Project Numbers:	**IST-1999-10077 AQUILA**
	IST-1999-11017 CADENUS
	IST-1999-11253 TEQUILA
Project Titles:	**Adaptive Resource Control for QoS Using an IP-based Layered Architecture (AQUILA)**
	Creation and Deployment of End-User Services in Premium IP Networks (CADENUS)
	Traffic Engineering for Quality of Service in the Internet, at Large Scale (TEQUILA)

IST Premium IP Cluster

Authors:	**Bert F. Koch, Martin Potts, Danny Goderis et al.**
Editors:	**Gerald Eichler / Bert F. Koch**
Contribution File Name:	**jd001-b0.doc**
Version:	**Version 5**
Company:	**AQUILA, CADENUS, TEQUILA**
Date:	**March 31, 2003**
Distribution:	**Public**

Table of Contents

Table of Figures

Table of Tables

EXECUTIVE SUMMARY

The three IST projects AQUILA, CADENUS and TEQUILA investigate IP Quality of Service support in large IP networks. The main objective of the projects is the same: providing Premium IP services over the Internet as a basic step towards the Next Generation Networks (NGN) of tomorrow. All the partners involved in these three projects consider that having this common goal is a very positive fact (since the acceptance of three projects shows that this is one of the most important concerns of today's research in IP services and networks) and an excellent opportunity to investigate the technical feasibility of different approaches for addressing this shared concern. The common goal and, by consequence, the unavoidable overlap of some of the technical areas being investigated by the three projects, is judged as a *strength and opportunity* of the IST Premium IP cluster and not at all as a threat or a weakness.

This jointly prepared deliverable contains a brief description of the three projects in terms of objectives, architecture, service and resource management. The common goal of the Premium IP cluster projects as well as differences and their complementary approaches are presented, so that the projects are “comparable” by means of tables, which allow the reader to easily assess complementary approaches and the (main) differences between the projects. In addition, the document reports on current co-operative activities like Monitoring and Measurement or contributions to IETF, as well as future activities like collaboration with the IST project INTERMON or validation through trials.

1 FOREWORD/DISCLAIMER

1.1 Focus of this Deliverable

This document focuses on the work being done by three IST projects, which are all placed in the NGN Premium IP cluster. These projects are

- Adaptive Resource Control for QoS Using an IP-based Layered Architecture (AQUILA)
- Creation and Deployment of End-User Services in Premium IP Networks (CADENUS)
- Traffic Engineering for Quality of Service in the Internet, at Large Scale (TEQUILA)

The common context is seen in the provisioning of QoS-based IP service offerings over the Internet. Although the authors of this document are well aware of other IST projects that are somehow related to the same and generic (QoS) topic, briefly mentioned in section 4.1, the clustering activity is restricted to the aforementioned projects. Common reviews with open workshops reflect this aim.

This document aims at providing a comparative analysis of the work being done within the AQUILA, CADENUS, and TEQUILA projects. As such, it is not the intention of this document to provide a complete and detailed description of the respective approaches, but rather to focus on the similarities and the differences of the projects, according to a set of well-defined characterisation parameters.

From this perspective, the document is organised as follows:

Section 3 describes the respective objectives of the three projects following the same base structure with objectives, architecture, service and resource management. Section 4 first outlines the common goal of the Premium IP cluster projects. Then this section provides a comparison table of the respective approaches. Section 5 gives some ideas for current collaboration, while section 6 focuses on future activities. Section 7 provides a list of the bibliographical references for an in-depth description of the technical investigation being conducted by the three projects.

1.2 Introduction to Premium IP Cluster

The Premium IP cluster covers several IST projects focusing on Quality of Service. Figure 1-1 gives an overview about these projects following a hierarchical manner. This delivery covers the three projects: AQUILA, CADENUS and TEQUILA.

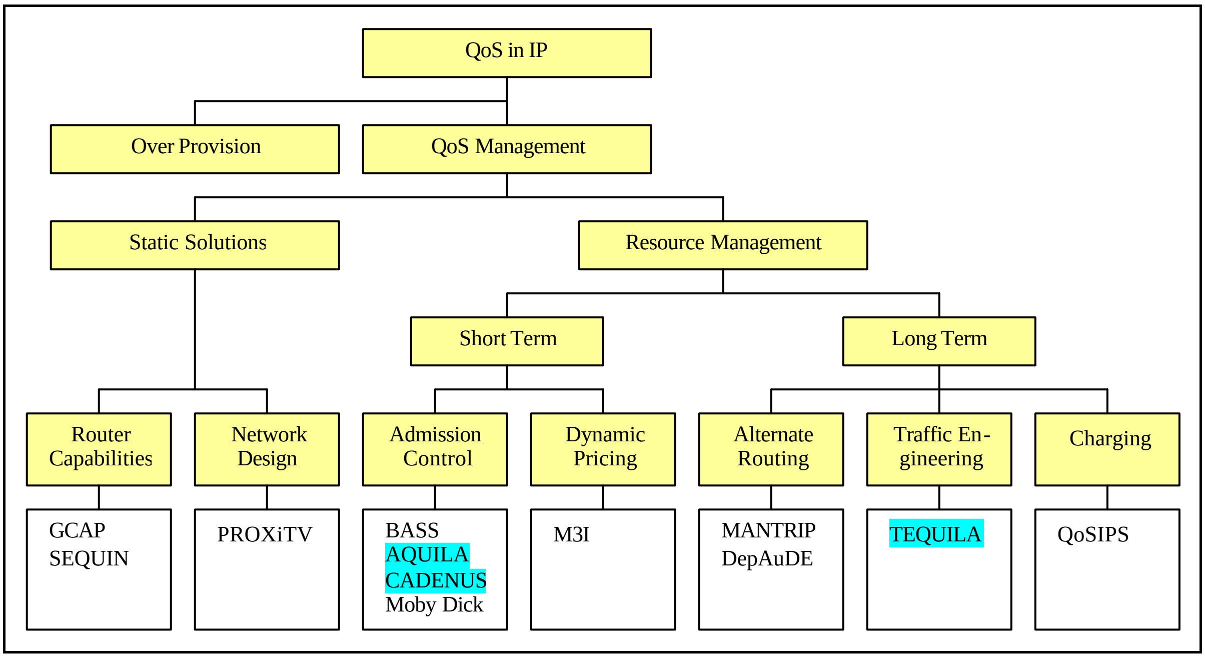


Figure 1-1: *Premium IP Cluster projects.*

2 DESCRIPTION OF SELECTED PREMIUM IP PROJECTS

2.1 AQUILA (IST-1999-10077)

2.1.1 Objectives

AQUILA defines, evaluates, and implements an enhanced architecture for QoS in the Internet. Existing approaches e.g. Differentiated Services, Integrated Services and label switching technologies have been exploited and significantly enhanced, contributing to international standardisation. The architecture has been designed to be cost-effective and scalable. It introduces a software layer for distributed and adaptive resource control and facilitates migration from existing networks and end-user applications. Technical solutions have been verified by experiments and trials, including QoS-enhanced on-line multimedia services.

The key objectives of the project are:

1. To enable **dynamic end-to-end QoS** provisioning in IP networks for QoS sensitive applications e.g. Internet telephony, premium web surfing and video streaming. Static resource assignments have been considered as well as dynamic resource control.
2. To continuously analyse **market situations** and **technological trends** for QoS solutions and to exploit the results of the project creating applicable business plans based on the user and service provider requirements.
3. To design a **QoS architecture** including an extra layer for resource control for scalable QoS control and to facilitate migration from existing networks. The Differentiated Services architecture for IP networks has been enhanced introducing dynamic resource and admission control.
4. To **implement prototypes** of the QoS architecture as well as QoS based end-user services and tools in order to validate the technical approach of the solution design.

2.1.2 Architecture

The project assumes the DiffServ architecture as the most promising starting point for its work. The project develops extensions of this architecture in order to avoid the statically fixed pre-allocation of resources to users. Dynamic adaptation of resource allocation to user requests is enabled in a way that keeps the overall architecture scalable to very large networks.

2.1.2.1 Resource Control Layer (RCL)

The Resource Control Layer (RCL) is an overlay network on top of the DiffServ core network (see Figure 2-1). The Resource Control Layer provides an abstraction of the underlying layers. The RCL mainly has three tasks, which are assigned to different logical entities:

- to monitor, control and distribute the resources in the network by the Resource Control Agent (RCA).
- to control access to the network by performing policy control and admission control by the Admission Control Agent (ACA).
- to offer an interface of this QoS infrastructure to applications by the End-user Application Toolkit (EAT).

