Network Working Group
Request for Comments: 3334
Category: Experimental

T. Zseby
S. Zander
G. Carle
Fraunhofer FOKUS
October 2002

Policy-Based Accounting

Status of this Memo

Copyright Notice

Abstract

This document describes policy-based accounting which is an approach to provide flexibility to accounting architectures. Accounting policies describe the configuration of an accounting architecture in a standardized way. They are used to instrument the accounting architecture and can be exchanged between Authentication, Authorization and Accounting (AAA) entities in order to share configuration information.

This document describes building blocks and message sequences for policy-based accounting in the generic AAA architecture (RFC 2903). Examples are given for the usage of accounting policies in different scenarios. It is also shown how accounting components can be integrated into the AAA authorization framework (RFC 2904). This document does not propose a language for the description of accounting policies. Rather, it is assumed that a suitable policy language can be chosen from existing or upcoming standards.

Table of Contents

1. Introduction

1.1 Motivation

Even if we will have much more bandwidth in the future than now, the control of network resource utilization remains essential for the support of applications with special demands and for the prevention of (malicious or accidental) waste of bandwidth. Charging provides a possibility to control utilization and sharing of network resources. Charging in multi-service networks can be done based on the reserved or the actual used resources. Charging on reserved resources is an important concept since reservation usually precludes other users from using the reserved resources. Nevertheless, if charging is limited to reservation parameters only, the applied charge depends on the ability of the user to give a good prediction of the expected traffic characteristics. This can be extenuated by using a charging scheme that is based on both the reserved and the used resources. In order to support usage-based charging, the collection of information about the resource reservation and utilization is required. The collection of data about resource usage is called accounting.

Service providers have various options for service differentiation, charging schemes and the provisioning of accounting services. The applied charging schemes for the provided services are one significant feature used by providers to distinguish themselves from competitors. Therefore, providers use different charging schemes and may change the schemes in accordance with their business plan. Providers can also offer different accounting services (e.g. standard, comprehensive, etc.) in order to allow customers/users to choose one scheme that meets the customers/users needs. Furthermore, it may be advantageous for a provider to outsource accounting functionality to a third party. Users introduce various traffic profiles and may have individual preferences regarding accounting services (like itemized invoices, accounting indications, spending limits etc.).

One further challenge for the configuration of accounting services are heterogeneous metering and accounting infrastructures within provider domains. Also, the usage of different accounting and metering solutions used in different provider networks complicates the sharing of configuration parameters (e.g. in roaming scenarios).

The configuration and dynamic adaptation of the accounting process to the business model and specific user demands requires a flexible configurable accounting infrastructure. The utilization of standardized policies for the expression of conditions and related configuration actions also allows the configuration of heterogeneous infrastructures. For this purpose we propose to use accounting policies to configure the accounting infrastructure and use the Authentication, Authorization and Accounting (AAA) architecture to exchange and to deploy these policies.

1.2 Document Scope

This document describes the structure and usage of accounting policies. It shows how the characteristics of the provider network influence the requirements for accounting. The relations between the different roles that are involved in the accounting process and the required building blocks for an accounting architecture are introduced. This document describes an architecture and mechanisms to configure the accounting service. It proposes to use the AAA protocol for the exchange of accounting configuration information expressed in policies. It does not propose a specific protocol for the accounting configuration itself. The configuration itself can be done by existing protocols (e.g. Common Open Policy Service Protocol for Support of Policy Provisioning - COPS-PR, Simple Network Management Protocol - SNMP, etc.). Furthermore, it is shown how different accounting services can be provided in intra- and inter-domain scenarios. Examples are given for the usage of accounting

policies in different scenarios. They show how accounting components can be integrated into the authorization framework proposed in [RFC2904].

Accounting management architectures and objectives as well as the transport of accounting records are discussed in [RFC2975] and are not further explained here. This document focuses on the configuration of the accounting architecture and measurement devices.

The policy-based accounting architecture represented in this document describes policy-based accounting from the perspective of a Generic AAA Server [RFC2903]. Such a server combines into a single entity the functions of managing accounting policy, together with the functions of managing user-specific authentication, authorization and service provisioning. Some service providers may choose to implement an approach that does not combine these functions into a single entity or protocol, in which case that particular aspect of this architecture does not apply.

This document does not propose a language for the description of accounting policies. It is rather assumed that a suitable policy language can be chosen from existing or upcoming standards.

2. Terminology

Accounting Indication/Confirmation
: Accounting indication messages are pushed from the originating AAA server (the server where the accounting information was generated) to the recipient which can be an AAA server or a customer/user application. Accounting indications contain accounting records which describe the resource consumption for a service. Accounting indication messages can also contain aggregated information for multiple services. There can be interim and end-of-session accounting indication messages. Interim indications are delivered in specified intervals to the recipient during the service session while end-of-session indications are given to the recipient at the end of the session only. Accounting indications may be acknowledged by accounting confirmations to provide application layer reliability.

Accounting Policy Indication/Confirmation
: Accounting policy indication messages contain accounting policies and are sent from a customer/user or a AAA server to another AAA server. Accounting policy indications may be acknowledged by accounting policy confirmations to provide application layer reliability.

Accounting Request/Answer
: Accounting requests are sent by an AAA server to another AAA server to request the current accounting information for a particular session set (polling). The request is answered with an accounting answer which contains the accounting records.

Accounting Policy Request/Answer
: Accounting policy requests are sent by an AAA server to another AAA server or a customer/user to request accounting policies for a service. The request is answered by an accounting policy answer that contains the accounting policy.

Accounting Policies
: Accounting policies describe rules for generation, transport and storage of accounting data. These rules are used for the configuration of the accounting process.

Application Specific Module (ASM)
: An ASM provides the functionalities required for the user configuration of a service to an authenticated and authorized user. It gets application specific information (ASI) (e.g. for user configuration) from the AAA server, either in a generic format or in an application specific format, encapsulated in a standard message sent to the ASM. The ASM either extracts the ASI from the message or converts information given in a generic format into the appropriate application specific format. Further information on how the ASM is used can be found in [RFC2903].

Charging Schemes
: A charging scheme is an instruction for calculating a charge. Usually, a charging scheme is represented by a formula that consists of charging variables (e.g. volume, time, reserved peak rate) and charging coefficients (e.g. price per time unit). The charging variables are usually filled by information from accounting data.

Classifier
: This document uses the definition of classifier as given in [RFC2475]. Since this document assumes that meters already include classification functions, the term classifier is only used for entities that perform additional classification (e.g. as part of data post processing).

Meter
: This document uses the definition of meter as given in [RFC2722]. This meter definition already includes the classification of packets. It differs from the DiffServ model [RFC2475] where classifier and meter are considered as separate entities.

Meter Reader/Collector
: This document uses the definition of meter reader and collector as given in [RFC2722].

Meter Manager
: This document uses the definition of meter manager as given in [RFC2722].

Policy, policy condition, policy action
: The terms policy, policy condition and policy action are used as defined in [RFC3198].

QoS Auditing
: Quality of Service (QoS) Auditing is the process of evaluating whether a given quality of service guarantee (e.g. thresholds for QoS parameters given in a Service Level Agreement - SLA) has been met during the service provisioning.

Service Class
: A service class specifies the handling of a service (as defined in [RFC3198]) belonging to that class by the service provider. A service class has some kind of identifier (e.g. name) and the handling of the service is defined by a Service Level Specification (SLS) as described in [RFC3198].

User Configuration
: We refer to User Configuration as the process of configuring a service for a user which has been authenticated and authorized by the AAA architecture. Although an AAA architecture is not directly responsible for this user-dependent configuration, it may be responsible for triggering the process.

Further definitions of service related terms (Service, Service Subscriber, Service User, Network Provider, Service Provider, Broker) can be found in section 4 (business roles and their relations).

3. Impact of Provider Network Characteristics on Accounting

There are many options for future service providers for the realization of service differentiation and provisioning. Therefore, provider networks can vary with respect to several characteristics that impact accounting and charging:

- Size and Purpose
A small ISP that deals with individual customers may charge individual users based on single flows. Backbone operators often have small ISPs and large corporations as customers, and usually charge based on traffic aggregates instead of individual flows.

- QoS provisioning technique
Diffserv accounting requirements differ from Intserv accounting requirements (e.g. meter granularity).

- Service classes
The definition of service classes within a network and the degree of freedom that customers are given (e.g. gold/silver/bronze service vs. a free choice of individual traffic profile parameters) is important, e.g. for the flow classification within the network, and influences the accounting functions required.

- Charging scheme
There exists a wide variety of charging schemes using tariff variables based on different technical and/or economic models. The chosen charging scheme(s) influence the accounting requirements for the provider. While some charging schemes lead to zero or only few accounting requirements, other charging schemes may be highly demanding. For instance, flat rate charging schemes require no accounting infrastructure at all. In contrast to this, volume-based charging schemes require the measurement of the transmitted volume and, with this, increases the complexity for accounting. Tariffs that introduce variable prices may require to provide the users regularly with accounting information (e.g. by interim accounting indications).

- Accounting Services
Providers may offer different accounting services (e.g. accounting indication, itemized invoice, etc.)

- Accounting agreements with other providers
Providers may have agreements with other providers in order to share accounting tasks and distribute accounting data so that, e.g., metering need only be done once. If so, it may be useful if providers can not only exchange accounting data, but also information on the configuration of accounting modules (e.g. meters). It is

important for providers to agree beforehand how accounting data will be collected and monitored, and how disputes concerning accounting data will be resolved. In order to minimize disputes between providers, it is important for them to agree that either both will collect accounting data - and will compare it with the other's data at regular intervals, e.g. monthly - or both will use a single source of accounting data provided by one of them (or by a trusted third party).

- Exploiting Capabilities of Existing Infrastructure (meters, data collection points)
Providers may already have functions within the network that can provide accounting functions (e.g. MIB objects, profile meters, proprietary accounting solutions). In order to avoid duplicated functionality, it should be possible to use these accounting resources. Therefore, the configuration of different types of accounting modules (e.g. meters) should be possible. A common language to express accounting module configurations would be useful for this purpose.

4. Business roles and relations

In investigating service provisions in the current and forthcoming Internet, we identified different business roles which are part of the service usage lifecycle. In this section we first define the term service. Afterwards, the different roles and their relationships are defined. The business roles in this model are used in the later examples.

