Delivering QoS enabled IP-VPN services

Autor(en): **Bucurescu, Vlad / Ben-Yacoub, Leila Lamti / Schneider, Johannes**

Objekttyp: **Article**

Zeitschrift: **Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology**

Band (Jahr): **79 (2001)**

Heft 2

PDF erstellt am: **29.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-876516

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Exploration Programmes:
Corporate Technology Explores Future Telecommunications

Delivering QoS Enabled IP-VPN Services

The upcoming availability of service differentiation in IP networks by IETF's DiffServ framework, and the tendency in telecommunication to have different business aspects operated by independent providers, lead to new aspects of IP service management. Three relevant aspects of delivering IP VPN's transporting applications with Quality of Service (QoS) requirements have been investigated: firstly, the relevant business roles and their relationships in terms of Service Level Agreements; secondly, the QoS requirements at the IP network layer for a selected set of widespread applications; and thirdly, the design of an IP-VPN provisioning tool with support for applications requiring QoS guarantees.

The Exploration Programme "Customer Care and Service Management Platforms" deals with technologies and processes providing ways for Swisscom to differentiate both in Customer Relationship Management (CRM) and in service management. In customer care, the work is concentrating on multimedia web-based customer contact centre technology and on customer behaviour analysis using data mining techniques. Concerning service management, a platform prototype is built aiming at a radical simplification of 1) provisioning processes – particularly for QoS based SLA (Service Level Agreement) management – and 2) billing processes for IP services.
With its Exploration Programmes, Corporate Technology is exploring telecommunication technologies and new service possibilities with a long-term view of 2–5 years. Further, the expertise built up in the course of this activity enables active support of business innovation projects.

For IP-VPN's to become a mass-service for SME customers, automatic, fast and efficient provisioning is a key success factor. Services such as IP telephony, video conferencing, or multimedia streaming on an IP-VPN will require QoS guarantees. The ability to guarantee QoS values in Service Level Agreements (SLA) with the customers will therefore become a competitive advantage.

VLAD BUCURESCU, LEILA LAMTI BEN-YACOUB AND JOHANNES SCHNEIDER

The demand for IP Virtual Private Network services (VPN) for SME's is expected to grow in the future [1]. For the large number of SME customers, automatic IP-VPN service provisioning is very attractive. In fact, it saves operational costs for the network operator and allows quick service provisioning. Today, IP technology is developing in a direction where the support of services requiring guaranteed QoS becomes possible, thus complementing data services based on best-effort transport. The IETF DiffServ Framework is a major effort in this direction [2]. These developments will allow the offer of applications requiring QoS, such as telephony, video or multimedia streaming, web-based e-commerce, etc., on future IP-VPN's.
A recent tendency of telecommunication network operators is the "decomposition of the value chain", meaning that different business aspects, such as network wholesaling or service retailing, are run by different units or even different companies. In this context we use a model in which three independent business roles are involved: A Backbone Network Operator (BNO) operating an IP network, an Access Network Operator (ANO) operating an access network, and a Value Added Service Provider (VASP), operating a virtual IP network (fig. 1).

