Design and Implementation of a Charging and Accounting Architecture for Secure VPN Services to Mobile Users[*]

Thanasis G. Papaioannou and George D. Stamoulis

Department of Informatics, Athens University of Economics and Business (AUEB), Patision 76,
10434 Athens, Greece.
{pathan, gstamoul}@aueb.gr

Abstract

In the emerging context of mobile Internet, Secure VPN is becoming a very important service. Provision of this problem is among the subjects of IST project INTERNODE. Besides provision of the necessary technical means, charging and accounting also are key related issues. These issues are the subject of this paper. Only by dealing with them successfully, Secure VPN providers can recover their provision costs, increase their profits, and provide the right incentives to their users, thus leading to an efficient operating mode of their network. In this paper, we first define a charging scheme that is fair for the users and provides them with the incentives to use the resources they really need. We then show how the contributing providers can share the total charge earned by each service instance in a fair way, with each provider earning the portion of charge that corresponds to the consumption of his own resources for the service. This is also a very important issue for the commercial viability of Secure VPN service, given that its provision spans multiple domains. Furthermore, we define an appropriate charging and accounting architecture implementing the specified charging scheme for Secure VPN, and the mechanism for revenue sharing. This architecture is compliant to the relevant standards and can serve as a basis for applying other charging schemes as well.

Keywords: security, VPN charging, mobile Internet, accounting architecture

[*] The present work has been performed as a part of the IST project INTERNODE (IST-1999-20117), through subcontract with INTRACOM S.A. © Copyright the INTERNODE consortium: BYTEL, EI-NETC, GMD, BALTIMORE, CR2, INTRACOM, UPC.

1 Introduction

The globalization of commerce as well as the ease in human transportation has increased the mobility of professionals around the world. Also, in recent years the use of mobile phones has grown tremendously. The increased terminal capabilities as well as the development of a great number of SMS and WAP applications have brought the notion of mobile Internet into reality. In this new networking environment, mobile users need to retain seemless and secure connectivity, as if being at home domain. Also, mobile users should be able to form private working groups independently from their respective point of attachment to the Internet. These requirements are fulfilled with the provision of Secure VPN (S-VPN) services. Furthermore, S-VPN services should be customized in order to satisfy certain user preferences regarding levels of security and quality of service (QoS). On the other hand, S-VPN providers should account and charge for their services, in order to recover their provision costs, increase their profits, and provide the right incentives to their users, thus leading to an efficient operating mode of their network. The users should be provided with the right incentives to use as many network resources as they really need, while they should be charged in a fair way; i.e., pay exactly for the network resources they actually consume. Moreover, charge assigned to each instance of S-VPN provision should be shared among the providers involved in an efficient and fair way. In this paper, we present an accounting and charging architecture that applies to the case of providing S-VPN services to mobile users. We propose a proper charging scheme that satisfies the requirements discussed above. We also develop an accounting and charging architecture that implements the charging scheme and supports live accounting, transparent/opaque billing and pre-paid services. This work is part of the IST project INTERNODE [1], which studies among others the provision of customized S-VPN services to mobile users. The remainder of this paper is organized as follows: in Section 2, we describe the context of INTERNODE for providing S-VPN services to mobile users. In Section 3, we briefly describe the most relevant studies for charging and for accounting for IP services. In Section 4, we consider the business roles for providing S-VPN services w.r.t. accounting and charging. In Section 5, we discuss the charging issues for providing S-VPN services and the proposed charging scheme. In Section 6, we describe the proposed accounting and charging architecture. Finally, in Section 7, we give some concluding remarks together with issues for further study.

2 The Context: The INTERNODE Environment

In this section, we describe the context of IST project INTERNODE for providing S-VPN services to mobile users. INTERNODE designs, specifies and implements a platform, which will be used to create multi-domain S-VPN services for mobile users (e.g. E-business, mobile Internet and intranet access, personalized services, etc.) Specifically, VPN connectivity is handled by a VPN provider that owns a VPN Service Provisioning and Support Platform (SPS) capable among others of automatically configuring and managing the S-VPNs on behalf of the VPN subscribers. A customer subscribes to the VPN SPS and registers a number of mobile (end-) users to use his S-VPN services. Through the SPS platform the S-VPN provider:

- Allows for VPN access control, ensuring that only authorised users will make use of VPNs to authorised destinations.
- Collects accounting information and performs the subsequent charging on the basis of the customer SLA.
- Manages and automatically configures the VPN termination points, so as to provide the security level end-to-end. INTERNODE assumes that the home and visited domains are trusted, and thus the security level has to be provided on a gateway-to-gateway basis (from the source network domain to the sink network domain).
- Co-operates with connectivity providers (CPs) through federated APIs so as to guarantee QoS declared in the SLAs for the S-VPN customers and share charging information. Note that all have to apply the security and mobility support technologies adpted by the S-VPN provider. Therefore, we assume that upon such federation agreements, the VPN SPS leases to the aforementioned CPs a Security Gateway (SG), and an enhanced router supporting mobility; i.e., the Home Agent (HA) or the Foreign Agent (FA) respectively. SG and HA/FA are used as *mediation* devices by the federated CPs, in order to associate resource usage to particular users (and thus to customers), support the mobility and security features of the VPN services, and check the conformance with the SLAs that the VPN SPS has established with its customers.