- Service
A service is a set of capabilities offered by a provider to a customer. In this definition, provider and customer can be one of the business roles defined later. Different kinds of services have to be recognized.

  - Information services handle the delivery of information to the customer on top of transport services. In content-based services, the service subscriber pays for the content (e.g. for a file, an image, a video, etc.). In communication-based services, the service subscriber pays for the provisioning of a certain form of communication (e.g. video conferencing or IP telephony).

  - Transport services describe the provisioning of pure transportation of IP packets. At the IP layer, this may include the differentiation of packets (e.g. number of packets with a certain DSCP), Intserv based reservation or other methods for QoS enhancement (e.g. Automatic Repeat reQuest - ARQ, Forward

Error Correction - FEC). A transport service might also include mechanisms on other layers for improving the transport (e.g. MPLS).

- Management services are responsible for the management of resources (e.g. configuration, accounting, security). Accounting services describe the provisioning of data about the current or previous resource reservation and usage. Accounting services are needed by providers to generate a bill or by users to monitor their resource usage.

- Service Subscriber
The service subscriber is the entity that has subscribed to a service and thus has a contractual relationship with a service provider and a network provider which provides the underlying transport service. A service subscriber can also act as a service user. The service subscriber might have a relationship with a broker that provides service relevant information.

- Service User
The service user is the entity that uses the service. The service user can be identical to the service subscriber. In cases where subscriber and user are not identical, the service subscriber should be able to control the service usage for all service users she is responsible for.

- Network Provider
A network provider is the entity that provides the underlying network infrastructure for the service user, service subscriber, service provider and broker. A network provider provides transport services. The services are delivered on top of the network infrastructure. The service provider has a contractual relationship with the service subscriber and service provider (and the broker). The transport network of a network provider is probably not a global network which connects all subscribers, providers and brokers. The transport network is segmented into a number of sub-networks or domains controlled by different network providers with business relations existing between them. Each domain is responsible for intra-domain management and accounting. For inter-domain management and accounting, appropriate communication interfaces between network providers must exist.

- Service Provider
A service provider entity provides a service. A service provider can offer a service directly to the service subscriber/user. A service provider can also act like a wholesaler selling a service to another service provider (retailer) which re-sells the service to the service subscriber. The service provider has contractual relationships with

other service providers, subscribers, brokers and network providers. A service provider provides information services on top of transport services provided by network providers.

- Broker

The broker entity allows the other roles to access the information controlled by the broker. The broker can provide different information to different business roles. For example, a service subscriber can get references to appropriate service providers and/or network providers (e.g. a broker gives the subscriber a reference to a network provider which can provide bandwidth as required by the subscriber). A broker can also interact with other brokers to complete their information. In this case, broker-to-broker business relationships exist.

Figure 1 depicts the different roles and the business relations between them.

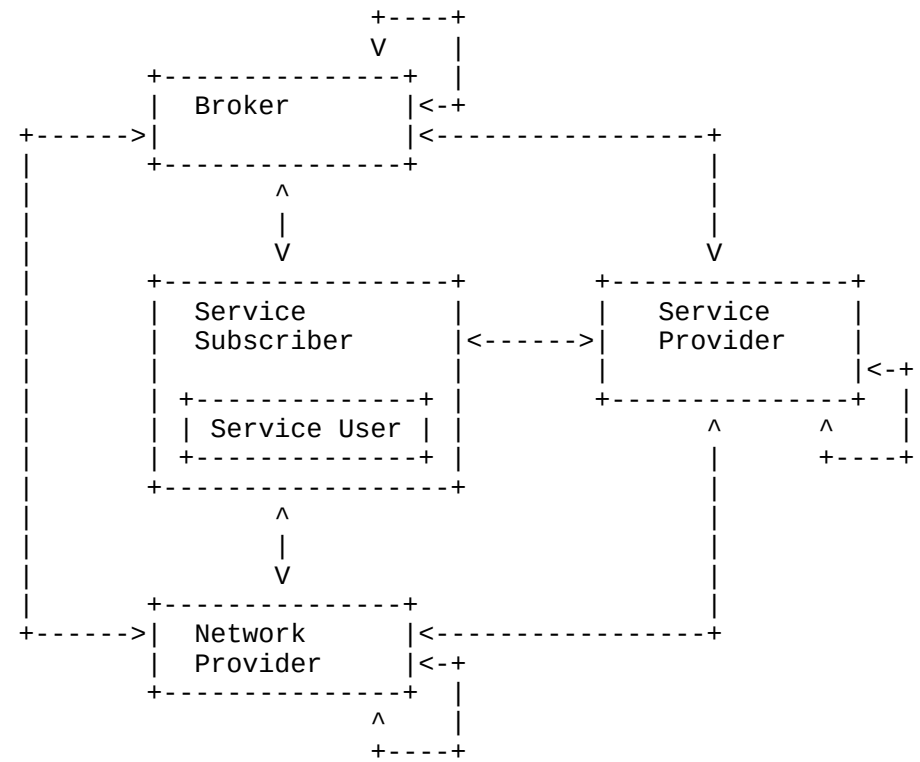

Figure 1: Roles and business relations

The following examples show how this business relationship model can be applied to different services.

Example 1: This example describes an Internet printing scenario according to the "print-by-reference" model [RFC2566]. The subscriber is a company and the users are the employees of that company. The file server and print server belong to two different service providers. The company subscribes to the print server service which acts as reseller for the file service. The file server service chooses the appropriate transport service (maybe based on user preference), thus the file server has a contract with a network provider using the offered transport service for downloading the data from the given location and sending them to the print server.

Example 2: A company (service subscriber) has a contract with a video archive (service provider). An employee can download clips in different qualities from the archive. The employee can use different transport mechanisms for the download. In order to get the appropriate transport, the user contacts an agency (broker) that returns a reference to a network provider which provides the required transport service. As an alternative, the content (video) can be delivered in different qualities via different transport mechanisms by the service provider. The service provider chooses an appropriate network provider which provides a transport service compliant with the conditions the service provider offers to the subscribers. In this case the service provider can use the facilities of a broker to get a reference to appropriate network providers.

5. Reference Model and Building Blocks

We have developed a reference model for describing the interactions between the different metering, accounting and charging processes and their configuration via policies. This reference model is shown in Figure 2. At the right side, five layers show the different building blocks. The blocks are layered according to the processing of the data from the bottom level metering via accounting, up to the final billing process. Data aggregation is not only done at the collection layer, it can also be done at the other layers. The building blocks on the different layers are configured through the policies shown on the left side. 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. The tasks of the different building blocks are as follows:

- Metering

Meters are needed for capturing data about resource consumption in the network (e.g. transmitted volume). They will probably be placed at the edges of the network. Two types of meters can be

distinguished: Static meters and configurable meters. In the case of static meters, all flows are measured with a fixed granularity, not distinguishing if a subsequent charging process needs the specific meter data or not. In most cases the large amount of captured data makes filtering and/or aggregation after the metering necessary. In case of a configurable meter, the meter collects meter data only for flows specified by metering policies.

For configuration of the meter process, the following issues must be addressed: (a) metering scope (whether to meter all flows or only selected flows), (b) flow granularity (e.g. micro flows or traffic aggregates) (c) metered flow attributes (i.e. which data is to be collected for a specific flow), and (d) meter accuracy (measurement intervals etc.).

- Collection

The data gathered by the meter(s) has to be collected for further processing. Collection of meter data can be initiated by the meter itself (push model) or by a collector entity (pull model). Collected data can be aggregated before being passed to the accounting layer. Metering policies define how collection and aggregation is done.

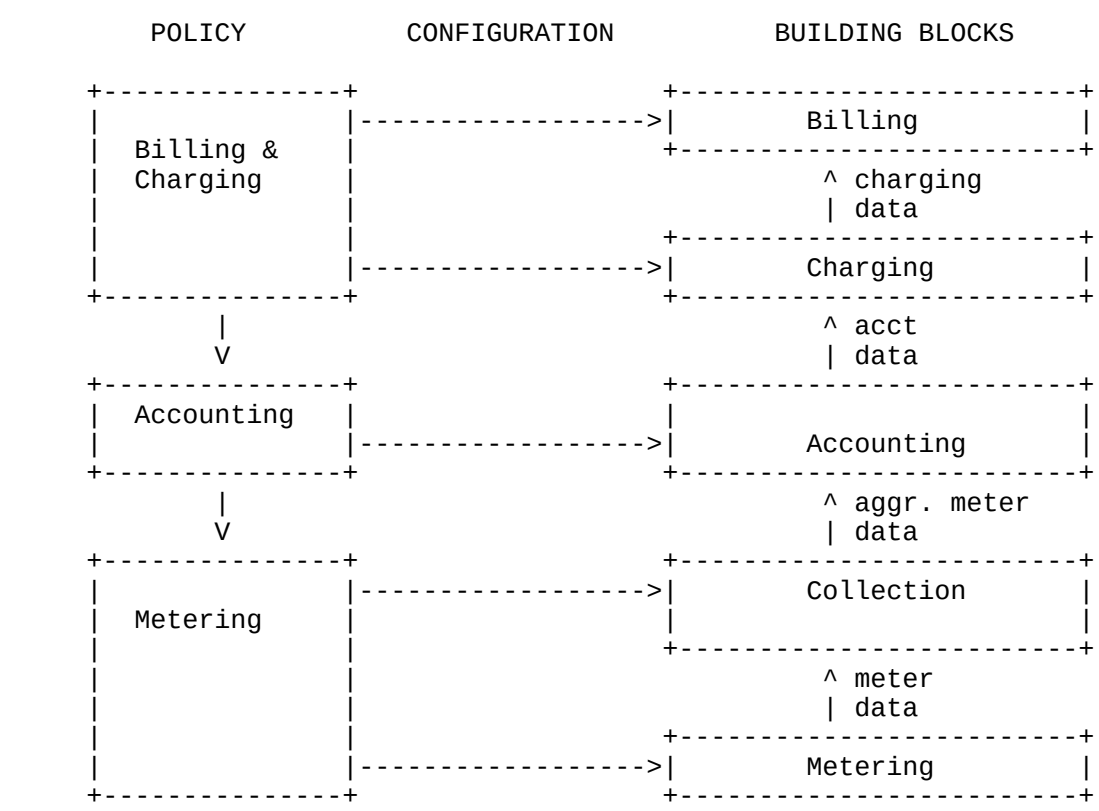

Figure 2: Reference Model

- Accounting
Accounting describes the collection of data about resource consumption. This includes the control of data gathering (via metering), transport and storage of accounting data. For subsequent charging, the metered data must be associated with a user that is the initiator of a flow and a customer (service subscriber) that is responsible for payment. For initiation of an accounting process, a user or foreign provider must be authenticated and authorized. These three functions can be performed by the AAA server. The accounting process is configured through accounting policies.