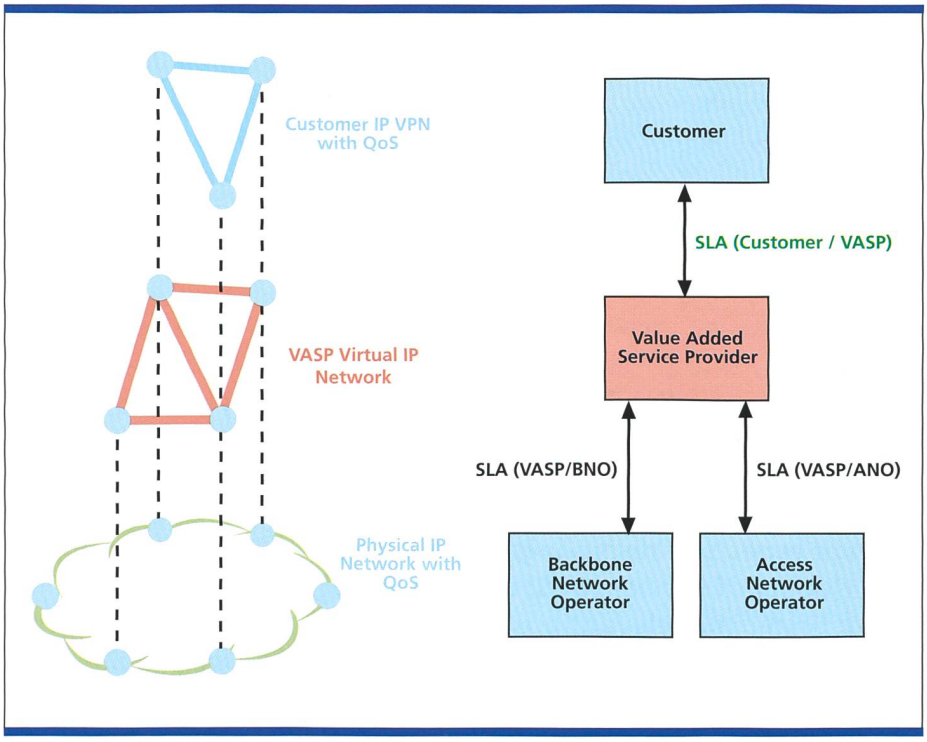

Fig. 1. Involved actors and their relationships in the IP-VPN service provisioning chain.

We have investigated service management aspects of IP-VPN's with QoS support, adopting the perspective of a Value Added Service Provider. This latter buys bandwidth from a broadband wholesaler and sells IP-VPN's to final customers. The work gives an answer to the question of how to fulfil an SLA for a new QoS-oriented IP-VPN service.
This article concentrates on three aspects. The first one deals with the relationships that exist between the involved business partners, i.e. final customers, VASP, BNO and ANO. We mainly focus on the Service Level Agreements established between the VASP and the BNO. The second aspect deals with the definition of some mapping rules that allow the VASP to translate application quality as required by final customers into network quality classes supported by the BNO.
The third aspect concerns the development of a Graphical User Interface (GUI) allowing the VASP to offer the IP-VPN service to SME's.
In the new Swisscom holding structure, the BNO and ANO together correspond to the Network Services & Wholesale Unit, whereas the VASP corresponds to the Units Consumer Com or Enterprise Com. In addition, an external company may play the VASP role and compete with the Swisscom internal VASP.

QoS enabled IP-VPN's provided by a VASP

Relationships between Involved Providers

Assuming the above-mentioned value-chain decomposition, the business roles and the relationships between involved providers have been identified. In addition, the interconnection points between them have been characterised in terms of SLA's.

Mapping of Application QoS into Network QoS

Customers running multimedia services over their IP-VPN are interested in getting a guarantee for the service availability. This availability depends on the network quality delivered by the DiffServ framework. The required network quality parameters at the IP layer, such as guaranteed bandwidth, loss, delay, and jitter (delay variation), have been determined.

GUI for IP-VPN Provisioning

Web-based order entry through a GUI is a method which allows efficient provisioning of IP-VPNs for SMEs. This GUI has to include the topology of the VPN and the applications with the different supported quality classes. A prototype of such a GUI allowing to demonstrate clearly its required features has been implemented. Such a GUI may be used by Swisscom staff or directly by the customers over an e-commerce platform.

Results

Relationship between Involved Providers

The business model considered in this paper (fig. 1) has been proposed by the TINA-Consortium [3]. It defines the business roles, the management domains and the interactions between the involved actors.