The traffic generated by a mobile user is forwarded via his access network to the appropriate gateway of the S-VPN provider. The gateway, which has to be configured by the VPN SPS, applies security procedures and then routes traffic to the selected destination SG; this de-capsulates the packet and forwards it to its final destination. The mobile user may change his point of attachment. In that case, the co-operation of the SPS platform and Mobile IP [2] infrastructure is activated and the new point of user's attachment is forwarded to the SPS. Figure 1 below shows the entities involved in the activation of S-VPN for a mobile user.

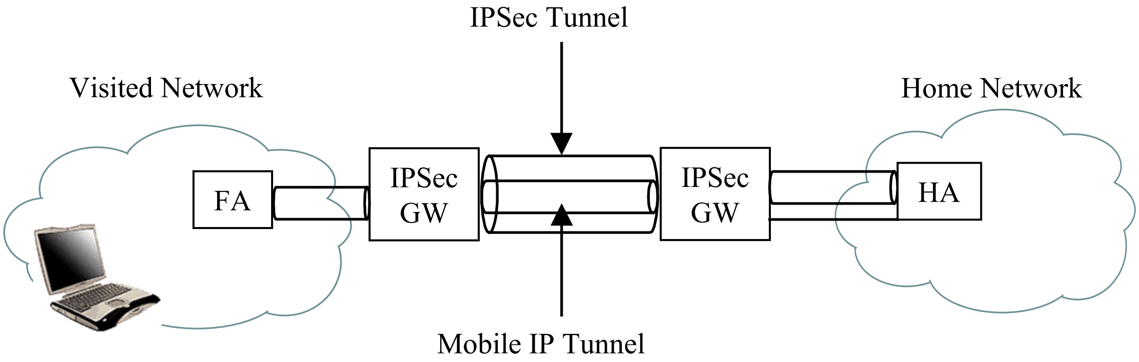


Figure 1: S-VPN provision to a mobile user from a Visited Domain to a VPN Destination.

From a technical perspective, INTERNODE uses the IPsec protocol for providing security, and especially the tunnel approach i.e., each IP packet is encapsulated into a new one. QoS differentiation over IP networks can be supported by means of the Differentiated Services (DiffServ) architecture. This can be accomplished if the DS field of each internal packet is copied into the DS field of the external packet. Consequently, the QoS of the provided service depends on the DiffServ QoS class, on the encapsulation time and on the overhead (data and processing) induced by the IPsec encapsulation procedure. Also, it has to be noted that for a secure duplex end-to-end communication, the creation of two IPsec tunnels is necessary, i.e. one for each direction of the traffic between the sender and the receiver.

3 Background Material on Charging and Accounting

3.1 Charging

In this section, we present the most significant proposals for charging "traditional" (best-effort) and recent (DiffServ) point-to-point Internet services, as well as VPN services. The best-effort service provides no guarantees of performance to the transmitted traffic except for minimal losses if the source is elastic (i.e. adapts to flow control signals). The DiffServ architecture provides guaranteed performance differentiation to the transmitted traffic. Henceforth, the best-effort service will be referred to as "elastic", while the DiffServ services will be referred to as "guaranteed". For simplicity, in the discussion to follow we assume that DiffServ flows traverse only a single link. If this is not the case, then the charges should be summed over all links of the path.

3.1.1 Charging Guaranteed Point-to-Point Services

The on-off bound approach: Courcoubetis and Siris proposed in [3] the following scheme for charging DiffServ SLAs:

$$\begin{aligned} & c_i(x) = \bar{a}_i(x;m)p_iT \\ & \bar{a}_i(x;m) = \frac{1}{s_it_i}\log\left[1 + \frac{m}{H(t_i)}(e^{s_it_iH(t_i)} - 1)\right] \\ & H(t_i) = \min\{h, \rho + \beta/t_i\} \end{aligned} \tag{1}$$

x in the above formula is the SLA that conforms traffic to dual leaky-bucket conformance, one leaky-bucket bounding the peak rate with h and the other having parameters (ρ, β); $H(t)$ is the corresponding *effective peak rate*. $m \in [0, \rho]$ is the mean rate of the traffic to be induced by the source, and T is the duration of the flow for that QoS class. p_i is the price per unit of effective bandwidth $\bar{a}_i(x;m)$ for a QoS class i. s_i, t_i parameters are the *operating point* of a QoS class, i.e. the operating point of the link over which QoS class is implemented. In fact, $\bar{a}_i(x;m)$ is an upper bound on the *actual effective bandwidth* and corresponds to that of an on/off source. The actual effective bandwidth of a source is computed according to the so-called inf-sup formula, derived by means of Large Deviations techniques [3], and is a single parameter reflecting resource usage of a bursty source. As explained in [1], this charging scheme is fair (i.e. reflects actual usage), under certain conditions. Also, it gives the incentives to users to select SLAs that better match their actual needs.

