monitoring, a relevant feature is to set thresholds for the received traffic and monitor them in real time, because a reaction to an attack must occur quickly.

* Data aggregation

Collected data can be aggregated before being passed to NMS or SS. The concept of aggregation describes the task of reducing the granularity by identifying common criteria and combining information from multiple records which may come from different meters into a single record, providing a comprehensive association among records.

Aggregation criteria can use a combination of different types of data. One type of aggregation is based on common criteria (key fields). Specifically for different accounting records with the same key field, merge such multiple data sets into one. These key fields include source/destination address, source/destination port, QoS parameters, etc. Another type is to aggregate over time. Aggregation is applied to both accounting and performance records within specific period

* Data record correlation and enrichment

Another task at the mediation layer is correlating information from different monitoring sources to enrich the data records.

Grouping information from different sources into a common data records is a clear benefit of upper-layer applications, such as billing, which can retrieve enriched data sets instead of very basic sets, which need correlation afterwards.

In addition, data record correlation can replace the key of record for easy understanding of applications in NMS.

* Data record de-duplication

If data records are collected at several locations in the network, chances are great that one record will be collected multiple times at different metering locations. Duplicate records lead to inaccurate results at the application level; therefore, these duplications need to be eliminated. The de-duplication algorithm identifies a data record’s constant parameters. If multiple data records have the same constant parameters and were received from multiple devices within a defined time window, they can be considered duplicates, and all data records except one are eliminated.

* Data formatting and storage

The processed data records are stored in a database and made available to other applications. Records have to describe usage type details, such as keys and values, where a key links to an index in a database table. A common data format definition protects the NMS and OSS applications from the variety of accounting formats that are implemented at the device level.

The location where the records are stored can be a simple flat file system or a complex relational database system that provides sophisticated operations for local and remote access. In both cases, the format in which data records are stored should be consistent among various vendors.

SS sets the policy on how each sub-function in mediation is done. Some tasks, such as threshold monitoring and aggregation over time, can be applied at the upper-layer application level instead of the mediation device.

### Detailed procedures

#### Accounting configuration

The accounting policies describe rules for generation, transport and storage of accounting data, which are used for the configuration of the accounting process. As shown in Figure 7-7-2, the procedure of accounting configuration is described as follows,

* After the success authentication of a user, SS sends accounting configuration message to ANC with the policy specified to this user. The accounting policy includes the following information:
	+ Accounting policy condition: user ID, address of network devices from which the service usage takes place, time, service class (like the different level of QoS), and accounting type.
	+ Accounting policy action: accounting record structure, accounting record destination, report interval, storage time, record access list, flow granularity, meter accuracy.
* ANC receives the accounting configuration message and replies ACK. Then it converts the accounting policies into monitoring configuration message and sends to the appropriate NE, such as NA in this case..
* NA acknowledges the monitoring configuration message and sets up local meter.



Figure 7-7-2 Procedure of accounting configuration

The accounting is applied towards the authorized service (like Ethernet access service). Therefore, the accounting configuration procedure can be integrated into the authorization procedure (like AAA authorization framework). The configuration of accounting infrastructure can be carried together with the user configuration (like user specific QoS requirements) of the devices in the access network (e.x NA), which might involve the transfer of configuration data to multiple NEs in the network.

#### Accounting

As shown in Figure 7-7-3, detail procedure for accounting is described as follows,

* ANC sends the accounting request to start the accounting service towards specific user. The accounting request (start) should include the following information:
	+ User name
	+ ANC identifier or address
	+ Meter port and port type
	+ Accounting session ID
	+ Service type or other information of service provisioning.
* Upon reception of the request, SS sends an accounting response as acknowledgement. Optionally, SS may record the starting time or other information related to the accounting service of this session.
* Confirmed by the response, ANC sends a monitoring request to NA starting the metering process. The same information in previous Accounting request can also be included in the monitoring request (start).
* NA replies a monitoring response as acknowledgement upon receiving monitoring request. And NA starts the metering process according to the metering configuration towards this connection session of the user.
* During the connection session, NA sends the monitoring indication to ANC according to the collection configuration. The monitoring indication includes interim metering results of the session , such as
	+ SessionOctestsRx
	+ SessionOctetsTx
	+ SessionFramesRx
	+ SessionFramesTx
	+ Session ID
	+ User name
	+ Session time.
* ANC sends monitoring confirmation to acknowledge the monitoring indication message. Reception of a monitoring indication may trigger the mediation process on ANC. As a result, ANC sends an accounting request (interim) to SS, so that SS (and even accounting server) can get the service consuming condition in real time. The accounting request (interim) includes the following information:
	+ Accounting delay time
	+ Input octets
	+ Output octets
	+ Accounting session ID
	+ Session time
	+ Input packets
	+ Output packets
	+ User name or other service provisioning information
* SS should send the accounting response to acknowledge the accounting request (interim), if the accounting data are recorded successfully.
* At the end of the connection session, ANC should send monitoring request (end) to retrieve the final session metering results and end the metering process on NA. The same information in the monitoring request (start) can also be included in the monitoring request (end).
* Upon receiving a monitoring request (end), NA should send a monitoring response with the final session metering results to ANC, and stop metering process.
* The accounting request (end) is sent by ANC to SS including the accounting data about the session and the cause of session termination, e.x EAPOL-logoff (user request), lost carrier, session timeout or any session error. At last, SS should send the accounting response as acknowledgement, if the accounting data are recorded successfully.



Figure 7-7-3 Procedure of accounting

### Mapping to IEEE 802 Technologies

#### Overview

The following table provides IEEE 802 technology specific attributes for accounting and monitoring.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 802.3 | 802.11 | 802.16 | 802.22 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

#### IEEE 802.3 specifics

#### IEEE 802.11 specifics

#### IEEE 802.16 specifics

#### IEEE 802.22 specifics

### References

[1] Benoit Claise and Ralf Wolter, Network Management: Accounting and Performance Strategies, 2007

[2] RFC 3334, “Policy-Based Accounting,” Copyright © The Internet Society, 2002

[3] 3GPP TS 32.401, “Telecommunication management; Performance Management (PM); Concept and requirements,” V13.0.0

[4] 3GPP TS32.240, “Telecommunication management; Charging management; Charging architecture and principles,” V13.0.1

[5] WMF-T31-119-R016v01, “WiMAX Forum ® Network Requirements; WiMAX Network Management; NMS to EMS Interface,” 2010

[6] IEEE Std 802.16-2012 “Part 16: Air Interface for Broadband Wireless Access Systems”, 2012

[7] RFC 2866, “RADIUS Accounting,” Copyright © The Internet Society, 2000