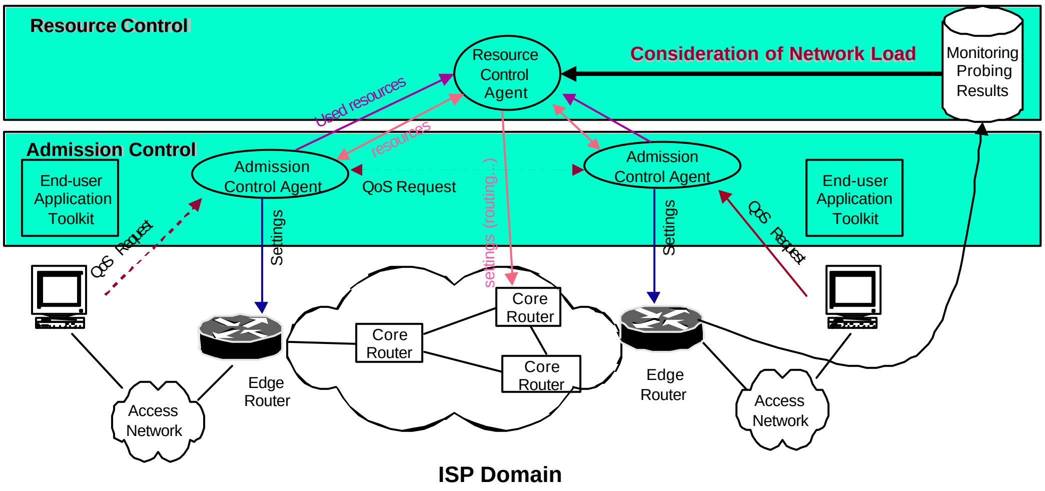


Figure 2-1: *AQUILA Resource Control Layer.*

2.1.2.2 Resource Control Agent (RCA)

A node in the Resource Control Layer is called a Resource Control Agent and represents a portion of the IP network, which internally has the same QoS control mechanisms. An RCA is a generalisation of the concept of the Bandwidth Broker in the DiffServ architecture. RCAs are logical units that run on several physical configurations, e.g. one server per RCA or several RCAs co-located on one server. The QoS control mechanisms used in the underlying network are of varying nature, e.g. in some part the routers may not even support DiffServ - which means that there is only a trivial best-effort QoS control - while in other parts they may be DiffServ capable. Moreover, some parts of the network may allow dynamic reconfiguration of resources, e.g. by adding ATM connections, others may have a more or less fixed configuration, e.g. pure SDH or WDM sub-networks. Another reason for the introduction of separate RCAs is that sub-networks are domains managed by different operators.

A Resource Control Agent is able to observe and in some sense to influence the actual configuration in the network portion it represents. Configuration parameters may describe the fraction of a network connection devoted to a specific DiffServ traffic class or the existence of a virtual connection (in ATM networks) with a specified bandwidth.

2.1.2.3 Admission Control Agent (ACA)

A DiffServ network can only provide Quality of Service, if it is accompanied by an admission control, which limits the amount of traffic in each DiffServ class. The AQUILA architecture uses a local admission control located in the Admission Control Agent, which is associated with the ingress and egress edge router or border router. To enable the ACA to answer the admission control question without interaction with a central instance, the RCA will locate objects representing some share of the network resources nearby the ACA. Resources are assigned to these objects proactively.

Admission control can be performed either at the ingress or at the egress or at both, depending on the reservation style.

The ACA will just allocate and de-allocate resources from its associated share. The ACA is not involved in the mechanisms used by the RCA to provide this resource share, to extend and to reduce it.

Resources are handled separately for incoming traffic (ingress) and for outgoing traffic (egress). The following description of resource distribution applies to both.

Resource distribution is performed by the RCA in a hierarchical manner using so-called *Resource Pools*. For this purpose it is assumed, that the DiffServ domain is structured into a backbone network, which interconnects several sub-areas. Each sub-area injects traffic only at a few points into the backbone network. This structuring may be repeated on several levels of hierarchy.

2.1.2.4 End-user Application Toolkit (EAT)

The End-user Application Toolkit (EAT) aims to provide access to end-user applications to QoS features. The EAT is a middleware between the end-user applications (Basic Internet Applications and Complex Internet Services) and the AQUILA network infrastructure.

The EAT supports two major kinds of (Internet) applications:

- Legacy Applications that are in fact QoS-unaware and that cannot be modified in order to directly access the EAT or any other QoS infrastructure. The most of existing Internet applications are legacy ones.
- QoS-aware Applications that can themselves request for QoS, by using an API, for example (EAT-based Applications use the EAT API), or by using signalling protocols such as RSVP and SIP.

Internet applications, however, have also to be distinguished with regard to their *complexity*. In AQUILA, we make a distinction between Basic Internet Applications and Complex Internet Services. They have to be supported in different ways: Whereas Basic Internet Applications are often legacy ones which cannot directly use the EAT, Complex Internet Services can be QoS-aware or even EAT-based although they consist of basic applications.

Generally, the EAT provides – at the control plane – a set of application interfaces in order to support the wide range of different applications (Figure 2-2):

- ***Legacy applications*** do not interact with the EAT. QoS reservations must therefore be made manually. For that reason, the EAT offers some **Graphical User Interfaces (GUIs)** for manual reservation requests (see below).
- For some ***specific legacy applications*** that dynamically negotiate data port numbers or rely on signalling protocols, special **Protocol Gateways (Proxies)** (e.g. for H.323, SIP) enable the selective processing of the application's control plane information by forwarding QoS-relevant data to the EAT Manager in order to initiate QoS requests. The Proxy Framework is flexible and extensible in order to include additional Proxies (e.g. for RSVP) later on.
- For ***QoS-aware, EAT-based applications***, an **Application Programming Interface (API)** provides interfaces and methods for login, reservation requests and releases, etc. This proprietary API is accessible via CORBA and provides the full AQUILA functionality. The **EAT Manager** directly implements the API in order to manage user access and reservations. (The EAT Manager is the main part of the EAT and controls the whole process. It also acts as mediator between the other EAT components and towards the ACA.)

Due to the fact that the EAT is fully transparent for legacy applications – even if they are supported by a Proxy – QoS reservations must be performed in a different way. For that reason, the EAT provides a set of GUIs in form of Web pages (the so-called **AQUILA Portal**), in which an end-user can *manually* request for QoS reservations. Moreover, the so-called AQUILA Portal offers among other things two different reservation modes: an advanced one for end-users that have knowledge about the technical details of an AQUILA request, and a regular one for end-users that are not familiar with AQUILA.

In order to support the regular reservation mode, an additional application "interface" is provided, the so-called **Application Profile** methodology. Application Profiles contain reservation "schemes" with technical parameters mapped to well understandable QoS metaphors. The **Converter** is the component which takes care of the mapping/converting of the technical parameters of the profiles and the (by the end-user subscribed) network services into the QoS metaphors corresponding to the application in use.

Note that the regular reservation mode is not necessarily part of the AQUILA Portal. In fact, Application Profiles are usable via the EAT API and can therefore be called by every Complex Internet Service that wants to make use of the AQUILA QoS capabilities. In that way, such an Internet service may offer its own regular reservation mode, by showing the QoS metaphors from the proper Application Profiles of its basic applications/plug-ins.

The following figure gives an overview on the above mentioned interfaces and components of the EAT, and how they interact:

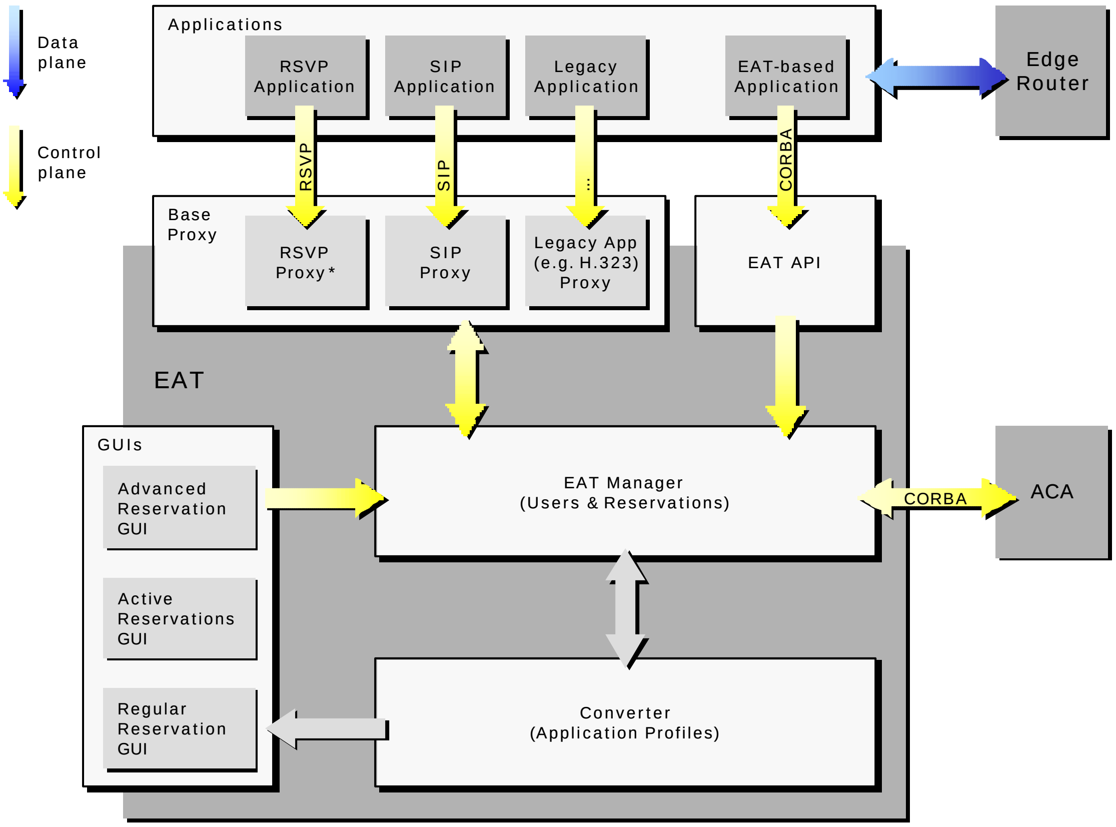


Figure 2-2: *EAT's basic building blocks and application interfaces.*

2.1.2.5 Distributed QoS Measurement

Advanced measurement and monitoring is a base to ensure and supervise QoS and performance parameters of applications over QoS-based IP networks and to verify them and to optimise their behaviour. To ensure that the developed architecture and its implementation is practically useable for providing application-specific QoS demands, a distributed QoS measurement infrastructure with several application-like traffic generators was developed. Measurements are able to simulate real users with different behaviours simultaneously within a test laboratory trial to prove the stability of the proposed architecture before integrating it into the more complex and expensive field trial with real user scenarios. The distributed QoS measurement enables the project to evaluate specific network and application profiles which cannot be realised in a field trial.

Distributed QoS measurement introduces new functionality for the analysis of applications and protocols like automation of test scenarios with different protocol parameters and network configurations ("tuning"). It is based on distributed measurement agents within different kind of networking components controlled remotely by an operator via a user-friendly graphical interface. This allows specification and execution of measurement test suites in different modes (multiplexed, point-to-point, point-to-multipoint, multicast), traffic characteristics, QoS measurement requirements and resource reservation parameters dependent on the applications. These can be stored in a measurement information database together with network device parameters and the measurement results. The calibration curves for admission control can be calculated from this database.

More information about the project can be found in [AQ-HOME].

2.1.3 Service Management

The AQUILA project aims at the *dynamic* provision of Quality of Services features for end-users over the existing Internet. For that, the AQUILA network offers different **network services** with different *predefined* QoS characteristics to the customers of the network and implements them internally by different **traffic classes**. Network services can be seen as products provided by the QoS-enabled AQUILA network and designed for typical application requirements.

The AQUILA project have defined four network services that are in fact four manageable premium transport options beside best effort for IP user traffic:

- **PCBR (Premium Constant Bit Rate)**, designed to serve a constant bit rate traffic. Examples of applications: voice trunking and virtual leased lines. This service should support circuit emulation and meets hard QoS requirements with respect to packet loss ratio (not greater than 10-8) and packet delay (not greater than 150 ms, low jitter).
- **PVBR (Premium Variable Bit Rate)**, designed to provide effective transfer of streaming flows of variable bit rate type. The traffic description of a flow has two parameters to declare, the Sustainable Rate (SR) and Peak Rate (PR). Policing assumes double token bucket. For the purpose of admission control algorithm, the notion of effective bandwidth (evaluated on the basis of SR, PR and dedicated for this service link capacity) is used.
- **PMM (Premium Multi-Media)**, designed to support greedy and adaptive applications that require some minimum bandwidth to be delivered with a high probability. Although the PMM service is not primarily targeted for applications using TCP, but there is optimisation regarding the TCP transport protocol.
- **PMC (Premium Mission Critical)**, designed to support non-greedy applications. The sending behaviour may be very bursty. This requires a very low loss and low delay service to be delivered with a high probability. Throughput is of no primary concern for PMC applications. There is an optimisation regarding the TCP transport protocol.

The network services and their detailed characteristics are defined by the network operator. Their goal of them is to provide a few specific offerings from the network operator to the customer, which are relatively easy to understand, suitable for a specific group of applications, and maintainable in large scale networks.

The network services are store as XML data (based on a common Document Type Definition) on a central drectory server. The **QoS Management Tool (QMTool)** provides for network operators access to the network services. It is able to retrieve the XML data from the server, to modify the entries in order to adapt the network service parameters, and finally to store the adapted entries on the server. (Even new network services can be created in this way.)

Customers can subscribe network services in order to have the policy to request for them for their applications. More specifically, customers initiate via the **End-user Application Toolkit (EAT)** QoS requests by firstly selecting a network service, which can be seen as *predefined SLS*, and secondly by giving additional data for the chosen **Service Level Specification (SLS)** such as:

- Scope, indicates the typology of the ongoing reservation with reference to the end-points of the traffic flows
- Flow identification, focuses on the association between packets and SLSs
- Traffic description, describes the traffic relevant to the reservation
- Performance guarantees, describes additional QoS requirements the customer and the commitment of the network operator to fulfil theses requirements
- Service schedule, provides the information related to the start and the duration of the service

The AQUILA notation is a practical utilisation of the notation, developed by the TEQUILA project and follows recommendations of the CADENUS project.

2.1.4 Resource Management

In chapter 1.1.2 we explained the AQUILA approach of the Resource Control Layer. Here we will focus on two aspects: the Resource Pools, and the design and implementation of BGRP for the Inter-domain approach of QoS provisioning in IP networks.

2.1.4.1 Resource Pools

Resource distribution is performed on a per DiffServ class basis. In the first trial, there was no dynamic reconfiguration of DiffServ classes. So, the resources of each class could be handled separately and independently of each other. This per class distribution however is not appropriate for edge devices, which are connected via small bandwidth links to the core network.

Resources are handled separately for incoming traffic (ingress) and for outgoing traffic (egress). The following description of resource distribution applies to both.

Resource distribution is performed by the Resource Control Agent (RCA) in a hierarchical manner using so called **Resource Pools**. For this purpose it is assumed, that the DiffServ domain is structured into a backbone network, which interconnects several sub-areas. Each sub-area injects traffic only at a few points into the backbone network. As described later, this structuring may be repeated on several levels of hierarchy.

When considering the resources in the backbone network, all traffic coming from or going to one sub-area can be handled together. So it is reasonable to assign a specific amount of bandwidth (incoming and outgoing separately) to each sub-area.

Depending on the topology of the backbone network, it may be useful to add some degree of dynamic to this distribution. The RCA may assign a larger bandwidth to one specific sub-area, when the bandwidth is reduced in other sub-areas. This dynamics may be described by the following formulas:

$$r_i \leq R_i$$

$$\sum_i r_i \leq R$$

where r_i is the resource limit actually assigned to ACA$_i$ and R_i is an upper bound for this value. R is the overall limit of all resources distributed to all Admission Control Agents (ACAs). These formulas express the following behaviour:

- The bandwidth assigned to each lower level entity r_i must not exceed an individual limit for this entity R_i. This limit R_i reflects the linkage of the lower level entity (e.g. sub-area) to the upper level entity (e.g. core network).
- The sum of the bandwidth assigned to all lower level entities must not exceed an overall limit R.

Depending on the values chosen for R_i and R, a more or less dynamic behaviour can be achieved.

Please note, that describing bandwidth with a single value (bits per second) is not sufficient in all cases. The characteristics of the traffic have to be taken into account. This may lead to an "effective bandwidth" formula, which is specific for each traffic class. It may also be necessary to describe bandwidth with a much more complex data structure, for which "addition" and "comparison" may be defined as rather complicated operations.

Resource shares are completely managed by the RCA. The resource share object itself is responsible to manage its resources and to check, whether a new bandwidth allocation request fits into the available bandwidth. If the amount of available bandwidth crosses some low-water-mark, the resource share object may precautionary request more resources from the resource pool. On the other hand, the resource share object will return unused resources to the pool.

Within a sub-area, there may be further subordinated sub-areas, which could be handled similar. Each resource share r_i assigned to a sub-area can be handled again as a resource pool R, which is distributed in a similar way among the sub-areas. Finally, resources can be used by ACAs as "consumable ResourceShare".

The depth of this hierarchical structure may be chosen as needed. It is also possible to mix several degrees of hierarchy, e.g. to break down the structure near edge routers more deeply than the structure of border routers, which are likely to be directly connected to the backbone.