The role of the ANO and the BNO is to operate the access and backbone network and to provide wholesale network services to a VASP acting as a retailer. We assume that the BNO operates an IP backbone on which it offers several transport qualities. The VASP buys large amounts of network capacity from the BNO in order to interconnect its different strategic locations, forming a virtual IP network. Moreover, the VASP has to make sure that customer sites are connected with an appropriate access type able to support the necessary performance for the requested applications. The VASP buys this service from the ANO. We consider different access technologies, such as ADSL, HDSL, ISDN, Cable TV, Leased-line, GPRS, UMTS etc. In fig. 2, we present the relationships between the considered actors as well as the Service Access Points (SAP) that define the responsibility domains for each of them. The BNO provides the Backbone SAP's between which the transport service is offered to the VASP. The ANO interface with the VASP allows to connect a customer

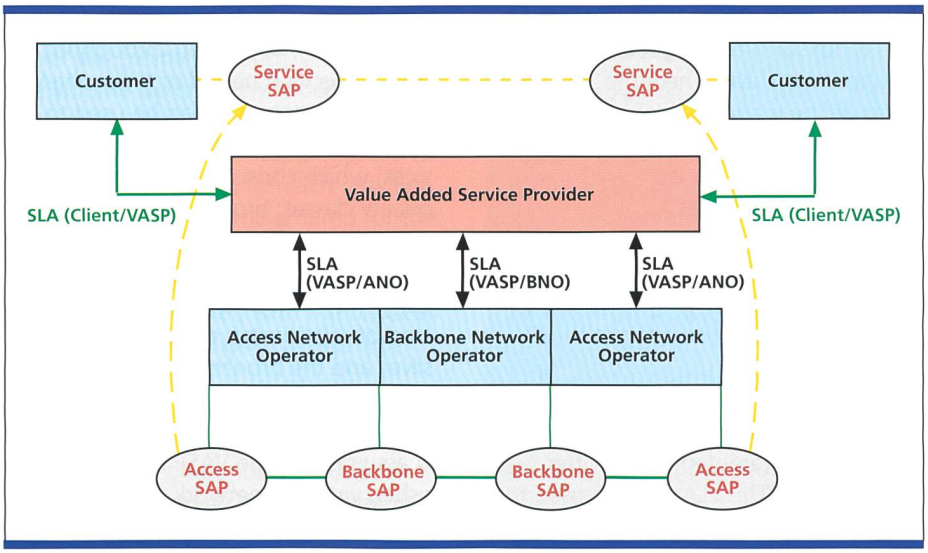

Fig. 2. SLA's and SAP's between involved actors.

equipment to the backbone through an Access-SAP. Finally, the interface between the VASP and the final customer is called Service-SAP and can be seen as an Access-SAP enhanced with services. The customer interacts only with the VASP.

Service Level Agreements

An SLA is a contract between a provider and a customer that specifies service levels in terms of performance and reliability. Generally, a successful SLA contains multiple components, each of which contributes to the definition of the service levels.

On one hand, there are network service metrics which include network availability, delay, packet loss, connection failures, etc. On the other hand, there are two main application performance metrics that are important to the final customers: service availability and application response time.

The VASP has to consider the capacities of the BNO in terms of network quality classes before offering service guarantees to its final customers. Mapping rules between application and network quality classes have to be defined.

Another issue is that service requirements can be specified by the customer in non-technical terms, such as: "I want my calls to go through quickly!" or "I want my calls to sound clear!". For this reason, the VASP needs to translate these statements into measurable parameters.

SLA Types between VASP and BNO

Between a VASP and a BNO, there are two types of SLA's that could be established between Backbone-SAP's (fig. 3):

- *Point-to-Point SLA:* In this case, the amount of traffic in each direction is specified explicitly between all pairs of SAP's.
- *Point-to-Cloud SLA:* In this case, the total traffic volume entering the SAP, called Ingress Committed Rate (ICR), as well as the total traffic volume exiting the SAP, called Egress Committed Rate (ECR), are specified for each SAP. The traffic defined in an ICR can reach any other SAP as long as the maximum agreed volume is not exceeded. Similarly, the SAP is able to receive traffic from any other SAP as long as the volume is below the threshold specified by the ECR.