The time-volume (a, b, c) approach: An important proposal due to Kelly [4] is that the charge of offering a guaranteed service should be a function of the initial contract, of the *prediction* of the user about his traffic, and of the traffic *actually* sent. The reason is that the network would like to use the information obtained both from the contract and the user prediction in order to assess if enough resources are available to satisfy its part of the contract for the new connection, while satisfying the contracts with the other on-going connections. Hence, a user should pay in the best case the exact cost of resource usage (if his initial prediction were accurate), and pay in the rest of the cases more than if he had given the accurate prediction. This extra amount compensates the network for its loss of revenue because of the effect of this deviation of the prediction in accepting new calls. When applied to a single connection, this yields a charge of the form

$$a*T + b*V + c = T*(a + b*M) + c \tag{2}$$

where T is the duration of the connection, V is the amount of traffic carried, $M = \frac{V}{T}$ is the actual mean rate, and the coefficients a, b, and c are selected by the user in call set-upfrom a set of offered network tariffs. Hence, through charging, the network provides users with the incentive to be as precise as possible in their traffic predictions, possibly by keeping statistics of past invocations of this service

Again, we use the effective bandwidth of an on/off source as a proxy for resource usage, given by $\bar{a}(x;m)$ in equation (1). The charging coefficients a, b are derived from the tangent to the curve of effective bandwidth at point m=M by means of simple algebra. The factor c in equation (2), contributes a fixed charge that compensates for the overhead of establishing a new connection. The time-volume formula has been proposed for ATM VBR services, but it also applies to DiffServ as well, since two leaky buckets are used for conformance control.

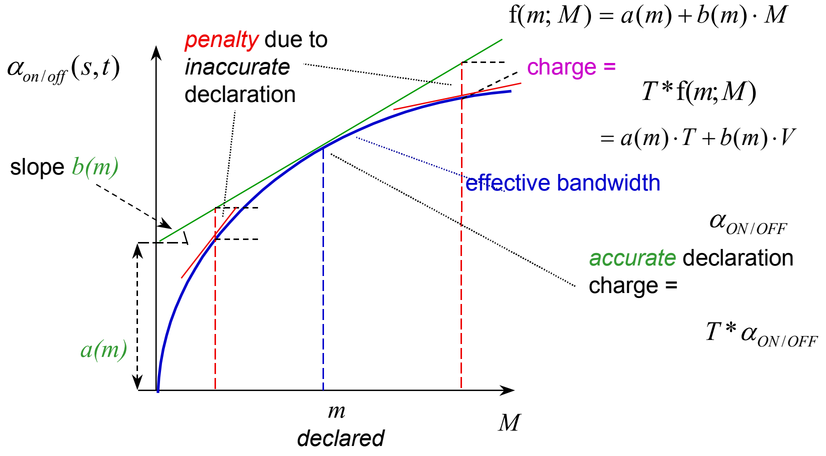


Figure 2: The charge as a function of the choice of user.

3.1.2 Charging Elastic Point-to-Point Services

While elastic services provide no guarantees of performance to the transmitted traffic, the traffic induced to the network by them has also to be charged, because it consumes network resources. This can be done: i) either proportionally to the volume of the inserted traffic (volume-based), i.e. to charge a fixed price per packet of the traffic inserted to these services, ii) or according to the burstiness of the traffic of the elastic services (burstiness-based) [5], e.g. by measuring the top 90-percentile of the distribution of the load produced per minute, as performed in a certain case.

3.1.3 Charging VPN Services

There is no significant scientific literature on charging VPN services. A theoretically justified solution would be to apply additive charging over all flows arising within the VPN [6]. In this case, the charge for each individual flow of the VPN should reflect the corresponding actual usage of network resources. Commercial approaches for charging VPN services vary. In some cases, VPN charging is additive, as was previously explained, plus some extra charges for certain features (security, always-on etc.). In other cases, the charge of VPN services is done on a per customer basis. Study of such cases falls outside the scope of INTERNODE.

3.2 Accounting

3.2.1 Auditing, Authorisation, Accounting (AAA) Architecture Considerations

The standard for accounting management, defined by the IETF AAA in [7], involves interactions between network devices, accounting servers, and billing servers. These are defined in a widely applicable way, and thus serve as background material for our work too. In particular, according to AAA, the network device collects resource consumption data in the form of accounting metrics. This information is then transferred to an accounting server typically via an accounting protocol, although it is also possible for devices to generate their own Session Data Records (SDRs). A SDR represents a summary of the resources consumed by a user over the entire session. The accounting server then processes the accounting data received from the network device in order to summarise interim accounting information, to eliminate possible duplicate data, and/or to generate SDRs. The processed accounting data is then submitted to a billing server. One of the functions of the accounting server is to distinguish between inter and intra-domain accounting events, and to route the former to accounting servers operating in other administrative domains too, when necessary (e.g. if trust among the network providers is an issue).

3.2.2 TeleManagement Forum (TMForum) Accounting and Charging Considerations

In this subsection we describe the basic management processes concerning the accounting and charging of a telecommunication service provision as provided by the TeleManagement Forum (TMForum) [8]. Specifically, the Telecommunications Operations Map (TOM) processes regarding the accounting and charging are as follows:

Network Data Management (NDM) processes: They provide the Service Quality Management processes (SQM), the Rating and Discounting (RD) processes, and the Customer

QoS Management (CQM) processes with usage/performance data for compilation of service quality data.

Service Quality Management (SQM) processes: They monitor service class data against the quality objectives that are created as a result of the SLA. If the objectives are not satisfied then a *QoS violation* is produced and forwarded to the CQM processes. SQM can also take actions based on a QoS violation. In order to do that, SQM takes into consideration usage/performance data produced by the NDM.

Customer QoS Management (CQM) processes: They compare the QoS violations received from SQM with the SLA of the customer and determine if there is a *SLA violation*. The QoS/SLA violations are communicated from a service provider to another using *customer reports*, and may also be sent to the RD processes. Customer reports are subject to the federated agreements among the providers, and contain among others usage/performance data, and violations of QoS and/or SLAs if any.

Rating and Discounting (RD) processes: They use the performance/usage data and probably the SLA violations in order to set the proper charging tariffs and schemes or *discounting* factors for the computation of the corresponding charge to the usage.