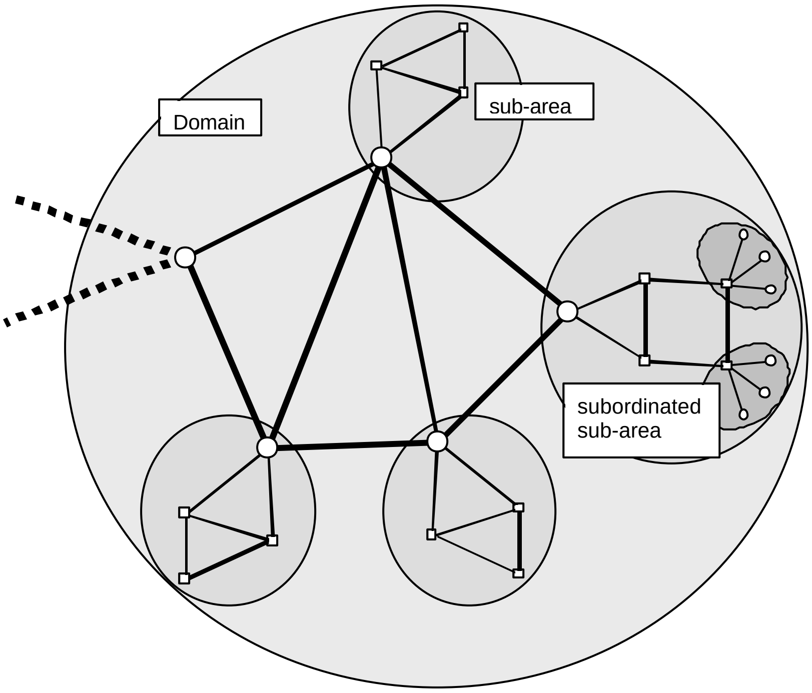


Figure 2-3: *Hierarchical resource pools.*

The figure above illustrates this. It shows an example domain, which contains four sub-areas and one border router. In one of the sub-areas, the further division into subordinated sub-areas is illustrated.

Obviously, the ability to structure a domain like this strongly depends on the topology. In the access area of a network however it is likely, that tree-like structures exist, which enable the definition of such a structure.

2.1.4.2 Border Gateway Routing Protocol (BGRP) Appliance

BGRP is a framework for scalable resource control [AQ-BGRP]. It assumes, that BGP is used for routing between domains (autonomous systems, AS).

The basic idea of BGRP is the aggregation of reservations along the sink trees formed by the BGP routing protocol. It is a characteristic of the BGP routing protocol to forward all packets for the same destination AS to the same next hop AS. This property guarantees the formation of a sink tree for each destination AS. All traffic destined for the same AS travels along the branches of this tree towards the root.

Similar to the QBone approach, some kind of "bandwidth broker" is established in each domain. However, not just a single entity is responsible for the whole domain. Instead, a BGRP agent is associated with each border router. Reservations for the same destination AS are aggregated at each BGRP agent. This has the following implications:

- The number of simultaneous active reservations at each domain cannot exceed the number of autonomous systems in the Internet.
- The source and destination addresses cannot be carried in the reservation requests between domains, because of the aggregation mechanism.

However, the aggregation mechanism does not automatically reduce the number of signalling messages. Each request may still travel end-to-end. Additional damping is necessary, e.g. by reserving additional resources in advance or by deferred release of resources.

In summary, the BGRP framework provides a possible approach to a scalable inter-domain architecture. However, the following issues have to be solved:

- Introduction of a damping mechanism as described above. The authors of [AQ-BGRP] make some proposals here. However, also the experiences from the resource pools used for the AQUILA intra-domain resource allocation are well suited to address this topic.
- Because BGRP messages not always travel all the way to the destination domain, the problem of QoS signalling within the last domain towards the destination host has to be solved.
- BGRP is still a framework only. The detailed information exchange between BGRP bandwidth brokers as well as the interaction with the intra-domain resource control has to be specified.

Inter-domain Requirements

An architecture for the AQUILA inter-domain resource control has to fulfil the following requirements:

- Scalability

  When high quality services will be established in the Internet world-wide, the number of individual resource reservations will grow rapidly. The architecture must be able to cope with that.
- Works with multiple intra-domain resource control mechanisms

  Operators should be free to use any resource control mechanism within their domain. The AQUILA intra-domain approach is just one possible example. An interface must be defined and standardised, through which the inter-domain resource control interacts with the domain specific QoS mechanisms.
- Edge-to-edge QoS guarantee

  The architecture must be able to support a certain level of QoS guarantee from the ingress edge of the source domain to the egress edge of the destination domain.
- Stepwise deployment

  It must be possible to deploy the architecture in the Internet step by step. An architecture, where any modification or enhancement has to be installed in each AS, is not acceptable.

Inter-domain Architecture

In order to fulfil the requirements listed above, an architecture according to the BGRP framework will be chosen. However, a number of extensions and enhancements have to be added to make a running implementation out of the framework.

Also, ideas and mechanisms developed for the intra-domain resource control will also influence the AQUILA inter-domain architecture.

This chapter specifies the general architecture for the AQUILA inter-domain resource control, where the next chapter addresses detailed aspects.

The following picture gives a rough overview of the architecture and depicts the basic interactions between the intra- and inter-domain resource control layer in the source, intermediate and destination domain.

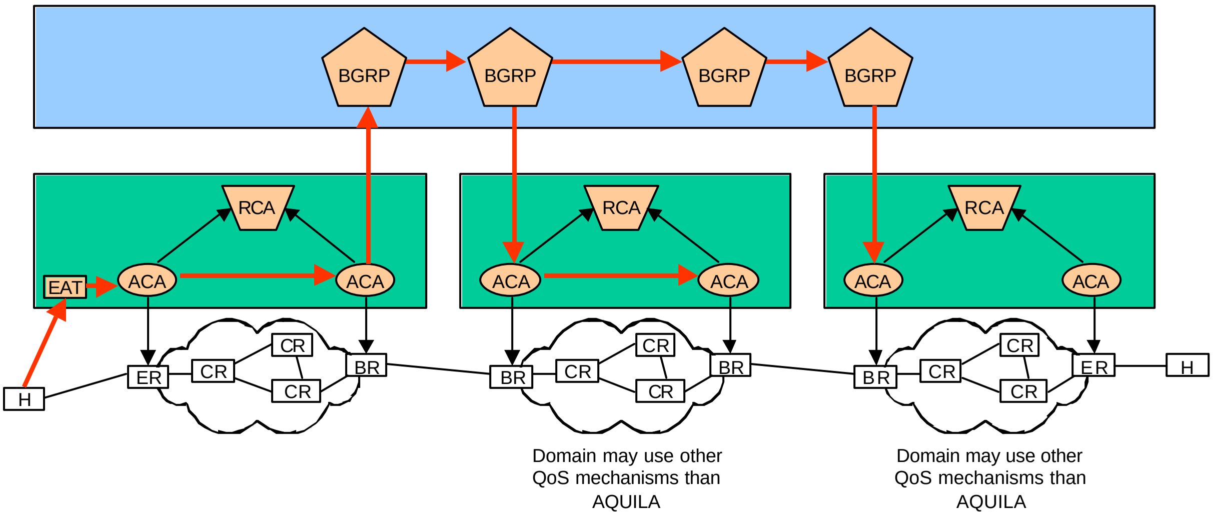

BGRP
BGRP
BGRP
BGRP
RCA
RCA
RCA
EAT
ACA
ACA
ACA
ACA
ACA
ACA
H
ER
CR
CR
CR
BR
BR
CR
CR
CR
BR
BR
CR
CR
CR
ER
H
Domain may use other QoS mechanisms than AQUILA
Domain may use other QoS mechanisms than AQUILA

Figure 2-4: *General inter-domain architecture and message flow.*

A so-called BGRP agent is associated with each border router. These agents interact with the AQUILA intra-domain resource control layer in the following way:

- Inter-domain resource requests are initiated by the ACA associated with the egress border router of the initiating domain and sent to the corresponding BGRP agent.
- BGRP agents associated with ingress border routers use the ingress ACA to establish intra-domain resource reservations.

Further information on the AQUILA project can be found at [AQ-HOME].

2.2 CADENUS (IST-1999-11017)

2.2.1 Objectives

CADENUS is building an integrated solution for the dynamic creation, configuration and provisioning of end-user services with QoS guarantees in Premium IP networks. The partners are developing, implementing, validating and demonstrating elements of a complete system that will support dynamic service creation, service selection and service configuration.

Much emphasis is pla ced on the business processes involved throughout the chain of events, and in this respect the software implementation is based on the commonly used ebXML.