- Charging
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
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, partial anyomization, etc.) and the time for billing (e.g. weekly, monthly, etc.).

We propose to use policies expressed in a standardized way to appropriately configure the meter, meter data collection and accounting processes.

6. Accounting Policies

Accounting policies describe rules for generation, transport and storage of accounting data. They can be exchanged between AAA instances at the user or provider premises. They provide a standardized representation of configuration information that can be converted into the appropriate settings for different elements of the accounting infrastructures (e.g. different meters).

As shown in Figure 2, accounting policies configure the accounting process. Policies for the configuration of the metering and collection process can be derived from accounting policies. Accounting policies are not used to configure the charging or billing process. Accounting policies reside in the AAA server (local policies) or are received from other AAA servers (extra-domain policies) or customers/users. Two different models of obtaining accounting policies can be differentiated: push and pull model.

Push Model
In the push model, accounting policies are pushed from another AAA server or customer/user in order to establish the policies in the local accounting infrastructure. The acceptance and use of pushed policies requires special security considerations. The evaluation of the policy should not take place without an appropriate security check of the policy in advance. Also, the evaluation of the condition can lead to unwanted actions in the AAA server if the condition contains critical data either intentionally (to attack the system) or by accident. Even the evaluation of the condition can cause problems (e.g. DoS). Therefore, not only the action, but also the condition, has to be checked for potential security hazards before it is evaluated.

Pull Model
In the pull model, the AAA server requests the policy from a remote AAA server or customer/user by sending an accounting policy request. The remote AAA server sends an accounting policy reply as an answer that contains the appropriate policy.

Accounting policies are enforced by the network elements that are configured in accordance with the policies. They influence the following settings in the accounting architecture:

- meter configuration
- data collection and aggregation
- accounting record distribution and storage

6.1 Accounting Policy Condition

An accounting policy consists of one or more rules, each having a condition part and an action part. The condition part expresses under which condition the policy should be enforced. The following attributes are examples for variables in a policy condition statement.

- customer/user ID

The customer/user ID identifies the customer or user of the service. It can be used in a policy condition in order to select a customer or user specific accounting configuration (as policy action). For example, it can be user-dependent whether accounting indications are sent to the user or not.

- IP address

IP addresses specify the devices or networks from which the service usage takes place. The address of specific hosts or subnets can be used to select accounting strategies specific to the customer or a user group associated with this address (e.g. all customers of an ISP, all public terminals etc.).

- time of day

The time of day can be used, for instance, to configure the level of detail for the accounting record, the report interval and the destination.

- service class

Service classes are defined by the provider. They describe different levels or different kinds of services that are offered by the provider and are usually defined based on a business model. Customers/users select a service class. This selected class can be used in accounting policies to define appropriate accounting settings per class. With this it is possible, for instance, to provide more detailed accounting records for higher prioritized services than for standard services.

- accounting type
Accounting types combine multiple accounting settings under one keyword. Like service classes, the offered accounting types are defined by the provider in accordance with the business model. With this, providers can offer, for instance, different accounting types for one service and allow the customer/user to select one. The combination of settings under one keyword simplifies the selection for users. An example is the combination of high granular accounting records with short report intervals under a keyword (e.g. "comprehensive accounting"), or less frequent generation of less detailed records accessed by another keyword ("standard accounting"). The definition of accounting types can also help in inter-domain scenarios if providers agree on accounting types.

6.2 Accounting Policy Action

The action part defines the action that takes place if the condition is true. The action for an accounting policy is usually the configuration of the accounting infrastructure. This can already include settings for meters and collection entities. The following list gives examples for parameters of the accounting infrastructure that can be configured by an accounting policy action:

- accounting record type/structure
The required accounting data depends on the charging scheme. Therefore, different accounting records should be supported. There are two possibilities: Either different record types are defined, or a flexible record is used that consists of a variable set of accounting attributes. Accounting policies can be used to communicate to neighbor providers which kind of accounting record is needed to provide appropriate data for the charging scheme. The specification of the required accounting attributes can influence the settings of different components of the accounting architecture (e.g. which attributes have to be measured). An overview of accounting attributes and records can be found in [RFC2924].

- accounting record destination
The accounting record destination describes to which entities accounting records are sent. The accounting record destination can be a charging entity, a neighbor provider, a user entity or a specific database. In these cases, authentication and authorization mechanisms have to be applied in order to ensure that unauthorized entities cannot get access to confidential data.

- report interval
The report interval specifies in what time intervals accounting records are generated and sent. This influences the configuration of meters and collectors in the accounting architecture.

- storage time
If the accounting record destination is a database or a log file, the storage time specifies how long the accounting records have to be stored.

- access list
The access list specifies who has the permissions to read the stored accounting records.

- flow granularity
The flow granularity determines how fine grained (in coverage) the flows in the network are measured. The granularity usually is configured by installing specific classification rules in the meter. It is also possible to set a specific granularity by configuring aggregation schemes that are applied after the metering process. The granularity can range from individual micro flows (e.g. determined by the quintuple <src, dest, proto, src-port, dest-port>) up to coarse granular traffic aggregates (e.g. all traffic from one network).

- meter accuracy
The parameters for the meter accuracy can determine, for instance, how often measurements take place at the meter, how accurate timestamps should be, etc. Meter accuracy parameters can also be used to configure sampling schemes.

6.3 Example for Meter Configuration

Note: In the following examples, the use of NeTraMet or NetFlow to collect accounting information does not guarantee exact accounting data, so it is not recommended for use in situations where exact accounting data are needed.

The following two examples show how accounting policies can be used to configure different meters. The accounting policy is sent from the AAA server to the ASM and there converted to the appropriate configuration information for the used meter.

If the meter NeTraMet [RFC2123] is used, the policy is converted into a NeTraMet ruleset that contains the relevant flows, attributes and reader instructions for the data collection. This information is passed to the NeTraMet manager that configures the meter and meter reader in accordance with the given configuration.

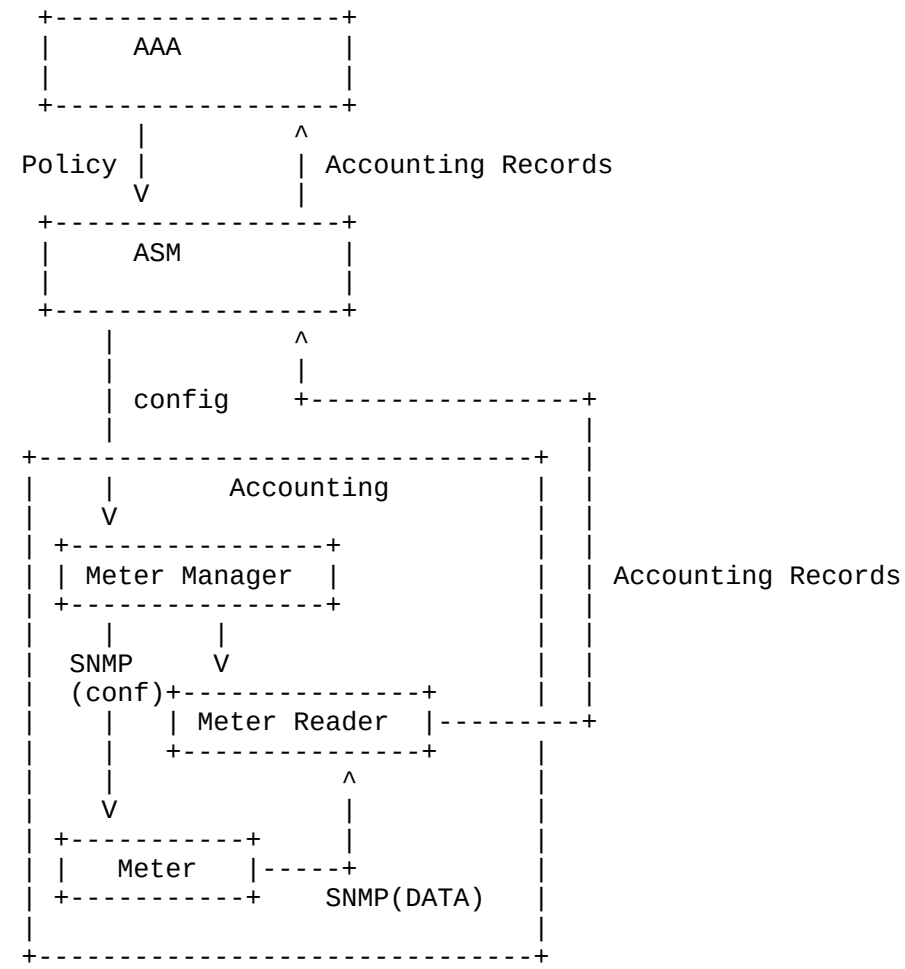

Figure 3: Policy based Accounting with NeTraMet

If the meter NetFlow [NetFlow] is used, the meter policies are translated by the ASM into filter instructions for the flow collector. The meter itself is static and therefore is not affected by the configuration information.