Invoicing Collection processes: They summarise the charging information from the RD processes and produce the corresponding customer bills.

4 Specification of Business Roles

In this section, we define the business roles related to accounting and charging Secure VPN (S-VPN) services provided as described in Section 2. We present this part to the charging scheme, since the structure of the latter (i.e. which role charges for what) is influenced by the business roles involved and by the interactions among them. As described in Section 2, S-VPN provider owns a VPN Service Provisioning and Support Platform (SPS) capable (among others) of automatically configuring and managing the S-VPNs on behalf of its customers. The S-VPN tunnel may traverse through any number of CPs between the home and the visited network. Each edge CP has the obligation, due to federation agreements with the VPN SPS, to support the S-VPN services provision in terms of QoS and accounting/charging. Thus, the federated CPs serve as 3rd-Party providers, each offering a certain part of the complete S-VPN service. The business agreements between the VPN SPS and the federated CPs are depicted in Figure 3. Note that in order for the traffic to be transported end-to-end, we assume the existence of interconnection agreements among the edge CPs and the intervening CPs (A, B in Figure 3) Detailed discussion of such agreements falls outside the scope of this paper.

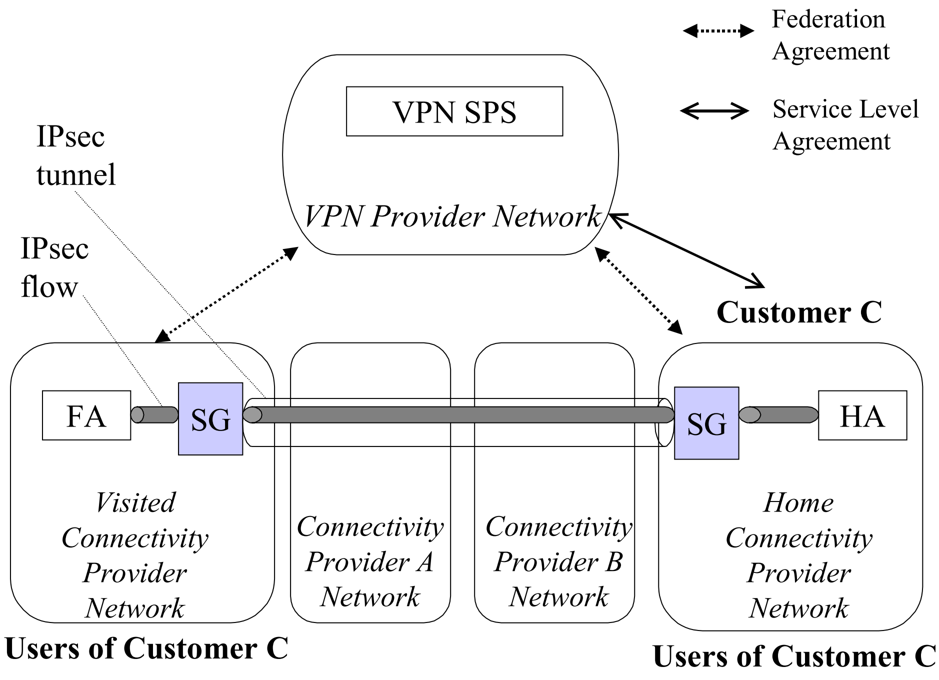


Figure 3: Business agreements for providing S-VPN services to mobile users.

The federated (home or visited) CP has to send the information on the charge that arises from its participation in the service provision to the accounting and charging subsystem of the VPN SPS. Specifically, the accounting and charging subsystem of this CP, in accordance with his federated agreement with the VPN SPS, and for the subscribed users to the S-VPN services, has to:

1. Measure the usage and associate it appropriately with its users, in order to allocate individual charges.
2. Send this information to the accounting and charging subsystem of the VPN SPS.

It is a responsibility of the federated CPs to charge for the usage according to conformance with the SLA and/or the federation agreement and the mobility support if any. On the other hand, the VPN SPS has to charge for the value added service of security.

5 Detailed Specification of Charging Scheme

5.1 Charging Issues

In this section, we present our approach for charging Secure VPN (S-VPN) services in the context described in Section 2. In particular, we adopt additive charging over all flows arising within a VPN; this is appropriate for charging S-VPN services (IPsec tunnels), as explained in

Section 3.1.3. The charging scheme for individual flows should reflect the actual usage of network resources. The main issues concerning charging of individual flows are describe below.

Charging for the transport of traffic: As already mentioned, the DiffServ architecture is used for QoS provision to the individual IP flows and/or the aggregates of traffic traversing the VPN pipes. Although, the charging scheme proposed by Courcoubetis and Siris is appropriate for charging DiffServ SLAs, the time-volume (*a*, *b*, *c*) approach is preferable for charging IPsec flows served by a QoS class, for the following reasons: a) The *time-volume* approach includes a constant charge per time unit for each IPsec connection, regardless of its usage, that compensates for the overhead of establishing the new connection; b) The main difference between the two charging approaches is that the time-volume approach benefits from a priori knowledge of the traffic properties. However, such knowledge can be made available for an IPsec flow through the specific type of user that generates that flow. In particular, we assume that the user identity is part of the S-VPN contracts (SLAs) and it is indicative of the expected network usage. Specifically, we assume that all users corresponding to the same identity or to a certain group of identities are of the same type, e.g. administrative employees or technical employees etc. A certain type of users corresponds to a certain type of traffic source; for example, administrative employees usually use videoconference applications, whose traffic volume and time duration can be monitored, thus leading to statistical information useful for future predictions of the mean rate.