In a DiffServ IP network, two quality classes have been defined: the Expedited Forwarding class (EF) and the Assured Forwarding class (AF) (see section "DiffServ Quality Classes" for more details). The choice of an SLA type can be done based on the network quality class and its guarantees. As an example, for the EF class, a point-to-point SLA seems to be appropriate, while for the AF class a point-to-cloud type would be more adapted. Generally, the point-to-cloud SLA type is more appropriate and fits better to the Diffserv paradigm.

Mapping of Application QoS into Network QoS

At the network level, the BNO can implement the DiffServ framework which creates several transport quality classes in the IP network. A transport class is specified as a vector of parameters including the quality factor (e.g. delay, jitter, packet loss) and the quantity factor (e.g. throughput).

However, using only these DiffServ definitions is not sufficient to guarantee QoS at the application layer. Therefore, the VASP has to define mapping rules between applications and network quality classes.

DiffServ Quality Classes

DiffServ defines two network quality classes: the EF class [4] and the AF class [5]. The traffic forwarding treatment in the routers is based on a tag in the IP header.

- EF class: its purpose is to provide a guaranteed bandwidth supporting strict QoS parameters (delay, jitter, packet loss). This class can be used to provide an end-to-end "Virtual Leased Line" type of service. It is suitable for any packetizeable traffic that currently uses fixed circuits (e.g. telephony, broadcast video distribution, leased data lines). Multiple flows can be multiplexed in the same virtual leased line and be assured a high level of QoS guarantees.
- AF class based services are able to support either a relative quality (better than a certain class, e.g. "better-than-best-effort"), or a mean throughput over a specified period of time when congestion occurs. It can be used to implement the so-called Olympic services, which consist of three network quality classes: bronze, silver, and gold. Packets in the gold class experience better network conditions than packets assigned to the silver class. The same kind of relationship exists between the silver and the bronze class.

QoS Mapping Rules

We assume that the VASP owns a fully meshed virtual IP network made up of nodes interconnected through end-to-end IP tunnels. Each tunnel belongs to a DiffServ network quality class and is characterised by QoS parameters and a maximum throughput.

The IP-VPN service offered by the VASP has to connect customer sites in order to transport traffic belonging to different applications (e.g. IP telephony, video-conferencing etc.). For this reason, the VASP has to assess customer needs in terms of application quality classes and throughput amounts between all his sites.

To translate quality classes from the application to the network layer, a series of tests with some widespread applications has been carried out within a Eurescom project [6]. Tested applications have been classified into 3 categories (table 1).

For each application category, two quality classes have been defined: premium and basic. A user can choose between them depending on his requirements.

The two classes should be defined such that a user will always perceive a difference in service quality between them. This allows a different charging model for each class and leads to better use of the network resources.

Based on the measurement results in the Eurescom project, and taking into account the available network technology (MPLS, DiffServ, and traffic engineering techniques), we propose mapping rules as presented in table 2. Network parameters (delay, loss and jitter) presented in this table concern only backbone network performances which are agreed between the VASP and the BNO, and are measured at the Backbone-SAP's. Additional delay, loss or jitter introduced by the access network are not considered in the presented values. However, the access rate is taken into account in the application quality class definition, since it influences the perceived quality.

For the specific case of non-interactive real-time services, we have specified 2 different premium classes because of the video-streaming application (Premium P1 and Premium P11). In fact, high access rates (1Mbps) need stringent backbone performances. In order to profit from this high quality, it is suitable to have the two classes specified in table 2.

Implications on the SLA between the VASP and the BNO

In order to optimise resource usage at the VASP side, we propose to multiplex several customer flows on the same virtual tunnel. This reduces the number of virtual tunnels allocated by the VASP.

The VASP has to choose between AF and EF network classes taking into account economic factors (EF is more expensive than AF) and customer satisfaction (e.g., AF may not satisfy performance needs of interactive bursty applications).