The ebXML framework aims at creating a single global electronic marketplace where enterprises of any size and in any geographical location can meet and conduct business with each other through the exchange of XML based messages. In order for enterprises to conduct electronic business, they must first discover each other and the products and services they have to offer. They then must determine which business processes and documents are necessary to obtain those products and services. Afterwards, they need to find out how the exchange of information will take place and then agree on contractual terms and conditions. Once all of this is accomplished, they can finally exchange information according to these agreements.

The specification of a business process is the main activity required when creating a new service. Afterwards, in order to enable effective negotiation, it is needed that any interested party defines and publishes a Collaboration Protocol Profile (CPP), where a reference to the business process is made, together with the definition of the role that the party wants to play inside such a process. The CPPs, in turn, form the basis for Collaboration Protocol Agreements (CPAs) established between business parties. Ultimately, the business processes specified in the CPAs drive the business service interfaces to execute those processes and send the required documents.

Network Management aspects (especially the relationship with the TMForum's Telecommunication Operators Map) and security (at all levels throughout the architecture) are also addressed.

The key objectives of the project are:

1. To **define an architecture** in which the relationship can be seen between end-user services requiring QoS, and the Premium IP network transport services used to deliver these services. To be taken into account are the resources reserved on registration/subscription, and those that are used - and subsequently modified - when the service is invoked/configured.
2. To **identify, specify, design and develop the key components** of the architecture. These are: Access Mediator, Service Mediator and Resource Mediator.
3. To consider the current business processes involved, including especially the definition of -, (automated) translation of -, and increased flexibility and dynamic nature of **Service Level Agreements (SLAs) and Service Level Specifications (SLSs)**.
4. To define a standard way to **create and manage** SLAs.
5. To trial and demonstrate the efficient delivery of **end-user services with QoS** guarantees via this architecture.
6. To show how the **service creation and configuration** processes within the architecture have generic functionalities that may be exploitable for futuristic services.
7. To **disseminate the results** in standards bodies.
8. To produce recommendations, architectures, mechanisms and policies concerning service configuration and provisioning for both **network operators and service providers** .

2.2.2 Architecture

The CADENUS solution is based on an architecture (see Figure 2-5), which includes key functional blocks at the user-provider interface, within the service provider domain, and between the service provider and the network provider. The capabilities of these functional blocks are reflected in the corresponding SLAs/SLSs.

The three key components in this process are: Access Mediator, Service Mediator and Resource Mediator. The overall mediation procedure includes the mapping of user-requested QoS to the appropriate service-/network- resources, taking into account existing business processes. The architecture is being proposed to ETSI and ITU as the basis for Next Generation Networks. Contributions on the corresponding SLAs and SLSs are being made to the IETF.

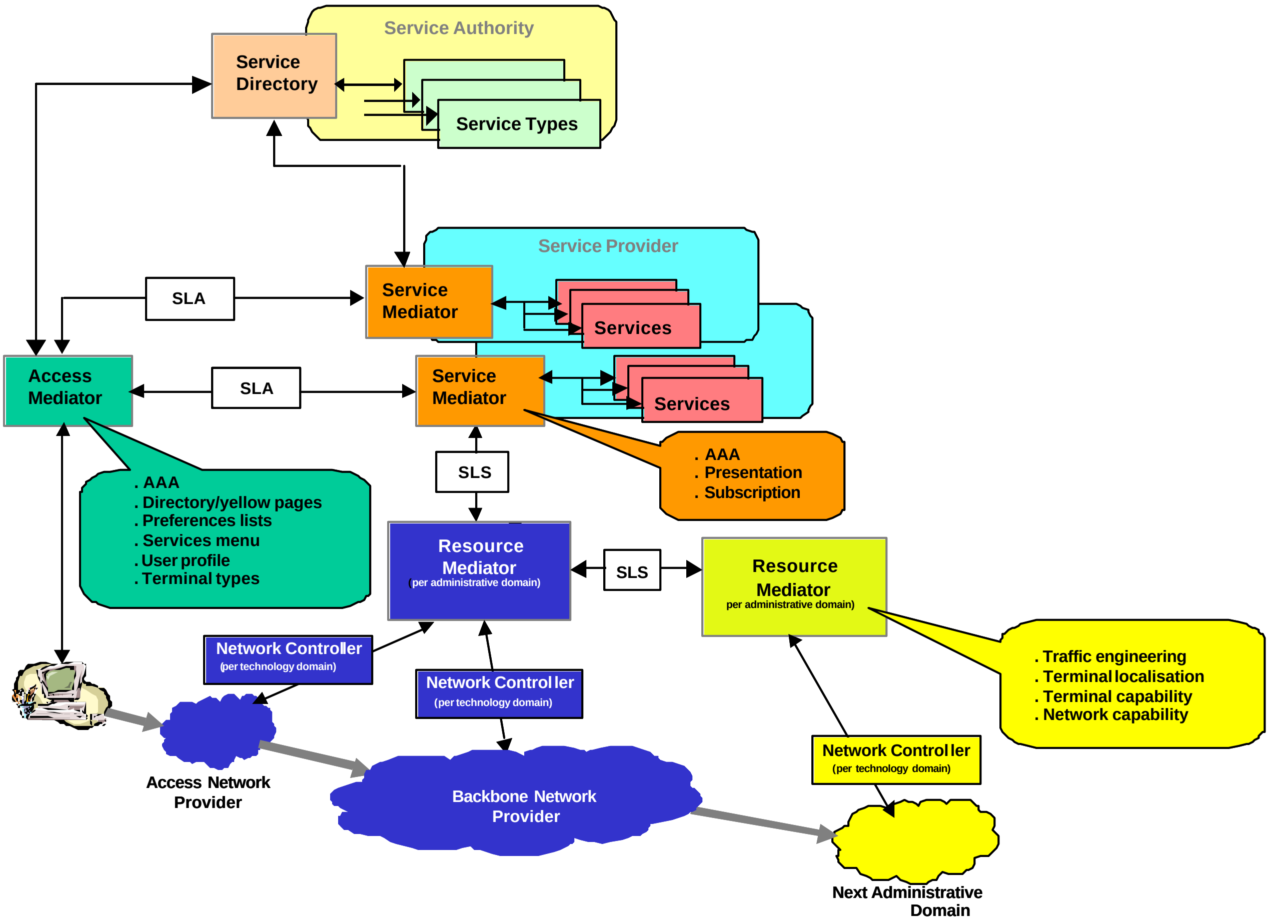


Figure 2-5: *The CADENUS Architecture*

2.2.2.1 Access Mediator (AM)

The Access Mediator presents the current service offers to the user. The source of the services is a so-called "Service Directory" database. The Service Directory assumes a role that is of paramount importance for the CADENUS framework. The Service Directory:

- contains the business processes of the standardised services, together with the associated components (GUI and SLA template),
- gives an SM the possibility to publish its own profile, together with the services it offers,
- gives the AM the possibility to retrieve information about the portfolio of services and about the SMs that are offering them,
- acts both as a registry and as a repository.

The Service Directory is implemented by exploiting the UDDI (Universal Description, Discovery and Integration) technology: a framework for the description and discovery of services based on the creation of a world-wide registry aimed at facilitating integration. UDDI uses XML to represent data and SOAP (Simple Object Access Protocol) to exchange messages, thus solving the integration and interoperability problem via a layered approach. By means of the Publisher's API, companie s may register information about the Web Services they offer; such information can then be retrieved by other companies via the Inquiry API. The data provided in a business registration is basically a categorisation of the companies/services based on taxonomies and/or standard identification mechanisms, and technical information about the Web Services offered by a company (e.g. endpoint URL, names and arguments of the methods that can be invoked, etc.).

To cope with the problems related to scalability and reliability, the UDDI business registry is implemented as a logically centralised, but physically distributed service, with multiple root nodes (also called site operators) that replicate each other's data on a regular basis. Once a registration is made at a specified root node, the data is automatically shared with the other site operators, thus becoming freely available to anyone who is interested in discovering the Web Services that have been exposed by a given company.

The Access Mediator:

- is the point of access for a user to the CADENUS system;
- performs AAA aspects;
- presents the services to the user;
- acts both as a registry and as a repository of information pertaining to the user's profile and the services he/she has subscribed to;
- performs SLA compliance checking.

The Access Mediator also maintains the several passwords, etc., in order to assist and ease the service selection process. This functionality may be under the control of a trusted 3rd party, and appears to provide novel opportunities for a value-added service provider or existing operator.

After authentication, the user requirements are captured, and the Access Mediator sends the information to the service provider who then employs the Service Mediators and Resource Mediators to map the requested and subsequently selected service into the deployed physical network. After the service selection has been agreed with all parties, the SLA is "signed" between the user and the service provider.

Records of usage and the associated SLAs are stored in the Access Mediator for future reference.