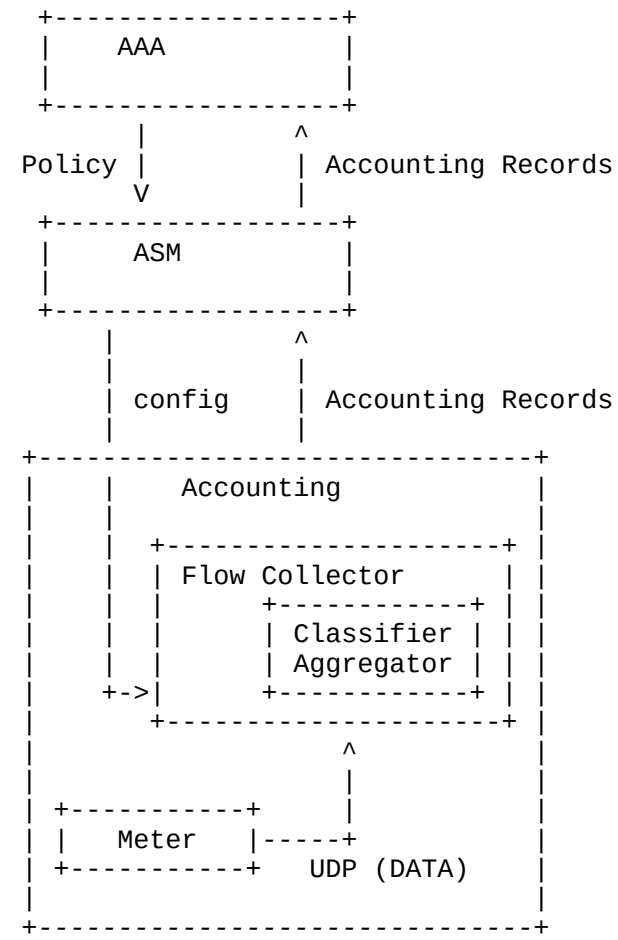

Figure 4: Policy based Accounting with NetFlow

7. Accounting Services

Accounting can be seen as part of the service provisioning process (integrated accounting) or as a separate service (discrete accounting). The different views and their impact on the accounting architecture are described below.

7.1 Integrated Accounting

In the integrated accounting model, the accounting is seen as part of the provisioned service. That means the accounting is coupled with a specific service. Therefore, the accounting process is tailored to the specific service and might collect accounting information by

directly exploiting some service specific entities. For example, accounting for IP telephony could use call signaling information from a SIP server. The configuration of the accounting architecture is done as part of the user configuration of the service equipment. Accounting policies are defined as part of the contractual agreement. The ASM converts the instructions from the AAA server into the appropriate user configuration including settings for the accounting architecture.

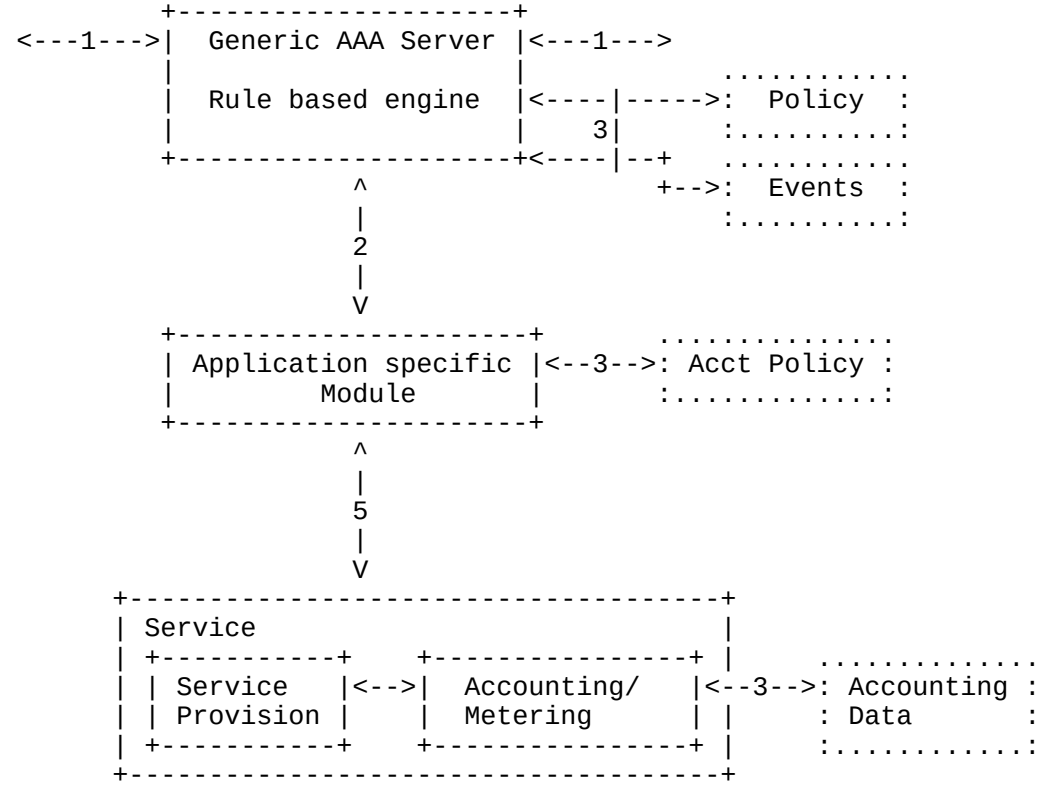

Figure 5: AAA Server with Integrated Accounting

Data about the resource consumption is sent back to the AAA server via the ASM. The accounting process within the service converts the metered data into accounting records which are sent to the AAA server. For generating accounting records data conversion, aggregation and filtering of data might be performed.

7.2 Discrete Accounting

In contrast to the integrated accounting approach, accounting can also be seen as a separate or discrete service on its own. In this case the accounting does not have to be coupled with a specific service. Discrete Accounting can be used for outsourcing the accounting task. The accounting service can be provided by a general accounting system which is able to account for different services.

For example, a generalized meter can do accounting for web traffic, FTP traffic and voice over IP traffic. If accounting is a separate service, one provider can do the accounting (charging and billing) for several other service providers. Accounting is offered just like any other service. This means authentication and authorization might be required prior to the accounting service provisioning. Furthermore, it is important that the involved parties agree beforehand how the accounting service is provided, what parameters can be set and how disputes will be resolved. After the accounting service has been configured, the AAA server can do the user configuration of the service.

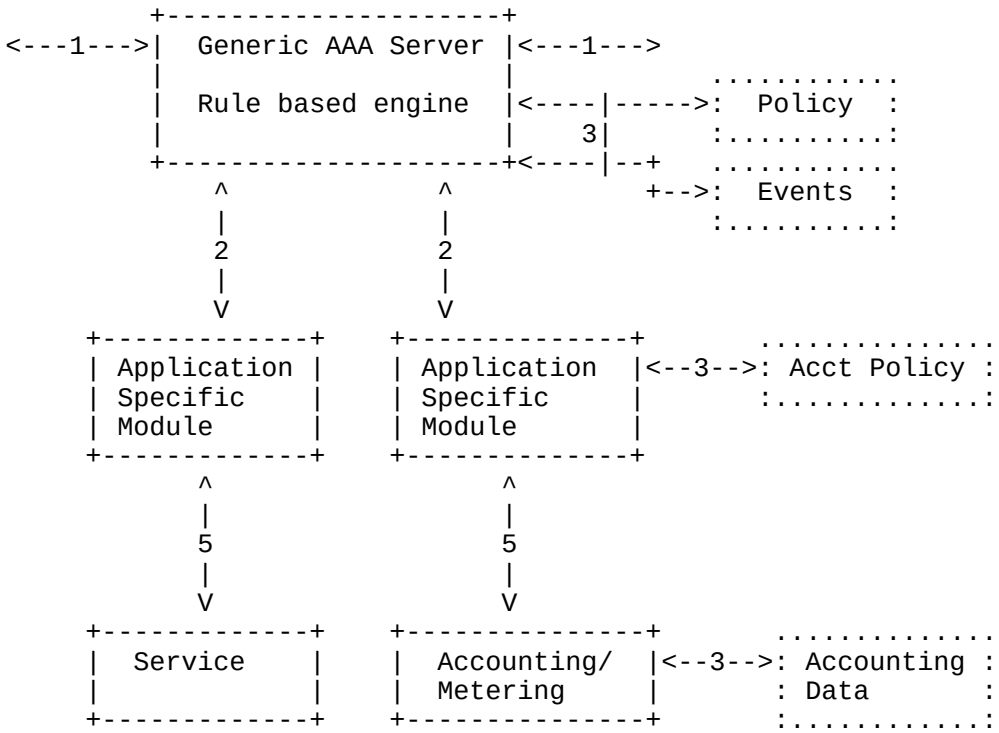

Figure 6: AAA Server with Discrete Accounting

A service provider that has outsourced the accounting service has to request this service from an accounting service provider. The generated accounting records are sent from the accounting provider to the service provider who may make modifications to the records before sending them to the final destination. Having such a general accounting service might speed up the creation of new services - especially specialized content services - in the Internet. This separation is also beneficial to support special accounting services (e.g. sending accounting indications to users) that are not directly coupled to a network service. Furthermore, this separation is useful if the same set of accounting strategies can be applied to different services (e.g. different tariffs which can be used for a set of services).

Another option is to outsource only the metering service. The meter service provider generates meter data and sends them to the service provider who has requested them. The service provider then generates accounting records based on the received meter data. A separate accounting or metering service provider can be used to validate the accounting data generated by a service provider. If the customer does not trust a service provider, or in the case of a legal action, a trusted accounting or metering provider is able to validate the correctness of the accounting data generated by the service provider.

7.3 Intra-Domain Accounting

In Intra-Domain accounting [RFC2975], the data about resource consumption is collected in one administrative domain for usage in that domain. Accounting policies are enforced locally. Since no exchange of accounting data with other domains is required in this scenario, accounting policies do not need to be exchanged with other entities.