Taking into account these aspects, we propose the virtual tunnel types as proposed in table 3. Each one is charac-

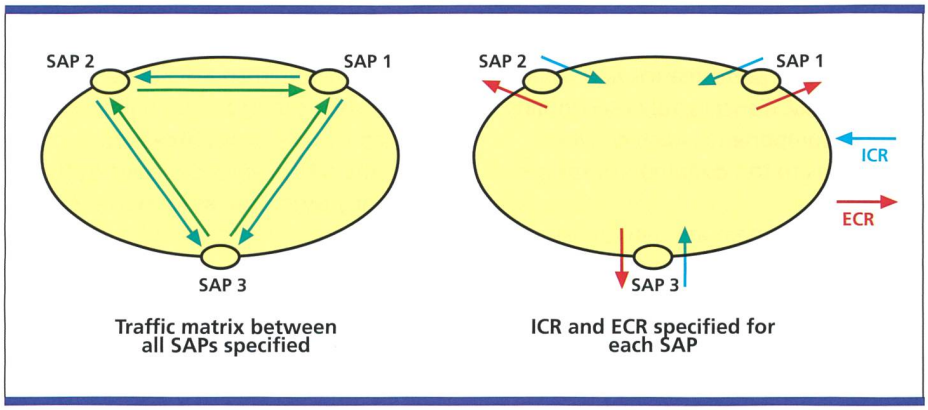

Fig. 3. Point-to-Point SLA (left) and Point-to-Cloud SLA (right). All SAP's are backbone SAP's.

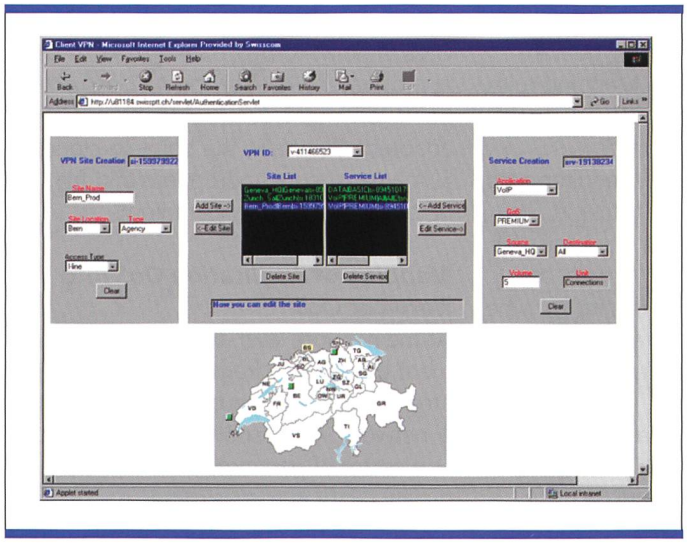

Fig. 4. A snapshot of the GUI.

terised by a set of network performance limits. Whenever possible, a common virtual tunnel for different applications requiring similar QoS guarantees should be used (e.g. virtual tunnel type 2 for both VoIP and video-streaming).

GUI for IP-VPN Provisioning

The developed GUI prototype which is suitable for a VASP for advanced IP-VPN provisioning is shown in fig. 4. Such a GUI may be used by the VASP staff or, in case of web-based e-commerce, directly by the customers. The GUI contains three logical parts: 1), the topological part allows configuring (i.e. to create) the sites of the VPN (left side in fig. 4). 2), the service part allows configuring (i.e. to create) the applications delivered at each site (right side in fig. 4). 3), the VPN part contains the list of all configured sites and of all configured applications (centre in fig. 4). In addition, the VPN part contains a map which visualises the geographical location of the configured sites (centre lower part in fig. 4).

For the configuration of a site, the GUI user can define a site name. He can then select the site location from the list of strategic locations, where the VASP has a backbone SAP, and choose the site type (headquarter or agency as examples). Finally, he chooses the access type from the list offered by the VASP, depending on the bandwidth needs. Each configured site can be added to the site list of the VPN part by the "Add Site" button in the centre part of the GUI. Sites which have been added can still be edited or deleted with the corresponding buttons in the VPN part.