The graphical user interface associated with the Access Mediator will also be developed in the project, and is expected to provide a harmonised interface to the user for the CADENUS services under investigation (VoD, VoIP, VPN).

In the case that the end-user is attached to a corporate network, the Access Mediator has the additional role of representing the combined traffic profile from all the users attached to the LAN, and to negotiate with the service providers on the basis of this aggregated profile.

2.2.2.2 Service Mediator (SM)

The Access Mediator may form associations with one or more Service Mediators to which requests are issued. Generally off-line, the Service Mediator supervises the incorporation of new services, their presentation in the "Service Directory", and the management of the physical access to these services via the appropriate underlying network, using the Resource Mediator(s). It is the task of the Service Mediator to prepare the SLA for the user to sign, and subsequently to authenticate the user and map the SLA from the Access Mediator into SLSs to be "signed" with the Resource Mediator(s).

In the case that several underlying administrative domains are involved, the Service Mediator may (if it is aware of all the administrative domains) sub-divide the request from the Access Mediator into multiple SLSs ("hub" model); else it passes the SLS to the first Resource Mediator and relies on it to pass on a modified SLS to the adjacent domain ("cascade" model).

In the case that the service is essentially one of connectivity, the Service Mediator may negotiate an SLS for bulk bandwidth from the Resource Mediator. For other services, at the time of invocation, there may be a need to pass parameters from the retail-SLA to the Resource Mediator.

The Service Mediator has an important role in CADENUS, as this is the place through which created services are incorporated into the architecture; part of this process involves communication with the Service Authority to propose new services to be "standardised". Once accepted by the Service Authority, such types of new services are then entered into the registry. The Service Mediator can then publish in its profile that it is a "seller" of these services, and the Access Mediator can publish in its profile that it is a "buyer" of these services. Both the Service Mediator and the Access Mediator can then query the registry to find each other and establish an agreement.

The Service Mediator:

- Performs AAA aspects
- Checks for SLA compliance (including monitoring)
- Quantifies the resource requirements (translates the SLA into an SLS)
- Supervises service integration, including generating entries into a Service Directory (for subsequent presentation to users)

The SM interacts with the Servic e Directory and the entity managing it, the Service Authority, to perform the following functions:

- Registry Browsing/Querying:
  - list of defined Service Types: this function provides the list of all Services defined in the CADENUS taxonomy.
  - list of BusinessEntities implementing a specific service type ,
  - list of BusinessEntities implementing a specific service type and all the subcategories,
  - list of BusinessEntities implementing a specific BusinessService.
- Registering for a Service:
  - In order to register the SM for a new service, the SM must specify the CADENUS service type of the new service. These are the services used by the AMs.
- Modification of a Service definition
- Cancellation of a Service definition

New service proposals to the Service Authority will follow a different process that typically will involve several interactions between the Service Provider and Service Authority.

The Service Mediator informs the network resource components about the impacts of service reconfigurations and informs the Access Mediators of all new service offerings, in order that they can present these to their users. The Service Mediator also has to check that the addition of a new service, or invocation of an existing service, will not affect the services that are currently operational.

A policy-based approach is one solution to handle the service requests and network resources, in a way that can be automated, and promises to be scalable. Subsequent to the service creation, a policy extension could be applied to the network to ensure that all services can be managed correctly. The system would have a common view of the configuration of the devices (including an accounting system) and the policy rules, to be applied. In such a case, it would be the function of the Service Mediator to update the service level management system with new rules and configuration as required (in conjunction with the Resource Mediators and the network resource management functionalities).

2.2.2.3 Resource Mediator (RM)

There is one Resource Mediator per administrative domain (“Autonomous System”), and one Network Controller for each network technology within that domain (e.g. one Network Controller for the ADSL “technology domain”, one for the DiffServ “technology domain”, one for the MPLS “technology domain”).

The Resource Mediator is associated with the underlying network and its capabilities for supporting QoS, but the communication between the Service Mediator and the Resource Mediator is generic (i.e. independent of the technology employed by the underlying network). This interface conforms to the TEQUILA SLS[1]. Subsequent reservations are made between the Resource Mediator(s) and the appropriate networks via the Network Controllers.

The communication between the Resource Mediator and the Network is based on COPS-like policy rules.

The Network Controller translates non network-dependent policies into the configuration commands for the specific devices used in the network. In this sense, within the CADENUS Mediation Framework, the Network Controller is the only component that depends upon the specific network technology used. It has been introduced to clearly separate domain independent vs. domain dependent functionality, where technology dependence is on the QoS implementation model (e.g. whether it is DiffServ or MPLS) within a network domain.

The Network Controller provides network configuration in two steps:

- Service subscription: NDPR (Network Dependent Policies Repository) generation. This represents the theoretical network configuration. It is needed to give the Network Controller a view of the network (current and future). It does not affect the network behaviour.
- Service activation: VDPR (Vendor Dependent Policies Repository) generation. This is the starting point for the device configuration. Device configuration is made by via TC, or (depending upon the vendor) by some other policies in the device.

The generation and configuration is implemented via policy rules, and each router accesses the Repository LDAP to gather all the policies to be enforced.

The Service Mediator sends requests for information about network resource availability to the Resource Mediators.

A network provider wishing to offer its resources must support an interface capable of handling messages defining an SLS, from its network management system to one or more Resource Mediator(s).

2.2.2.4 The entity-group Communication Scheme

The architecture suggests a novel, generic approach to creating and configuring services in a dynamic way. The mediation mechanisms introduce features that could enable a generalised Service Creation environment, which extends beyond purely resource management. This feature is unique and innovative, but was considered to be outside the mainstream work in the project, and therefore only followed as an interesting aspect of research. Contributions in this area were made to the “Midbox” Working Group of the IETF.

This common feature of the communication process surrounding the Access Mediator, Service Mediator and Resource Mediator components is an “entity-group, search-and-selection” mechanism. In detail:

- the Access Mediator is responsible for selecting the appropriate service provider (from several), according to the user’s request,

[1] Internet Draft: draft-manyfolks-sls-framework-00.txt ,

- the Service Mediator is responsible for finding - and, in some cases, building from individual elements - the service, requesting information from - and selecting - the appropriate Resource Mediator,
- the Resource Mediators are responsible for selecting the appropriate network provider, or network capabilities (if the network provider is given), given several available options.

2.2.3 Service Management

CADENUS tackles the broad scope of *end-user service management*, focussing on the "higher-level" issues of Service Creation, Service Level Agreements (service subscription and invocation), business processes, AAA, etc. This focus is particularly visible, through the work done on the Access Mediator, and Service Mediator.

Services in the future will be more flexible and will demand more dynamic control of network resources. These actions will be reflected in the corresponding SLAs and SLSs.

Service selection is achieved through co-operation between the Access Mediator and the Service Mediator (see Figure 2-5). The Access Mediator:

- Interacts with the Service Directory to create a menu of services (yellow pages)
- Completes, signs, automates the retail-SLA
- Negotiates the (dynamic) aspects of the retail-SLA, including the choice of Service Provider
- Handles the registration/subscription interface for a user
- Performs QoS monitoring (user-side)
- Builds and maintains the user profile ("bookmarking" of preferences, e.g. for the choice of the most appropriate Service Provider, and filling of the corresponding Service Provider SLA template)
- Performs AAA functions and management of passwords for access to the various Service Providers
- Supervises the terminal type (this impacts the choice of Service Provider and the service requested from the Service Provider)

In a LAN-type of CPE environment, the Access Mediator can be placed at the boundary of the access network and also:

- Manages the internal traffic with respect to external resources
- Performs QoS aware multiplexing
- Presents an aggregated traffic profile for the retail SLA.

The Access Mediator may form associations with one or more Service Mediators to which requests are issued. Generally off-line, the Service Mediator supervises the incorporation of new services, their presentation in the "Service Directory", and the management of the physical access to these services via the appropriate underlying network, using the Resource Mediator(s). It is the task of the Service Mediator to prepare the SLA for the user to sign, and subsequently to authenticate the user and map the SLA from the Access Mediator into SLSs to be "signed" with the Resource Mediator(s).

Flexibility in Service Management is achieved through the use of software engineering techniques such as the Active Object Model, which is based on metamodels for designing highly customisable and reusable software. With this approach, the focus is on making *data* more reusable, by including in the object model of the application a number of objects, which provide explicit representation of other objects and their relationships.

Specifically, the Service Design Environment and a number of components in Service Mediator are based on an ‘Active Object Model’ approach. Following this design, the business rules that describe how to combine simple service elements and network resources, to deliver aggregated, end-to-end services according to commercial offers are represented in the object model. Entities describing new types of services, network resources, SLAs and commercial offers together with their relations can be added dynamically to the model. Generic applications, which implement a system’s functionality, are not impacted by the introduction of new services.