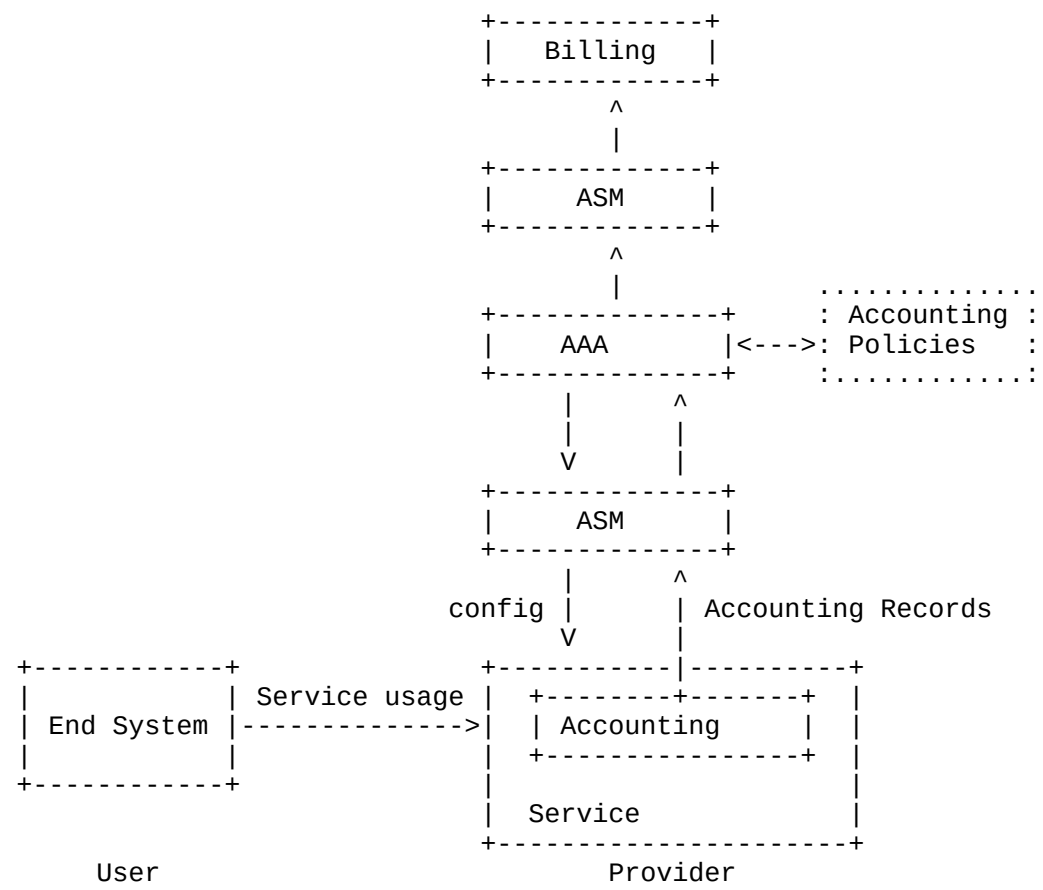

Figure 7: Intra-Domain Accounting

7.4 Inter-Domain Accounting

For Inter-Domain Accounting, at least two administratively separated networks are involved in the accounting process. These can be a Home- and a Foreign-Provider in a Roaming/Mobile IP Scenario [RFC2002] or a chain of providers if service provisioning involves data transfer and/or services from different domains. In these scenarios, the exchange of accounting policies between providers is necessary if accounting tasks are delegated to one provider or shared among multiple providers. The exchange of accounting policies is done by the AAA servers as shown in the figure below.

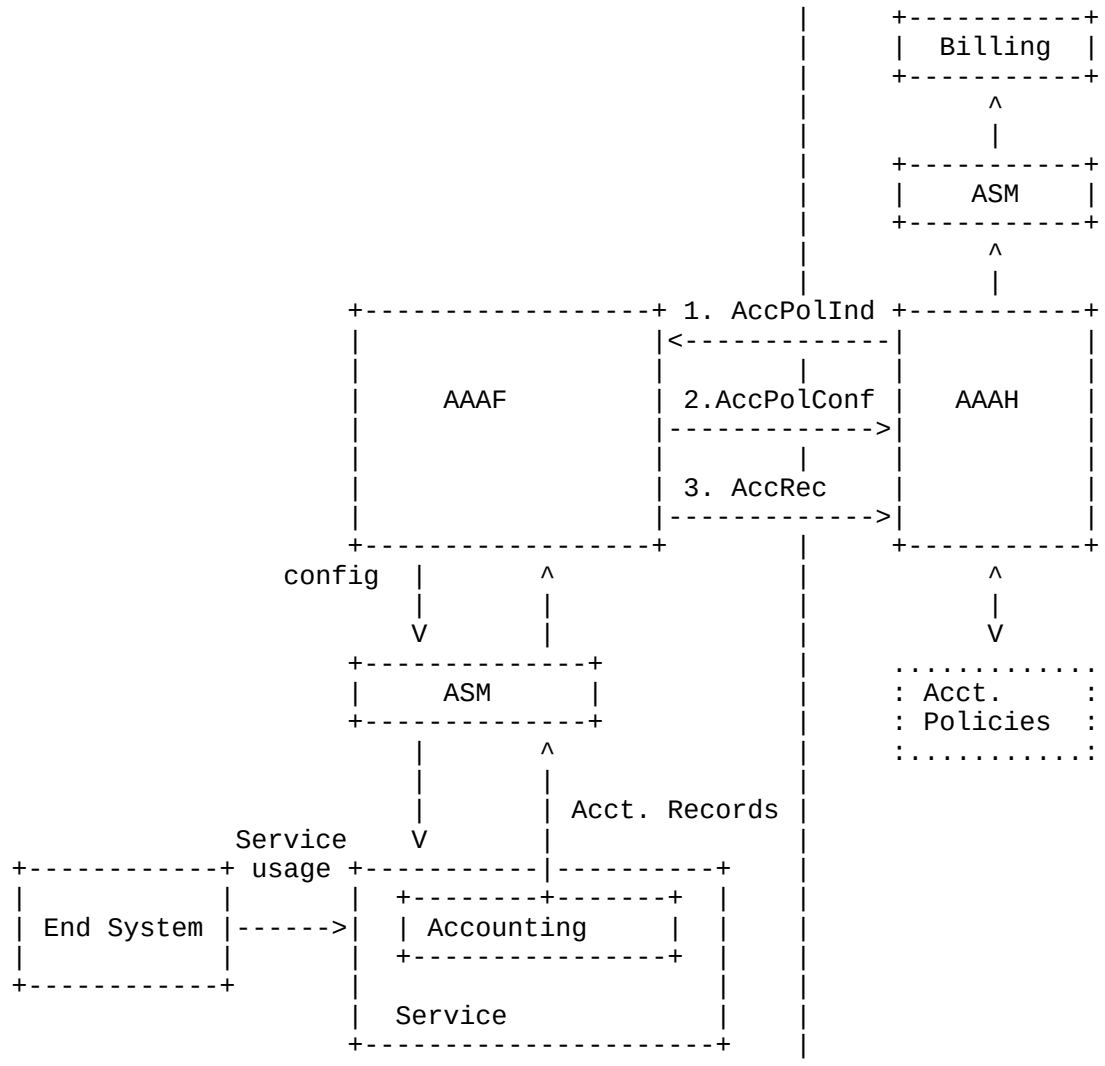

Figure 8: Inter-Domain Accounting (Roaming Example)

In this example, the foreign provider takes over the collection of accounting data. The home provider is responsible for applying a charging scheme and sending the bill. Therefore, the home provider needs accounting data from the foreign provider. In order to instruct the foreign provider about the desired accounting record type and report frequency, the home AAA server sends an accounting policy indication to the foreign AAA server. The indication contains

the accounting policy. Instead of sending an indication, the accounting policies could also be piggy backed onto an authorization reply. If the foreign AAA server is able to configure devices in a way to enforce the desired policy (e.g. the meters are capable of metering the requested attributes) the accounting policy indication is acknowledged. In case the requested policy cannot be enforced, the accounting service is denied. Reasons to deny the enforcement of a specific accounting policy could be, e.g. because the meter is not capable of measuring the requested attributes or the frequency of records cannot be provided, or the home provider is not authorized to get the requested detailed data. In this case procedures would be useful to negotiate the smallest common denominator for the involved AAA servers regarding the provisioning of accounting data.

8. Accounting with different Authorization Models

The AAA authorization framework [RFC2904] introduces different message sequences for authorization. The integration of configurable accounting services for the message sequences can be done as described in the following sections.

8.1 Agent Sequence

The appropriate accounting policy for the authorized service is either stored together with the authorization policy or in a separate repository. The configuration of the accounting infrastructure can be done together with the user configuration of the service equipment (messages 2 and 3 in Figure 9). User-specific configuration of the service equipment and the accounting infrastructure configuration might involve the transfer of configuration data to multiple entities in the network (e.g. to different routers for setting up QoS provisioning or to dedicated accounting meters).

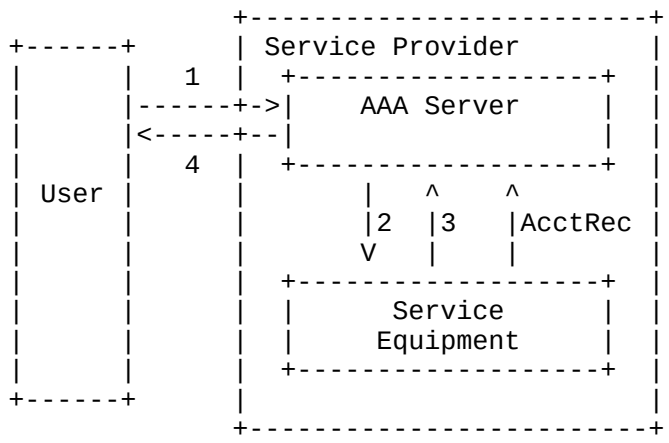

Figure 9: Accounting and Agent Sequence

In the agent sequence, it is possible to allow the user to send accounting policies (e.g. for accounting indications) together with the authorization request to the AAA server. Figure 9 shows the agent sequence authorization and accounting messages.

8.2 Pull Sequence

The configuration of the accounting infrastructure can be done similar to the agent sequence during the user configuration of the service equipment. Since the pull sequence does not involve the sending of a specific authorization request (e.g. if the service equipment is a Network Access Server (NAS) and the authorization sequence simply starts with the dial-in process), it would need additional communication to support accounting policy indications from users.