As the *time-volume* approach is used for the computation of the charge for the traffic of an IPsec flow, it is necessary to specify the way that the proper *a*, *b*, *c* tariff is selected for charging this flow. As already mentioned, the identity of the user sending/receiving traffic over an IPsec flow determines the type of the user, and consequently the traffic source (i.e. the group of applications that the user may use together with statistics of the associated traffic). We assume that for each different type of user and for each different application there are predefined leaky bucket parameters $\{h, (\rho, \beta)\}$ and an estimate *m* of the mean rate value for each QoS class that can serve this application. On the other hand, the SLA for a S-VPN service determines the DiffServ QoS class that serves the flow of a particular application for a specific type of user. Thus, a pair (user identity, SLA) determines the eligible *a*, *b*, *c* tariffs for the computation of the charge of each IPsec flow. The most appropriate triple (a, b, c) is selected on the basis of the available estimate of the mean rate *m* of the application traversing the IPsec flow. Recall that, initially, the charging module has an estimation of the mean rate for each application and for each type of users. The mean rate *m* for each application for a certain type of users is constantly monitored and its "future" value is predicted, e.g. as a weighted average of past measurements.

(The weights may be larger for more recent measurements.) Recall that it is very important to estimate the mean rate *m* of an IPsec flow accurately, as it minimizes the output charge for the user of that flow. The various connectivity providers (CPs) have the incentive to minimize the charge for their users in the competitive environment that is considered. Note that estimating the mean rate per application for each user type induces a storage and monitoring overhead. Another alternative with less overhead would be to monitor the aggregate mean rate per user type. This however may result to considerable inaccuracy in the prediction of the actual mean rate of an IPsec flow, while all such flows will have to be charged with the same (*a*, *b*, *c*) parameters. According to [4], this will result to a higher total charge for the entire S-VPN service provision. Thus, there is a trade-off between accuracy of the prediction of the mean rate and the monitoring overhead. On the other hand, if we assume that always a small number of users is serviced by a federated CP, then the accuracy in the estimation of the actual mean rate could be further improved by monitoring the mean rate per application and per individual user.

If an IPsec flow is served "best-effort", then the *time-volume* formula is still applicable for the computation of charge on a per volume basis. Also, the charge in this case can be computed according to a burstiness-based model (see Section 3.1.2), if considered appropriate, w.r.t. incentives and accounting complexity. Further study of this approach is left for future work.

Charging for security: Each federated provider that its network domain serves as a source or sink of the VPN service provision is provided by the VPN SPS with a Security Gateway (SG). Additionally, the consumption of computational resources in the security procedure should be charged. This charge is computed proportionally to the volume of the inserted traffic for recovery from the cost of resource consumption, i.e. there is a fixed charge for security for each packet. Also, the charging scheme should reflect that there is a constraint in the service rate of the processor that encapsulates the packets according to IPsec, which is similar to the constraint corresponding to the capacity in a telecom link. This constraint should be satisfied automatically only when the traffic of the IPsec tunnels is served by DiffServ QoS classes, since in this case the traffic inserted is policed (i.e. already constrained) according to the SLAs of the customers. In case of best-effort traffic, the extra charge so as to enforce this constraint should be computed according to burstiness (see section 3.1.2).

Additionally, there should be a constant charge per time unit for each IPsec flow, because the identity of an IPsec tunnel, as well as the number of multiplexed flows in it, are "scarce" resources (e.g. There can only be finitely many IPsec flows served simultaneously.). Thus, aimless or malicious creation (or maintenance) of IPsec tunnels is prevented.

Charging for mobility: We first consider the charging issues involved with the provision of S-VPN services in the context of terminal mobility. As explained in Section 2, the VPN SPS provides each federated CP involved with a Mobility Agent MA (Home or Foreign Agent). The computational resources of the MA that are consumed should be charged. This charge is computed proportionally to the volume of the inserted traffic for recovery from the cost of resource consumption, i.e. there is a fixed charge for mobility support for each packet. Also, the charging scheme should reflect the fact that there is a constraint in the service rate of the processor of the MA that encapsulates the packets according to Mobile IP, which is again similar to the constraint corresponding to the capacity in a telecom link. This extra charge is computed according to the discussion above for computing the charge for security. Also, each network domain that has a finite set of IP addresses that a potential visited user can use interchangeably. Charging for this scarce resource is accomplished by charging a fixed price per time unit for the time period in which a temporary IP address is used by a mobile node. This fixed price is determined by the CP depending on the demand for such IP addresses or on a specific pricing policy.

In case of personal mobility, the user leases a terminal for accessing the S-VPN services. This terminal can also be a scarce resource, as the number of the available terminals is limited. Thus, according to the discussion of the previous paragraph, this leasing should be charged by a fixed price per unit of time for the time period of leasing the terminal. This fixed price may be determined by the terminal provider according to the demand for terminals, the terminal capabilities, or a specific pricing policy.

Discount: The charging scheme should include a discount in the total charge for a S-VPN service over a certain period on the basis of the total volume of a customer over the entire VPN, the QoS/SLA violations (see Subsection 3.2.2) and/or the identity of the customer.

Finally, for our S-VPN service, we employ accounting per user, but charging per customer in the overall charging procedure. Thus, for each individual user, the charges accounting for his usage of resources are computed, and subsequently are associated with the customer with which the user is subscribed.