For the configuration of the services, the desired applications and the desired quality level for each application (Premium or Basic) can be chosen from a list of supported applications. For each application, the volume can be defined in an appropriate unit (e.g. bandwidth, number of connections, number of sessions). Moreover, it is possible to define the volume for three topological variants: firstly, the total volume on the VPN between any pair of sites, secondly, the volume between a specific site and any other site (point-to-cloud), and thirdly, the volume between two specific sites (point-to-point). For the point-to-cloud and the point-to-point topology, the volume can be specified for each direction individually. The volume entered for the different applications and topological variants is added in an appropriate way and can be compared with the physical limitations of the chosen access type.

Conclusions

Future IP VPN's will include applications requiring QoS guarantees included in the SLA's. The upcoming IP DiffServ framework has the objective to provide QoS-enabled IP services without capacity over-provisioning.

The objective of this paper was to look at the requirements for the provisioning of QoS-enabled IP-VPN's by a VASP, supposing IP DiffServ at the network layer. A clear view of each provider's responsibility in the value chain, as well as a clear relationship definition between them are presuppositions for a successful business. Moreover, SLA specifications between involved partners have to take into account application QoS requirements and map them to the supported QoS capabilities in IP DiffServ networks. Therefore, the work focused on three aspects:

- definition of the relationships between involved providers in terms of SLA's,
- mapping of application QoS into network QoS, in particular for IP DiffServ networks,
- development of a GUI prototype presenting ideas on how to provision QoS-enabled IP VPNs by a VASP.

Our objective is to help Swisscom in providing QoS-enabled IP-VPN's to SME's quickly and efficiently, in particular in a business environment with independent, collaborating providers.

Outlook

As a next step, the "point-to-cloud" SLA type with QoS guarantees at the IP network layer has to be explored. This SLA type gives simple guarantees for IP-VPN services, since it is not necessary to specify a traffic matrix between all VPN sites. However, in order to guarantee such an SLA with QoS specifications, the network operator has to assume the worst case traffic split between the different destination sites in the customer VPN. In fact,

Application Category	Chosen Application
Interactive Real-Time Data Delivery	Telephony over IP
Non-Interactive Real-Time Data Delivery	Audio/Video Streaming
Interactive Burst Transfer	Web E-commerce

Table 1. Chosen application categories.

Abbreviations

ADSL	Asymmetric Digital Subscriber Line
ANO	Access Network Operator
BNO	Backbone Network Operator
BW	Broadband Wholesaler
DiffServ	Differentiated Services
GPRS	General Packet Radio Service
GUI	Graphical User Interface
HDSL	High speed Digital Subscriber Line
IETF	Internet Engineering Task Force
IP	Internet Protocol
QoS	Quality of Service
ISDN	Integrated Services Digital Network
SAP	Service Access Point
SLA	Service Level Agreement
SME	Small or Medium Enterprise
TINA	Telecommunications Information Networking Architecture
UMTS	Universal Mobile Telecommunication System
VASP	Value Added Service Provider
VPN	Virtual Private Network

References

[1] E. Hindin, "IP VPN Market Renaissance Is Just Around the Corner", Yankee Group Report Volume 1, No 14, Sept. 2000.

[2] http://www.ietf.org/html.charters/diffserv-charter.html

[3] M. Yates et. al., "TINA Business Model and Reference Points", May 1997.

[4] V. Jacobson et. al., "An Expedited Forwarding PHB", RFC 2598, June 1999.

[5] J. Heinanen et. al., "Assured Forwarding PHB Group", RFC 2597, June 1999.

[6] Eurescom P906 Quasimodo: http://www.eurescom.de/public/projects/P900-series/P906/P906.htm

	Delay	Jitter	Loss	Nominal Access Rate
Non Interactive Real-Time				
Premium P1	<30 ms	<3 ms	0%	1 Mbit/s
Premium P11	<250 ms	<50 ms	0%	56 Kbit/s–100 Kbit/s
Basic B1	100–750 ms	<100 ms	<5%	>56 Kbit/s
Interactive Real-Time				
Premium P2	<85 ms	<3 ms	0%	– no requirements
Basic B2	<750 ms	<3 ms	0%	– no requirements
Interactive Bursty Applications				
Premium P3	<150 ms	– not defined	<7%	50 kbit/s–1 Mbit/s
Basic B3	150–300 ms	– not defined	7-15%	12–50 kbit/s