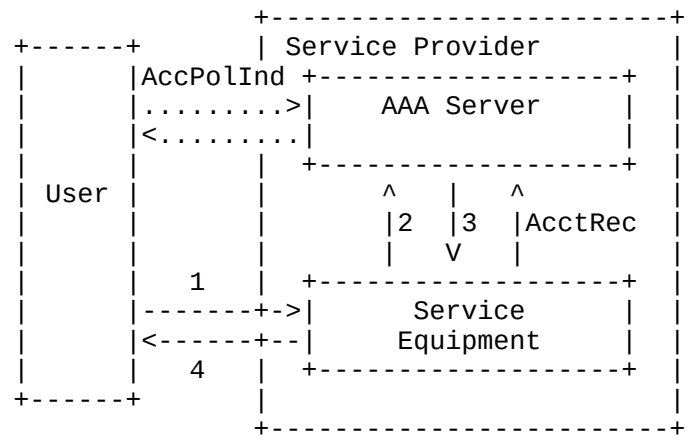

Figure 10: Accounting and Pull Sequence

This can be, for instance, achieved by a hybrid model of agent and pull sequence where the user sends an accounting policy indication to the AAA server in addition to the messages exchange for the pull sequence. Figure 10 shows the pull sequence authorization and accounting messages.

8.3 Push Sequence

In the push sequence, there is no direct connection between the AAA server and the service equipment. In this sequence there are three possibilities for setting up the accounting infrastructure:

a) A standard fixed accounting procedure that has been assigned in advance for the specific combination of authorized user and service is used.

b) The ticket (message 3 in Figure 11) contains information about the accounting policies used (e.g. different tickets for the same service with different accounting policies).

c) The ticket acts as a kind of digital coin and no further accounting is needed. This model also supports the anonymous usage of a service.

Figure 11 shows push sequence authorization and accounting messages.

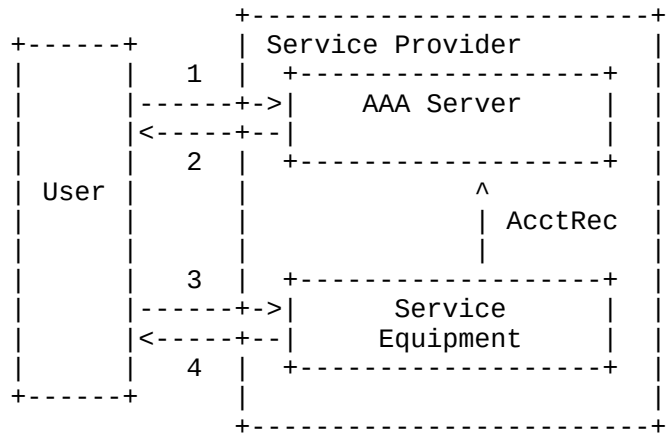

Figure 11: Accounting and Push Sequence

8.4 Roaming

If the provisioning of the service and the final authentication/ authorization process is done by different organizations, accounting is rather coupled to the service provisioning process than to the authentication/authorization process. Since the data doesn't have to traverse the home providers network, the home provider has no possibility of collecting data about the resource consumption. Therefore, accounting will usually take place in the foreign provider domain (i.e. in the domain that does the service provisioning). Nevertheless, in order to ensure consistency of the authentication, authorization and accounting processes (e.g. allocation of user IDs to accounting records) and the production of a bill, a connection between the accounting process in the service provisioning domain and the deciding authentication/authorization process (e.g. at the home provider) is needed.

A possible way of doing this is if the foreign provider gets the accounting policies from the home provider and sets up the accounting architecture in accordance to the given policies, the foreign provider can generate accounting records and send them back to the home provider. The home provider then can apply charging and can produce a bill. An example for this is given in section 9.2. This scenario requires a prior agreement between the involved providers about the possible policies and parameters that are allowed to be set.

9. Examples

The following examples illustrate the use of policy-based accounting. Please note that the services used in the examples are used only for illustration purposes and their use in reality requires different messages and parameters.

9.1 Printing Service Example

The Internet Printing Protocol (IPP) [RFC2566], and especially the "print-by-reference" model, provides a very interesting example scenario for accounting and the interaction between authorization and accounting. We will describe possible solutions for the accounting of this service and how the accounting is triggered by the authorization. We will show how the model presented above can be used for this example.

IPP "print-by-reference" allows a user to request a print service to print a particular file. The file to be printed is not on the client system but rather on a public server. That is, the clients print request can contain a reference, or pointer, to the document instead of the actual document itself. The print service must then read the file to a file server (used for spooling) prior to the printing. There are two possible setups: The file and print server either belong to a single organization (Intra-Domain Accounting) or to two different organizations (Inter-Domain Accounting). In the first case, the user must be authorized by a single service provider for service usage. In the second case, two different possibilities for establishing a trust relationships between the involved entities have to be distinguished [RFC2905].

9.1.1 Intra-Domain Accounting

In the case of a single organization, the file and print service is provided by a single service provider. The service subscriber and user role are either one entity (e.g. private home user) or different entities (e.g. company as subscriber, employee as user). For data transport via the underlying network, the transportation service of a network provider is used. In this case, the AAA server of the provider controls the access to the file and the print server. This means the AAA server enforces the accounting policies and collects accounting data for both servers.

9.1.2 Inter-Domain Accounting

If two different organizations are involved there are two possibilities for trust relationships as shown in [RFC2905]:

1. The user has an agreement with the print server; the print server has an agreement with the file server.
2. The user has agreements with both print and file server.

In case 1, the user is first authorized by the print service and the request is forwarded to the file server. The file server authorizes the print server and determines if the printer is allowed to access the file. In this case which is shown in Figure 12, the accounting policies from the user arrive at the print service AAA server.

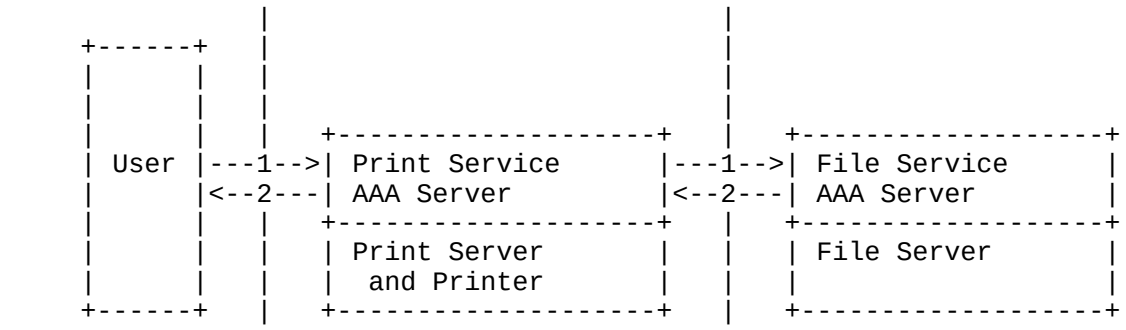

Figure 12: Inter-Domain Accounting and Printing Service

The print service AAA server has to decide which policies can be enforced locally and which must be passed further to the file service AAA server. The print service can add additional accounting policies. In case the file server does not support the desired accounting policies, the print server must notify the user's AAA server and some policy conflict resolution must occur. After the file server has transferred the file to the print service, it generates an accounting record according to the accounting policy and passes it to the print service. The print service generates the final accounting record for the service session based on its own and the file service data after finishing printing. This record will be used for the later billing process. Additionally, the print server can send the final record to the user's AAA server. There it can be used for later authorization decisions based on used resources, i.e. if the customer is a company and the user is an employee.

In case 2, the customer AAA server has an agreement with file and print server. In this case, the user's AAA server sends accounting policies to the file and the print server. After finishing the service, both servers generate accounting records for the delivered services which are used for later billing. As in the former case, the accounting data can be sent to the user's AAA server for use in later authorization decisions. The user's AAA server can tie both accounting records together and assign them to the user using audited session information (authorization and accounting messages for a particular session could be coupled via a session ID) and policies that define which activities a certain session is composed of.

9.1.3 User Accounting Indication

For the printing service, there are a number of possible options for sending accounting indications to the user. Accounting indications give the user an indication of how much resources have been used until the time of the indication. A user can receive accounting indications or not depending on the accounting policy for the user.

For Internet printing with the "print-by-reference" model, such indications would be very helpful for the user. Since the file is not on the clients site, the user might not have information on the file size or the number of pages that will be printed. This means the user has no idea of the costs of the service usage. If user and subscriber are a single entity, accounting indications would help users to avoid exceeding their spending limit. Additionally, accounting indications give the user a hint as to which resource usage has caused the charges. This can be compared to an itemized telephony bill where not only the monetary sum per month is printed but, in addition, information for every call (start time, duration, distance etc.) and its corresponding charge.

9.2 Mobile/Roaming Example

In this section, the "Dial-in with Roaming" example from the authorization examples [RFC2905], [RFC2002] is used to show how accounting functions could interact with authorization functions. The accounting modules (e.g. collectors and meters) are seen here as part of the service equipment which is, in this example, located at the visited ISP premises. The basic configuration of the accounting modules is probably done by the visited ISP itself, but the visited ISP can allow the home ISP to influence certain parameters (like report interval or accounting record format). This is useful if the home provider generates the invoice and therefore needs appropriate accounting records to calculate the prices.