5.2 The Charging Scheme and Sharing of Revenue

According to the discussion above, a user of a certain user type j using a set of applications I during a S-VPN service should be charged by the formula below:

$$\sum_{applications}^{I}\left\{\left[p_m + a_{ij}(m_{ij})\right]T_i + \left[p_{s\_class} + b_{ij}(m_{ij})\right]V_i + c\right\} \tag{5}$$

where T_i is the application period and V_i is the volume transferred for the application *i*. p_m is the price per time unit for the usage of a temporal (care-of) IP address by a mobile node in a visited network domain, p_{s_class} is the price (for the security level) per volume unit transferred within a security class *s_class*, [$a_{ij}(m_{ij})$, $b_{ij}(m_{ij})$, *c*] is the charging tariff, according to the time-volume formula, for this user of type *j* and a SLA contract (which influences the exact values of p_{s_class}, $p_{m,}$ and the leaky bucket parameters to which the applications are conformant). If charging is applied according to the burstiness of an elastic application *i*, then the value of volume V_i should be set to the value reflecting the burstiness of the source over the time period T_i. The charge for all users that are registered by a potential customer to the S-VPN services is given by the sum of the individual charges of the users, i.e. adding the outcome of the equation (5) for each user.

The traffic of a user of the S-VPN services that flows through his home and a visited network domain, according to his SLA with the VPN SPS, is charged by the accounting subsystems of these federated providers using the time-volume formula. Thus, the "*a*, *b*, *c*" tariffs are set by each federated CP that contributes in the provision of a certain S-VPN service. Thus, each of the "*a*, *b*, *c*" tariffs in equation (5) is the sum of the corresponding tariffs set by each CP contributing to a S-VPN service. Recall that, we do not deal with the way that the CPs that intervene in the traffic path from the home to the visited CP and back (e.g. CPs A, B in Figure 3), according to the discussion of Section 4. The visited CP also sets the value of p_m, as it owns the care-of IP addresses, which are scarce resources, charges for the mobility support, and collects the corresponding charges. The CP that serves as a home for the users of a customer (if not owned by the customer) charges the same way as a visited CP and also collects the resulting charges. If the home CP is owned by the customer, then the corresponding charges may be computed for monitoring purposes, without being included in the total charge. The VPN SPS charges for the security levels offered to the traffic of the users of the subscribed customers and collects the resulting charges. Also, it sets the value of p_{s_class} and computes the discount over the total charge for a customer. Finally, a customer is billed with the total charge resulted.

Finally, if a discount is applied, then the quantity in (5) should be multiplied by d_{cust_id}, which is the discount factor applied to the total charge and depends on the identity *cust_id* of the customer, the value of the charge, and the QoS/SLA violations (see Subsection 3.2.2).

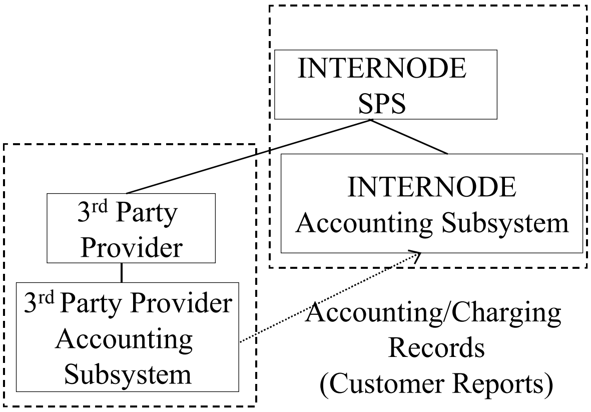
6 The Accounting and Charging Architecture

6.1 Accounting Issues

In order for the charging scheme previously described to be properly applied, the accounting subsystem has to measure the traffic of each IPsec flow and associate it with a specific type of users belonging to a customer. In order to accomplish this, the accounting subsystem has to:

1. Find the identity of the user and thus specify the type of the user as well as the customer that the user belongs to. In the case of personal mobility, the user identity is determined by the source IP address of the user, which is either his home address or a temporary IP address assigned to the user by the Visited CP after login. In the case of terminal mobility, the way the user identity is determined depends on the privacy policy of the Home and the Visited CPs. If the home IP address of the user is public, then the user is uniquely identified by his home IP address. On the other hand, according to [2], if the home IP address is private [9], then the user is uniquely identified by the pair (home IP address, Home Agent IP address).
2. Measure the traffic (volume and/or burstiness) inserted in a tunnel by each user. This accounting procedure is performed outside the IPsec tunnel; otherwise, it would have been very complicated. Mobility Agent (MA) is responsible for this task.
3. Provide to the customer a feedback of his current charge; this is referred to as live accounting. This capability may include support for debit payments and/or pre-paid services, and provides the customer with certain warning messages concerning his charge so far.
4. Support the capability of providing the customer with one total bill for the service (i.e. opaque billing) from the VPN SPS or with separate bills from each contributing provider to the service provision (i.e. transparent billing).