The system configurations needed to support a newly introduced end-user service are the following:

- Design the SLA Template (service offer), defining the different grades of service offered, including the different groups of SLA parameters and thresholds
- Define the Service Template, describes the Service Offering (i.e. an entry in the Service Provider’s Catalogue of Services) by means of Service Types, including meta-data information describing the characteristics of a type of Service, such as the hierarchy of included Service Types, the relationships and constraints among Service Types and the set of attributes for each Service Type
- Define the workflows for resource reservation (a set of ‘rules’ to be used by the system to determine the resource needs for a SLA) and service configuration activities (describing the steps to accomplish the service configuration phases, to be executed by specific automated agents or human operators). This represent processes internal to the Service Provider, as opposed to the business process that implements the AM-SM interaction
- Define SLA-SLS translation rules, describing the mapping between the QoS parameters and thresholds included in the SLA; first into an SLO for each elementary service in which the original service has been decomposed and then into an SLS (or a set of SLSs) to be sent to RMs to reserve the needed resources
- Define Data Format Adaptation rules, i.e. the mapping between "external" data formats, i.e. those exchanged between AM and SM, into the SM internal data formats (e.g. IP-VPN service request into the OSS specific internal service structure).

CADENUS follows a policy-based approach for handling the service requests and network resources, in a way that can be automated, and promises to be scalable. Subsequent to the service creation, a policy extension could be applied to the network to ensure that all services can be managed correctly. The system would have a common view of the configuration of the devices (including an accounting system) and the policy rules, to be applied. In such a case, it would be the function of the Service Mediator to update the service level management system with new rules and configuration as required (in conjunction with the Resource Mediators and the network resource management functionalities).

2.2.4 Resource Management

Whilst resource management techniques are not a major activity of CADENUS, the project has to be aware of the traffic control parameters that can be manipulated, the measurements that can be obtained, and the emerging schemes for intra-domain and inter-domain resource management.

CADENUS uses both MPLS and DiffServ networks as appropriate examples on which to validate their service selection, configuration and creation architecture. This architecture relies on interactions with the management interfaces of such networks for the reservation of resources that guarantee the QoS for the various services. A resource management implementation has been made, in order to validate the other CADENUS developments, based on the following scheme:

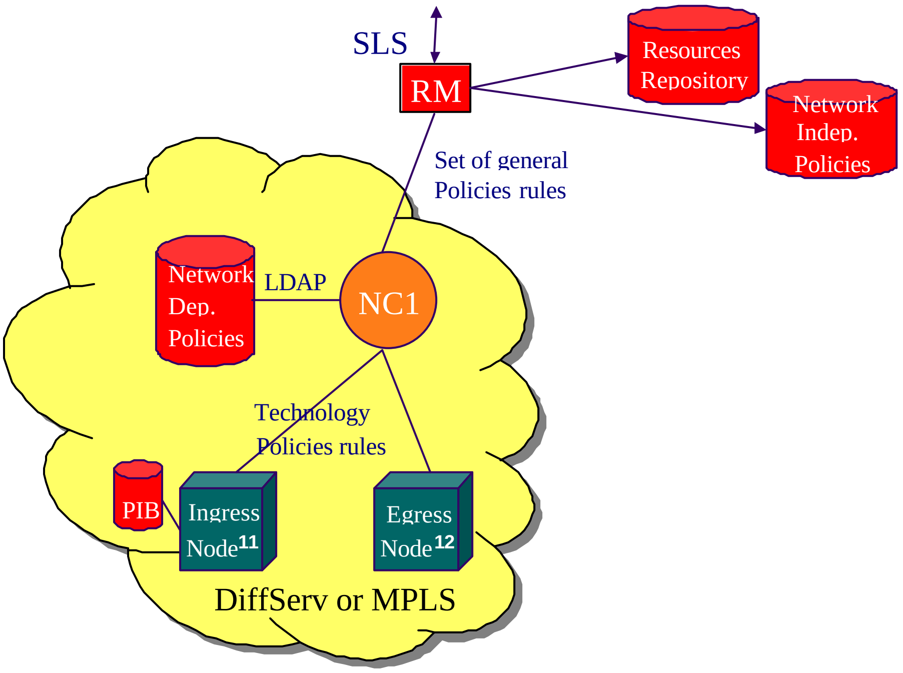


Figure 2-6: *Resource Management components in CADENUS.*

It is assumed that there exists a single instance of a Resource Mediator per «administrative domain». An administrative domain is an area in which a single Service Provider is offering all the elementary services included in the service "bundle" (e.g. for a VPN service, this might be: base access (non IP), to IP access, tunnelling etc.). This can be considered a single Autonomous System.

The CADENUS Resource Mediator manages the resources in its Autonomous System. Inter-domain communication is at the Resource Mediator level.

The Resource Mediator stores information about the resources it manages in a *Resource Repository*, which doesn't give the current usage/status of resources. The management of the *Resource Repository* consists basically in marking resources as *pending*, *committed* and *free*. The Resource Mediator receives requests in the form of SLSs from the Service Mediator and translates them into network independent device configuration policies that are stored in the *Network Independent Policies Repository*. The upper layer of the Resource Mediator is independent of the specific network technology.

There exists a single instance of a Network Controller for each network technology (e.g. DiffServ, MPLS).

The Network Controller (NC) takes as input a set of network independent policy rules and translates them into a set of network dependent policy rules that are stored in a *Network Dependent Policies Repository*.

It has to be defined whether the NC, when notified by the Resource Mediator, directly accesses the *Network Independent Policies Repository* in order to obtain the policy rules to be translated, or the NC has to be given the rules directly by the Resource Mediator itself. The latter would be better if we want to keep archives independent from each other.

The resource allocation will initially be based on the available and reserved resources only (using the total amount of resources, no overbooking or allocation based on long term statistical measurement).

Admission Control has to be performed at invocation time, for example in the case of a SLA, which has time specified (e.g. three times a week). In this case, there should be an Admission Control to ensure that the user has not already used the service and to allow or deny it. This functionality could be provided by the Resource Mediator in two different ways: asking the NC information about the status of the network or maintaining this information inside the Resource Mediator.

We will avoid mixed architectures (e.g. DiffServ, MPLS), i.e. we assume that access network and backbone network use the same technology, and do not intend to demonstrate concatenated domains.

The Resource Mediator is associated with the underlying network and its capabilities for supporting QoS, but the communication between the Service Mediator and the Resource Mediator is generic (i.e. independent of the technology employed by the underlying network). This interface conforms to the TEQUILA SLS. Subsequent reservations are made between the Resource Mediator(s) and the appropriate networks via network-specific Network Controllers.

The communication between the Resource Mediator and the Network Controllers still needs further clarification, but it will probably look quite similar to COPS-like policy rules.

One Resource Mediator is envisaged per administrative domain (“Autonomous System”), and one NC for each network technology within that domain (e.g. one NC for the ADSL “technology domain”, one for the DiffServ “technology domain”, one for the MPLS “technology domain”). If necessary, for performance reasons, Resource Mediators may be replicated within an Autonomous System. A configuration has been successfully tried using one RM for the access network and one for the core.

The design of the Resource Mediator will include 3 layers:

The **RM Inter-Domain layer (RMID)** provides:

- interfaces to the SM,
- gets the SLS,
- identifies the source and destination,
- asks the RMNI for local routing,
- splits the SLS and sends to the next RMID,
- manages the Admission Control via the layers below,
- manages terminal adaptation to the environment (mobility, UMTS, Cache Server, (plug-ins for (e.g. MPEG1, 2, 4),
- monitors adherence to the SLS,
- locates and selects any necessary plug-ins needed by the user for a particular service, of which he/she was unaware.

The **RM Network Independent layer (RMNI)** is a logical layer between the RMID and the RMND: Its main roles are:

- discovering which RMND is involved
- forwarding the SLS portion to be translated
- to be responsible for the inter-technology-domain communication
- to manage the Admission Control via the layer below (RMND).

The **RM Network Dependent layer (RMND)** provides:

- the interface to the network
- Admission Control
- policies generation/translation

- resource discovery

A network provider wishing to offer its resources must support an interface capable of handling messages defining an SLS, from its network management system to one or more Resource Mediator(s).

Further information on the CADENUS project can be found at [CA-HOME].

2.3 TEQUILA (IST-1999-11253)

2.3.1 Objectives

The objective of the project is to study, specify, implement and validate a set of service definition and traffic engineering tools to obtain quantitative end-to-end Quality of Service guarantees through careful planning, dimensioning and dynamic control of scaleable and simple qualitative traffic management techniques within the Internet (i.e., DiffServ). The following technical areas are addressed:

- Specification of static and dynamic, intra- and inter-domain SLSs to support both fixed and nomadic users.
- Protocols and mechanisms for negotiating, monitoring and enforcing SLSs.
- Intra- and inter-domain traffic engineering schemes to ensure that the network can cope with the contracted SLSs - within domains, and in the Internet at large.