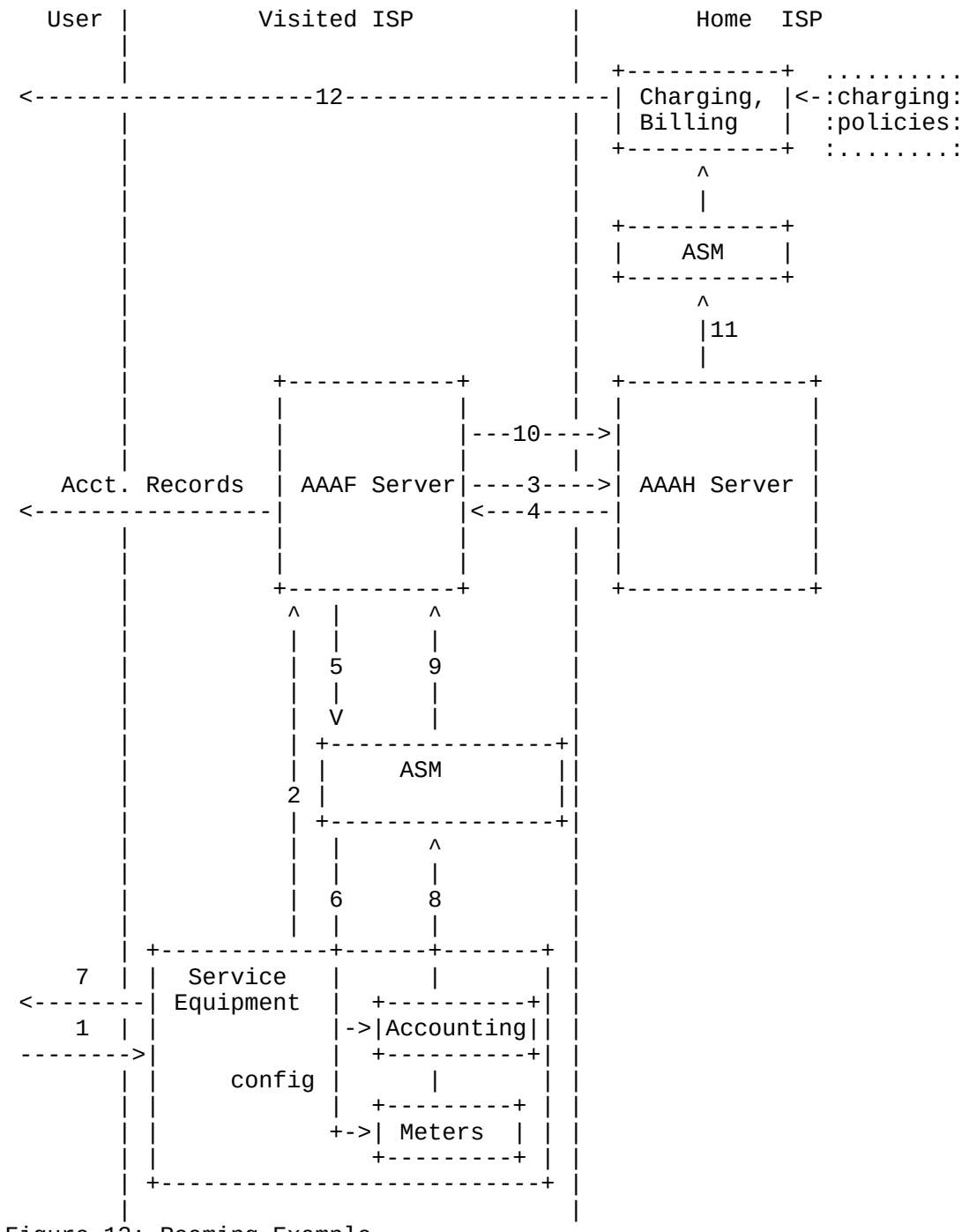

Figure 13: Roaming Example

The exchange of authorization data corresponds to the example in [RFC2905]. As an additional component, we introduce an ASM between home AAA and service equipment for the user configuration which happens after successful authorization. The extended roaming example is shown in Figure 13. Steps (1), (2) and (3) describe the forwarding of an authentication/authorization request from the user via the AAA sever of the visited ISP to the home AAA server. In step (4), user specific service parameters are given to the visited ISP's AAA server and are forwarded to the service equipment (5) where the user configuration is done. The user-specific service parameters could additionally include the desired policies for the configuration of the accounting infrastructure of the visited ISP. An accounting policy could be, for instance, "for user X one accounting record of type Y has to be generated every 30 seconds". This accounting policy is used by the visited ISP to configure his modules (e.g. metering, data collection).

User-dependent service parameters are converted by the ASM into the appropriate configuration information (6). Then the user is informed about the completed authentication/authorization process (7). The accounting architecture starts metering the resource usage and sends metering records to the ASM (8). The ASM uses the metered data to fill the required accounting records and sends them to the visited ISP's AAA server (9). The visited ISP can either post-process the data or directly forward them to the home ISP (10). With this data as input, an invoice is generated by the charging and billing modules within the home providers domain (11) by using charging policies (tariff formulas), and then sent to the user/customer (12).

As an additional option, accounting records can also be offered to the user (accounting indication) as a special service. For this special service a separate authorization is required.

9.3 Diffserv Example

This example explains how integrated accounting is configured via policies for a Diffserv service [RFC2475] based on bandwidth brokers [I2-BB]. The service is the transport of packets with a higher priority and the service includes accounting and QoS auditing. Figure 14 shows the service setup. The user issues a Service Request (SR) for a Diffserv service to the AAA server. The request contains a user ID and the parameter for the desired service class.

```
User->AAA: user-x@nw-a, service=diffserv, class=gold,
           amount=2Mbit, dest= nw-b
```

In this example, user-x is located at network A (nw-a) and requests a gold class service for all flows from this network to the destination network B (nw-b). After authentication and authorization has been completed successfully, the AAA server extracts the ASI from the request and passes them to the ASM of the Diffserv service.

```
AAA->ASM: service=diffserv, class=gold, amount=2Mbit, src=nw-a
          dest=nw-b
```

The ASM takes over the task of translating the application specific information into appropriate user configuration information for the service equipment. For the given Diffserv example, the service equipment consists of three components: accounting equipment, the QoS auditing equipment and the bandwidth broker architecture. The ASM has to address all three components to set up the requested service for the user. The translation of the ASI into configuration information for the components can be done by evaluating service provisioning policies. For example, the ASM could have the following service provisioning policy:

```
if class==gold {
  set bw-request.class = gold
  set accounting.type = comprehensive
  set qos-audit.metric = one-way-delay
  ...
}
```

This results in sending a bandwidth request to the BB which asks for a gold service with the given parameters. Furthermore, the ASM issues a request to the accounting equipment for comprehensive accounting and a request to the QoS auditing equipment for a one-way-delay measurement between the given networks.

```
ASM->BB: BW-request(gold, src=nw-a, dest=nw-b, amount=2Mbit)

ASM->Acct: Acct-request(comprehensive, src=nw-a)

ASM->QoS: QoS-audit-request(one-way-delay, src=nw-a, dest=nw-b)
```

The bandwidth broker then sets up the Diffserv infrastructure to provide the prioritized forwarding according to the definition of a gold class. This is done in accordance with the actual bandwidth broker's architecture and is not further considered here. For the Accounting Configuration and the QoS Audit Control, local configuration policies exist for setting up the service.

```
Accounting-Policy:
          if type==comprehensive {
            set meter-location = access-point(nw-a)
            set record type =detailed
            set report interval = 120 s
            set report target = 193.175.12.8
            ^ indent of last two lines
           }

QoS-Measurement-Policy:
            if metric==one-way-delay {
              set method = passive
              set timestampsize = 48 bit
              set ingress-meter-location = access-point(nw-a)
              set egress-meter-location = access-point(nw-b)
             }
```

In this case, the local accounting policy sets the meter location to the network access point of network A. It states that for comprehensive accounting, a detailed record type is required with a report interval of 120 s. The resulting records have to be sent to the given report target. The QoS measurement policy sets the measurement method to passive measurement. It sets the size used for timestamp representation to 48 bits. As meter locations, the meters at the access points of network A and network B are used.

After evaluating these policies, the instructions for the meter configuration are passed down to the measurement infrastructure. In our example, the accounting configuration instructs the meter at the first measurement point (MP1) to add a new rule with the given flow attributes and settings for storage and reporting of results.

```
   Acct->MI: MP1: add rule dscp=23, src=a.a.a/24, dest=b.b.b.b/24
                  save volume
                  set report interval = 120 s
                  set report target = 193.175.12.8
```

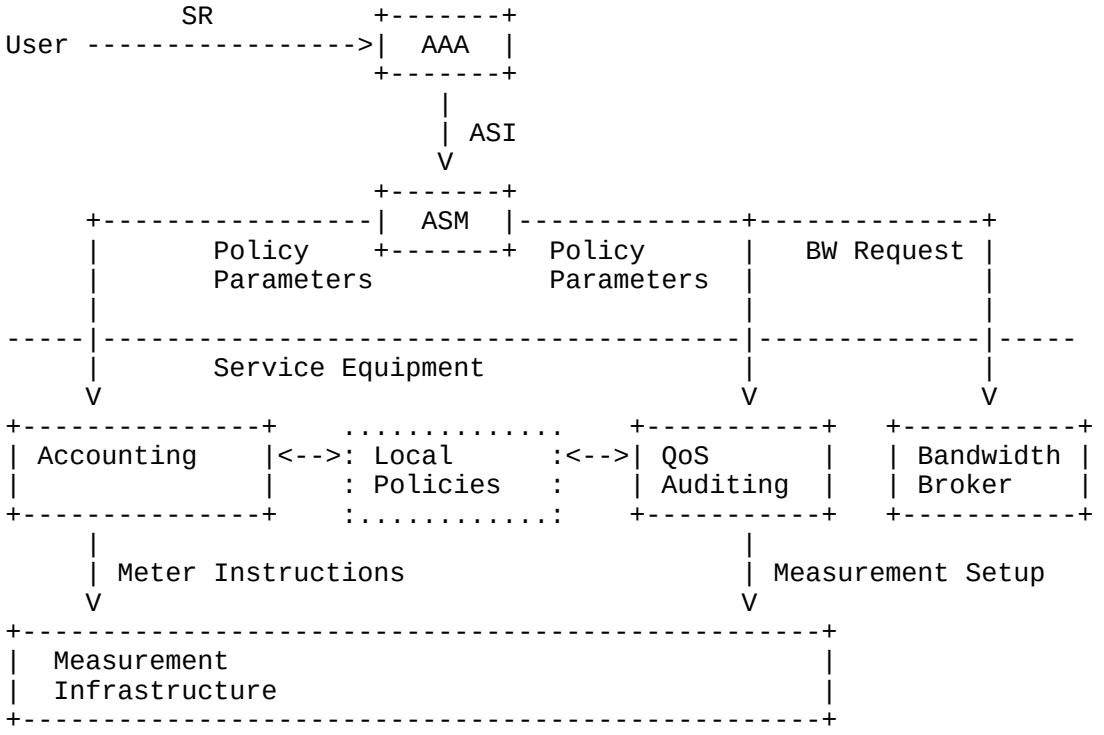

Figure 14: Diffserv Service Provision Setup

The QoS audit control instructs two meters (at MP1 and MP2) to set up a passive one-way-delay measurement.

```
   QoS->MI: MP1: add rule dscp=23, src=a.a.a.a/24 dest=b.b.b.b/24,
                 save timestamp-48
            MP2: add rule dscp=23, src=a.a.a.a/24, dest=b.b.b.b/24,
                 save timestamp-48
```

9.4 User Accounting Indication Example

This example explains how discrete accounting can be used to provide accounting indications for the user. Accounting indications are sent to the user in order to inform the user about current resource consumption. The accounting indication is a special accounting service that can be provided in addition to the standard accounting performed by the provider. Like for any other service, an authorization should take place before the accounting indication service provisioning. Therefore, the accounting here is seen as a separate service. That means the accounting service is independent of the main service and therefore can be applied to different services. It might be used as an addition to an integrated accounting that is part of the service. The authorization process for the accounting service is out of the scope of this document and therefore is not further explained here.