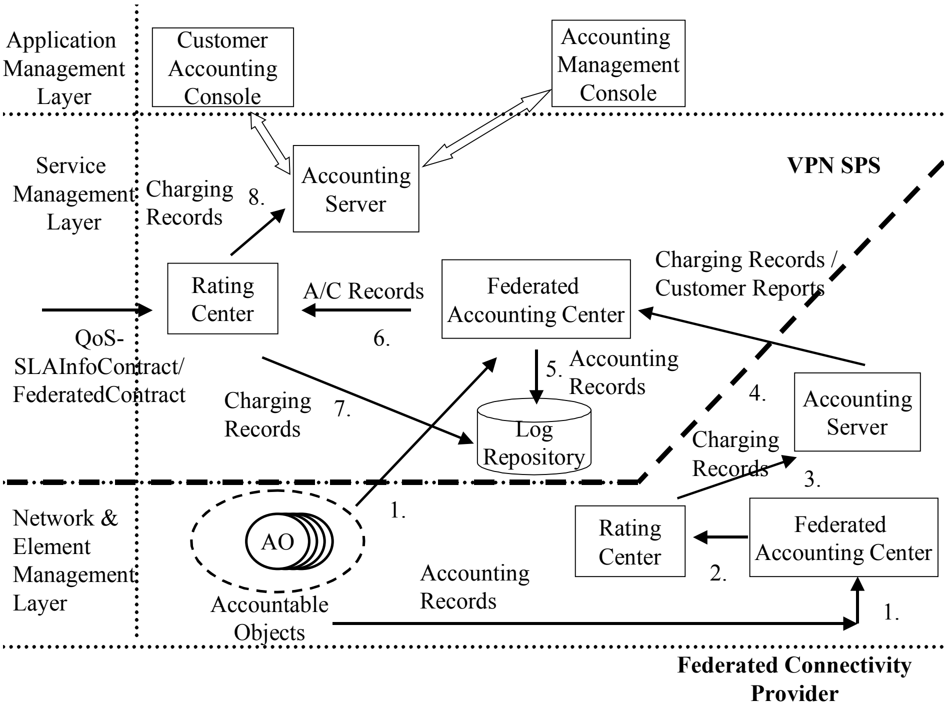
The overall model of flow of accounting information is depicted in Figure 4, in a Telecommunications Management Network (TMN) hierarchy. The inclusion of the accounting subsystem of the VPN SPS and the 3rd-Party providers is based on the principles of TINA accounting information model [10]. From an IETF AAA perspective, all accounting and charging records are generated by the accounting subsystems of the 3rd-Party providers and forwarded to the accounting subsystem of the VPN SPS, as described in Subsection 3.2.1. Also, the format of the accounting and charging records is defined according to the standards for Session Data Records (SDRs) of the IETF AAA group [11]. Finally, according to the Telecommunications Operations Map (TOM) (see Subsection 3.2.2), the way the SDRs are generated and the information contained therein depend on the contractual agreements between the federated CP and the VPN SPS.



INTERNODE SPS
INTERNODE Accounting Subsystem
3rd Party Provider
3rd Party Provider Accounting Subsystem
Accounting/Charging Records (Customer Reports)

Figure 4: Overall Accounting Information Model.

6.2 The Building Blocks



Application Management Layer
Customer Accounting Console
Accounting Management Console
Service Management Layer
Charging Records
8.
Accounting Server
VPN SPS
Rating Center
A/C Records
6.
Federated Accounting Center
Charging Records / Customer Reports
QoS-SLAInfoContract/ FederatedContract
Charging Records
7.
5.
Accounting Records
Log Repository
4.
Accounting Server
Charging Records
3.
Network & Element Management Layer
AO
Accountable Objects
1.
Rating Center
2.
Federated Accounting Center
Accounting Records
1.
Federated Connectivity Provider

Figure 5: A high-level view of the building blocks of the accounting architecture.

In this section, we give a high-level description of an accounting and charging architecture that is suitable for both the VPN SPS and a federated CP. Below, we describe the functionality of the building blocks of the architecture, which is presented in detail in Figure 5.

Accountable Objects (AOs): For each new S-VPN creation, AOs are associated with the corresponding Mobility Agents (MAs) and the Security Gateways (SGs) for this S-VPN, while an other AO is associated with the S-VPN service itself. The AOs associated with MAs and SGs collect the accounting information associated with the VPN and forward this information to the AO of the corresponding VPN service. Thus, the AOs form a ladder (i.e. a hierarchy in the flow) of accounting information for each S-VPN service, according to TINA. Subsequently, the AO associated to the S-VPN service forwards the accounting events to the Federated Accounting Centers both of the federated CP and of the VPN SPS. The latter receives the events so as to checking the validity of the charging information provided by the federated CP).

Federated Accounting Center: The Federated Accounting Center receives all accounting information collected by the AOs associated with the VPN services provided. Also, it categorizes usage and charging information on a per customer basis, produces Accounting Records, and forwards them to the Rating Center, according to the accounting rules. Furthermore, the Federated Accounting Center configures AOs, subject to the accounting policy rules received by the Accounting Management Console of the federated CP. The accounting information is also stored to a database called *Log Repository* for future use.

Rating Center: The Rating Center takes accounting information from the Federated Accounting Center and produces Charging Records taking also into account both the SLA/QoS violations (see Subsection 3.2.2) and the charging scheme (see Subsection 5.2) for the offered SLA. In order to check for SLA/QoS violations, the Rating Center perfoms the functionality of the SLA Fulfillment Subsystem and the QoS Assurance Subsystem, discussed in Subsection 3.2.2. The Rating Center also takes Charging Records (i.e. Accounting Records plus charging information) from the Federated Accounting Center concerning the final charge resulted from usage in a federated network. In this case, the Rating Center calculates the charge, taking also into account the security level provided as well as other charge contributors.