Table 2. QoS mapping rules.

in this SLA, only the total traffic volume exiting from the customer site to the network is specified with a set of QoS guarantees. The customer can send this traffic to any combination of other sites in the VPN as long as the maximum agreed volume is not exceeded.
The over-provisioning solution in this case results in a huge waste of resources since the network operator has to guarantee QoS in the worst traffic split case, i.e. when all the agreed traffic volume is sent to only one destination. Therefore, more efficient solutions must be explored, namely dynamic connectivity and flexible reservations between customer sites. [7]

	Tunnel Type	Delay	Jitter	Loss
Non Interactive Real-Time (Video Streaming)				
Premium P1	EF virtual tunnel – **type 1**	<30 ms	<3 ms	0%
Premium P11	EF virtual tunnel – **type 2**	<85 ms	<3 ms	0%
Basic B1	AF silver virtual tunnel – **type 3**	<750 ms	<100 ms	5%
Interactive Real-Time (VoIP)				
Premium P2	EF virtual tunnel – **type 2**	<85 ms	<3 ms	0%
Basic B2	EF silver virtual tunnel – **type 3**	<750 ms	<100 ms	5%
Interactive Bursty Applications (WEB e-commerce)				
Premium P3	AF gold virtual tunnel – **type 4**	<150 ms	no jitter limit	7%
Basic B3	AF bronze virtual tunnel – **type 5**	<150 ms	no jitter limit	15%

Table 3. Proposed tunnel types.

TINA-Consortium:
http://www.tinac.com

Vlad Bucurescu *studied Communication Systems at the Swiss Federal Institute of Technology (EPFL, Lausanne) and Eurecom (Sophia-Antipolis, France) from 1992 to 1998. He did his Diploma thesis at Swisscom Corporate Technology in the field of Mobile-IP. Since 1998 he has been working at Corporate Technology mainly in the two domains Mobility and Service Management.*

Leila Lamti Ben-Yacoub *studied computer science at an engineering school in Tunisia from 1990 to 1995 and performed Ph.D. studies in ENST Bretagne France from 1995 to 1999 where she worked as a research assistant. Her Ph.D. work dealt with traffic management and QoS engineering in IP and ATM networks. In fall 1999, she joined Swisscom Corporate Technology. She is working in the area of service provisioning and performance management for IP networks, with a specific focus on Voice over IP services and MPLS-based Virtual Private Networks.*

Johannes Schneider *studied physics at the University of Berne and graduated in optics in 1988. He joined the Telecom PTT R&D department in 1989, where he worked in technology of integrated optics until 1993. From 1993 to 1998, he worked in transmission in the access network, specifically on Fiber in the Loop, ATM and interconnection. In 1999, he led a project in the area of multimedia and human-machine interface. Since 2000, he has been working in the area of Service Management for telephony, IP networks, and UMTS.*

Zusammenfassung

Das IP DiffServ Framework von IETF ermöglicht verschiedene Qualitätsklassen in IP-Netzen. Damit können zukünftige IP-VPNs Applikationen unterstützen, die auf IP-Netzen Qualitätsgarantien benötigen. Zudem besteht die Tendenz, dass bei Telekom-Netzen verschiedene Geschäftsbereiche von finanziell unabhängigen Einheiten betrieben werden. Dadurch ergeben sich neue Anforderungen beim Bereitstellen von IP-VPN-Diensten. In diesem Zusammenhang wurden drei wichtige Aspekte geklärt: Erstens die involvierten Geschäftsbereiche und ihre durch Service Level Agreements geregelten Beziehungen und zweitens die Qualitätsanforderungen in der IP-Netzschicht für einige wichtige Applikationen. Drittens wurde ein Prototyp entwickelt für das Provisioning von IP-VPN-Diensten mit Applikationen, welche Qualitätsgarantien benötigen.