Figure 15 illustrates the configuration message sequence for setting up the accounting service. First, the user sends an Accounting Service Request (ASR) to the AAA server which includes desired parameters for the provisioning of the accounting service (e.g. report interval).

```
user->AAA: user-x@nw-a, service= accounting indications,
           report interval= 60 s
```

The AAA server passes the ASI to the ASM of the accounting service after the user has been authenticated and authorized for the service usage.

```
AAA->ASM: user-x@nw-a, service=accounting indications,
          report interval= 60 s
```

The ASM generates an accounting policy based on the ASI and passes this policy to the Accounting Configuration.

```
ASM->Acct: If src=a.a.a.x {
             acc-indication = on
             report interval = 60s
             report target= a.a.a.x
           }
```

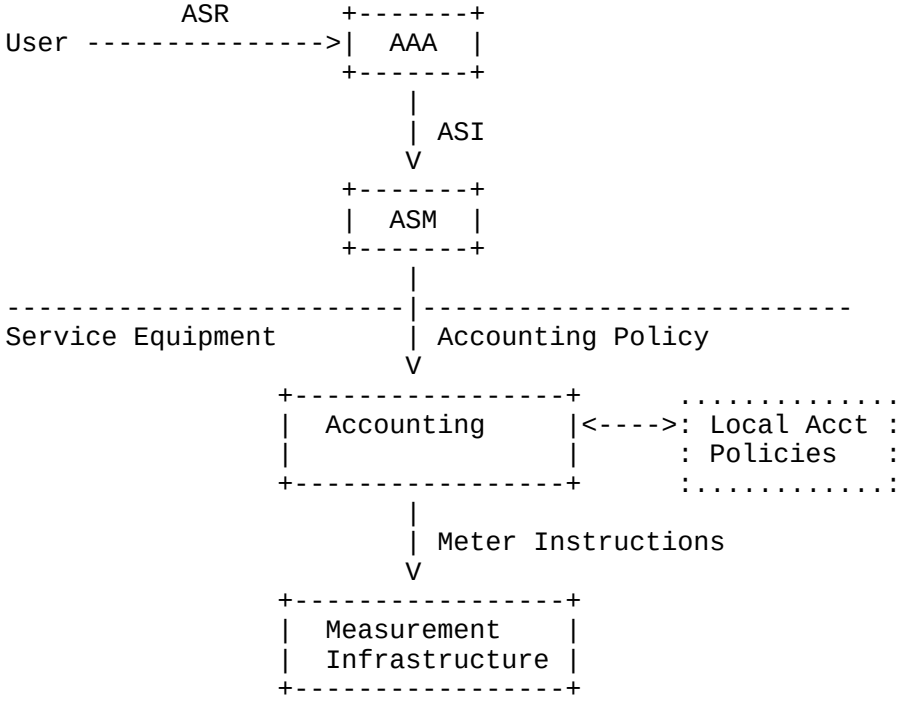

Figure 15: Accounting Indication Configuration

The Accounting Configuration generates meter instructions according to the accounting policies from the ASM and local accounting policies and passes them to the measurement infrastructure.

```
   local Acct-Policy: if acc-indication {
                       record type = compact
                      }

   Acct->MI: MP1: set report interval = 60 s
                  add report target = a.a.a.x
```

10. Security Considerations

Accounting services provide the basis for billing. Therefore, the incentives (mainly saving money) and potential for fraud is extremely high in the field of configuration of the accounting architecture and the collection of accounting data. In the presented framework, two types of data communications are required, the exchange of accounting policies and the collection of accounting records. Both communications introduce potential security hazards.

The following potential security hazards can be identified:

- Forgery of accounting policies and accounting record information
Both accounting policies and accounting records can be the target of forgery of information. Accounting policies contain configuration information. Modifying this information can lead to a mal-configured accounting and metering system which either allows data to traverse the accounting system undetected (without being accounted for, e.g. by changing the classification rules of a meter) or produces bogus accounting records. Accounting records contain data about resource consumption and provide the basis for billing. Modifying accounting records may lead to erroneous bills. Furthermore, it is important that policies or accounting records are not redirected or removed and that forged policies or records are not inserted.

- Eavesdropping
It may be required to keep accounting policies and accounting records confidential between the involved parties.

- Denial of Service (DoS) attacks
Both the AAA server and the accounting/metering subsystem can be the target of denial of service attacks. A denial of service attack against the AAA server may lead to malfunction and even breakdown of the server. This means the server will not be able to provide proper authentication, authorization and accounting functionality. The service provided by the AAA server will become unavailable or unusable. An attack to the server can be worse than an attack to the service equipment itself, especially if multiple services use one AAA server. An attack against the accounting/metering system will cause loss of metering data and/or loss of accounting records.

This leads to the following security requirements:

- Secrecy of accounting policies and accounting data
Unauthorized entities should not be able to read or modify accounting policies or accounting records. This can be achieved with standard encryption methods.

- Authentication of accounting data and accounting policy sources
It should be ensured that the data is originated by the original source. Source-authentication can be achieved by using digital signatures.

- Protection of the integrity of accounting policies and records
It should be ensured that the data was not modified on the way from sender to receiver. Data-authentication can also be achieved with digital signatures.

- Verify correctness of generated accounting data
It must be ensured that the accounting data generated by the service provider is correct. A provider may generate incorrect accounting records either deliberately (i.e. forging) or unintentionally (e.g. faulty configuration). These incorrect accounting records probably have the consequence of incorrect bills. Customers can verify the correctness of the accounting data through their measurements and/or through data collected by a trusted third party. A trusted third party can be an independent accounting service provider as described in section 7.2 or a more general entity providing an auditing service.

- Prevention and protection against Denial of Service attacks
The AAA protocol and all building blocks should be designed and implemented in a way as resistant as possible to denial of service attacks. An additional strategy to defend against DoS attacks is to add a component to the meter system that is able to detect suspicious traffic patterns. Upon detection, further actions can be taken according to a pre-defined policy.

The prevention of these hazards has to be considered for the protocols used for accounting policy exchange and the transportation of accounting records. Since the security requirements for authentication, transmission level security, data object confidentiality and integrity are addressed in the criteria for AAA protocol evaluation [RFC2989], we assume that the future AAA protocol(s) will be suited for secure accounting record transfer and probably also for secure accounting policy transport. Furthermore, we assume that existing or upcoming solutions for secure transportation and enforcement of policies can be used. Real prevention of DoS attacks is quite difficult. A selective dropping of the attackers packets is impossible if the malicious packets cannot be separated from the valid customer traffic. Dropping of all packets of a certain type may prevent authorized customers from using the service and therefore help the attacker to achieve her goal.

11. References

[I2-BB] Internet2-QBone Bandwidth Broker, http://www.merit.edu/working.groups/i2-qbone-bb

[NetFlow] NetFlow Services and Applications, White Paper, Cisco Systems, 1999

[RFC2002] Perkins, C., "IP Mobility Support", RFC 3220, October 1996.

[RFC2123] Brownlee, N., "Traffic Flow Measurement: Experiences with NeTraMet", RFC 2123, March 1997.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang Z. and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.

[RFC2566] DeBry, R., "Internet Printing Protocol/1.0: Model and Semantics", RFC 2911, April 1999.

[RFC2722] Brownlee, N., Mills, C. and G. Ruth, "Traffic Flow Measurement: Architecture", RFC 2722, October 1999.

[RFC2903] de Laat, C., Gross, G., Gommans, L., Vollbrecht, J. and D. Spence, "Generic AAA Architecture", RFC 2903, August 2000.

[RFC2904] Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M. and D. Spence, "AAA Authorization Framework", RFC 2904, August 2000.

[RFC2905] Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M. and D. Spence, "AAA Authorization Application Examples", RFC 2905, August 2000.

[RFC2924] Brownlee, N. and A. Blount, "Accounting Attributes and Record Formats", RFC 2924, September 2000.

[RFC2975] Aboba, B., Arkko, J. and D. Harrington, "Introduction to Accounting Management", RFC 2975, October 2000.

[RFC2989] Aboba, B., Calhoun, P., Glass, S., Hiller, T., McCann, P., Shiino, H., Walsh, P., Zorn, G., Dommety, G., Perkins, C., Patil, B., Mitton, D., Manning, S., Beadles, M., Chen, X., Sivalingham, S., Hameed, A., Munson, M., Jacobs, S., Lim, B., Hirschman, B., Hsu, R., Koo, H., Lipford, M., Campbell, E., Xu, Y., Baba, S. and E. Jaques, "Criteria for Evaluating AAA Protocols for Network Access", RFC 2989, November 2000.

[RFC3198] Westerinen, A., Schnizlein, J., Strassner, J., Scherling, M., Quinn, B., Herzog, S., Huynh, A., Carlson, M., Perry, J. and S. Waldbusser, "Terminology for Policy-Based Management", RFC 3198, November 2001.

12. Acknowledgments

The authors would like to thank the members of the AAAARCH research group and in particular, the chairs, John Vollbrecht and Cees de Laat, for the fruitful discussions and comments. Special thanks are to Bernard Aboba, Nevil Brownlee and Ed Ellesson for their review and valuable input to this document.

Author's Addresses

Tanja Zseby
Fraunhofer Institute for Open Communication Systems
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany
Phone: +49-30-34 63 7153
Fax: +49-30-34 53 8153
EMail: zseby@fokus.fhg.de

Sebastian Zander
Fraunhofer Institute for Open Communication Systems
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany
Phone: +49-30-34 63 7287
Fax: +49-30-34 63 8287
EMail: zander@fokus.fhg.de

Georg Carle
Fraunhofer Institute for Open Communication Systems
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany
Phone: +49-30-34 63 7149
Fax: +49-30-34 63 8149
EMail: carle@fokus.fhg.de

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.