Accounting Server: It serves as the reference of the accounting architecture to external software components. All charging information is forwarded to the Accounting Server. The Accounting Server either forwards the charging information to the Federated Accounting Center of the VPN SPS according to the federation agreements (in case that it belongs to the federated CP); or it produces the bill and forwards it to the customer of the VPN SPS (in case that it belongs to the VPN SPS) according to the customer preferences (e.g. continuously/periodically).

In the Application Management Layer of Figure 5, depicted are the applications related to the interactions with the accounting and charging architecture by an administrator and by an user (or customer). Nevertheless, the information exchanged between the building blocks of the accounting and charging architecture is varies if it whether it belongs to the federated CP or the VPN SPS. Using TINA terminology, arrows 1, 2, 4, 5, 6, and 7 in Figure 5 show the accounting information originating from the Accountable Objects (AOs) that are associated with the Service Session Objects (SSOs); i.e. the VPN tunnels, the Mobility Agents (MAs) and the Security Gateways (SGs). Finally, arrows 3 and 8 show the charging information reaching the

Accounting Server having been converted to charging information. In particular, the sequence of events is as follows:

1. The Accountable Object associated to the VPN service forwards the accounting events to the Federated Accounting Center both of the federated CP (i.e. the CP federated with the VPN SPS; this applies also in the rest of this section) and of the VPN SPS.
2. The Federated Accounting Center of the federated CP receives all accounting records of the AOs associated with the VPN services provided, classifies it on a per customer basis and forwards them to the Rating Center of the federated CP. Also, the accounting information may be stored to the Log Repository of the federated CP for future use.
3. The Rating Center of the federated CP computes the charge for traffic transport and forwards the charging information to the Accounting Server of the federated CP; it may also store this information for future use into the Log Repository.
4. The Accounting Server of the federated CP sends the charging information as Customer Reports to the Federated Accounting Center of the VPN SPS.
5. The Federated Accounting Center of the VPN SPS stores the received charging and accounting information to the Log Repository of the VPN SPS.
6. The Federated Accounting Center of the VPN SPS classifies the received accounting and charging information on a per customer basis and forwards this information to the Rating Center of the VPN SPS.
7. The Rating Center of the VPN SPS computes the charge for the security level provided and thus produces the overall charge per customer.
8. The overall charge per customer is sent to the Accounting Server of the VPN SPS, which subsequently delivers the bills to the customers and the users.

7 Conclusions – Future Work

In this paper, we have studied the accounting and charging issues involved in the multiparty provision of Secure VPN services. We have proposed a proper charging scheme and an architecture for accounting and charging for such services that conforms to the existing standards for accounting. Using the proposed charging scheme, each provider collects exactly the revenue arising due to the consumption of his resources in the service provision. On the other hand, the users are charged for exactly the resources they actually use. Thus, the charging scheme is fair both for the providers and for customers. Furthermore, it provides the incentives to the providers to make their services better, to attract more users that use the S-VPN services for more time, in order to increase their revenue. It also provides users with incentives to use the S-VPN service according to their real needs, and indirectly (i.e. by means of their tariff selection) give providers their predictions on future traffic. Thus, the resources of the providers participating in a S-VPN service provision are protected from misuse or unnecessary use.

Apart from the functionality already described, there may be provided additional functionality to customers by means of intelligence. This may include support for accounting and charging management from customer side and efficient SLA selection or re-negotiation according to tariff updates by the INTERNODE SPS by a Customer Agent. This subject is left for future work.

References

[1] INTERNODE (IST-1999-20117). "Interworking Service Architecture and Application Service Definition". Work Package 2: Deliverable 3, December 2000. URL: http://www.internode.org

[2] G. Montenegro. "Reverse Tunneling for Mobile IP, revised". IETF RFC: 3024, January 2001.

[3] C. Courcoubetis and V. Siris, "Managing and Pricing Service Level Agreements for Differentiated Services", In *Proc. of IEEE/IFIP IWQoS'99, London*, May 31 – June 4, 1999.

[4] F.P. Kelly. "Tariffs and effective bandwidths in multiservice networks". In J. Labetoulle and J.W. Roberts, editors, The Fundamental Role of Teletraffic in the Evolution of Telecommunications Networks, Proceedings of the 14th International Teletraffic Congress, ITC 94, volume 1a of Teletraffic Science and Engineering, pages 401-410. Elsevier Science B.V., June 1994. Antibes Juan-les-Pins.

[5] UUNET. "Service Level Agreements for VPN service". URL: http://www.uunet.com/terms/sla/emea/vpn.xml

[6] C. Retsas. "DSL Technology, DLS Service Models, and Charging DSL Services". MSc Thesis (in Greek), Computer Science Department, University of Crete, Greece, November 2000.

[7] B. Aboba *et al*. "Introduction to Accounting Management". IETF RFC: 2975, October 2000.

[8] TeleManagement Forum. TOM Application Note: "Mobile Services: Performance Management and Mobile Network Fraud and Roaming Agreement Management". Document: GB910B, version 1.1, September 2000.

[9] Y. Rekhter, B. Moskovitz, D. Karrenberg, G. J. de Groot and E. Lear. “Address Allocation for Private Internets, BCP 5”. IETF RFC: 1918, February 1996.

[10] TINA-C. “Network Resource Architecture Version 3.0: Accounting Management”. Document No. NRA_v3.0_97_02_10, pp. 137-180, February 1997.

[11] N. Brownlee and A. Blount. “Accounting Attributes and Record Formats”. IETF RFC: 2924, September 2000.