All specified functionality has been validated through simulation, prototype development and network experiments.

The project has five key objectives:

- Study the issues behind, develop architectures for, and propose algorithms and protocols to enable: **negotiation, monitoring and enforcement of Service Level Specifications** between service providers and their customers and between peer providers in the Internet.
- Develop a functional model of co-operating components, related algorithms and mechanisms to offer a complete solution for **intra-domain traffic engineering** to meet contracted SLSs in a cost-effective manner.
- Develop a scalable approach, architecture and set of protocols for **inter-domain SLS negotiation** and **QoS-based routing** to enforce end-to-end quality across the Internet.
- **Validate** the above through both simulation and/or testbed experimentation.

Use, enhance and contribute to drafts, specifications and **standards** of the wider international community, participate in IST consensus activities and disseminate TEQUILA results.

2.3.2 Architecture

The next figure gives the high-level functional architecture for providing QoS in IP networks as it has been developed within the TEQUILA project. The architecture includes management, control and data-plane functionality. The QoS architecture shows the basic interactions between the provider and the customer, i.e. service subscription, service invocation and data-transmission. The customer may be a company, another (peer) network provider, an application service provider or a residential user.

The functional architecture describing the QoS functionality of the provider contains 5 sub-systems: Service Management, Traffic Engineering, Policy Management, Monitoring and Data-plane functions.

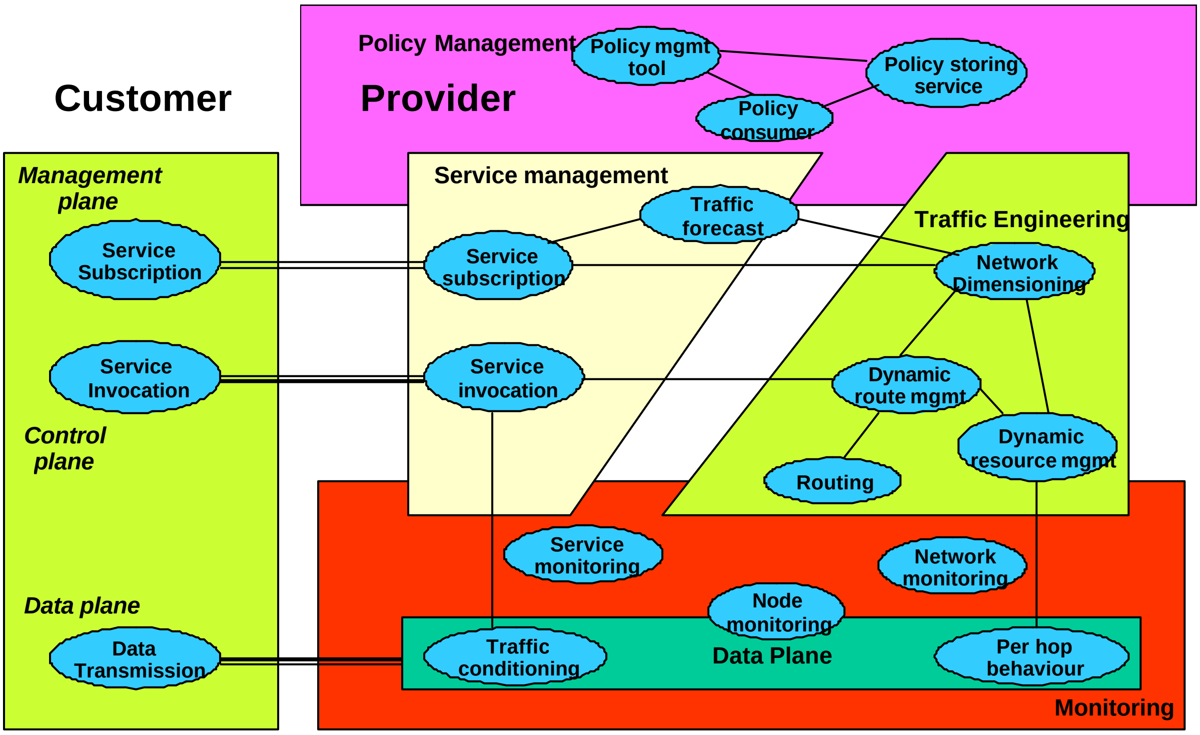


Figure 2-7: *TEQUILA functional architecture.*

The “low-level” **data plane** includes the DiffServ PHB (Per-Hop Behaviour) and TCBs (Traffic Conditioning Blocks), while the “high-level**”** **policy management** allows the administrators to define and enforce policies for both Service Management and Traffic Engineering purposes in an automated way. **Monitoring** is sub-system, which includes node monitoring, network monitoring and service monitoring.

The **Service Management** and the **Traffic Engineering** sub-systems are the essential parts of the system architecture and are the main focus of TEQUILA. Service management includes service creation, negotiation and assurance. Service creation is the process of defining services and service classes by the provider. Service negotiation is the actual negotiation and subscription of value-added IP services between provider and customer. This operational, “on-line” process is the most critical w.r.t. QoS issues, scalability and other resource-related problems, and is one of the main topics addressed by TEQUILA.

Service assurance enables the operator to verify whether the QoS performance guarantees committed in SLAs are in fact being met in its network. This requires an in-service verification of throughput, delay and packet loss characteristics. Service Assurance operates on the statistical data gathered by network monitoring through the network elements.

Traffic Engineering (TE) is the process of specifying the manner in which traffic is treated within the network. TE has both customer and system-oriented objectives. The customers expect certain performance from the network, which in turn should attempt to satisfy these expectations. The expected performance depends on the type of traffic and is specified in the SLSs. The provider on the other hand attempts to satisfy the customer traffic requirements in a cost-effective manner. Hence, the target is to accommodate as many as possible of the QoS requests (as expressed in SLSs) by optimally using the available network resources. This (SLS) service-driven resource management and traffic engineering is another basic TEQUILA research topic. Within TEQUILA, both IP-based and MPLS-based TE techniques are studied.

Main Characteristics of the Architecture

The TEQUILA architecture emphasises the importance of the Management plane in providing QoS and gives a functional decomposition of the main service and resource management aspects. The key concepts are the following:

- The architecture introduces a two-level approach for (operational) service management and negotiation, i.e. service subscription and service invocation. Both processes occur at a different time scale. Subscription handles the longer term-based service requests that may apply to IP services like IP VPNs, while service invocation acts on a per-call basis, within the context of the deployment of VoIP (Voice over IP) services, for example. The two-level approach in service management is mirrored in the resource management system. The architecture combines a longer-term off-line traffic engineering approach (*network dimensioning component*) with a dynamic on-line handling of traffic fluctuations (the *dynamic route management and dynamic resource management components*).
- The architecture makes a clear distinction between the customer (SLS) aware components and the resource (QoS class) aware components. The Service Management sub-system has the knowledge about the customers, while the Resource Management sub-system knows about the network resources, and acts on the processing of (aggregate) traffic that will be handled by a collection of QoS classes. The inter-working between the two aforementioned sub-systems is clearly defined through the resource provisioning cycle, controlling the interactions between three elementary components of the TEQUILA system: service subscription, traffic forecast and network dimensioning.

The main overall result is that this architecture enables the (dynamic) provisioning of hard QoS guarantees to individual (multimedia) flows while still maintaining a scalable solution. It solves the scalability problem for IP backbones by enabling a two-level approach for admission control.

The TEQUILA architecture is outlined into more detail in the IEEE Communication Magazine issue of May 2001 [TE-01-ARCH].

More information can be found in the technical annex and in the TEQUILA reference papers [TE-01 to TE-06].

2.3.3 Service Management

TEQUILA focuses on **operational management of IP connectivity services**. Within the TEQUILA project, an IP connectivity service is described by a set of Service Level Specifications and is the result of a (successful) negotiation between a provider and a customer. Thus, the TEQUILA approach relies upon two basic notions, as far as the provisioning of a guaranteed level of quality related to the deployment of a given IP service offering (ranging from Internet access to IP videoconferencing) is concerned:

- An IP connectivity service is a set of SLSs as defined by the TEQUILA SLS-Internet draft [TE-02-SLS]. The main aspects of this draft are the unambiguous description of the service IP traffic profile and the network IP QoS guarantees, i.e. *the traffic and resource related aspects of the IP service*. This definition may then be used as an unambiguous API, from the (lower) IP transport layer to the (upper) application layer for defining end-user services (see Figure 2-8). However TEQUILA is not performing in-depth research in the area of end-user services or service creation, i.e. the process of (automated) service definition by the provider. This is an area where TEQUILA could learn from the results of the CADENUS project.

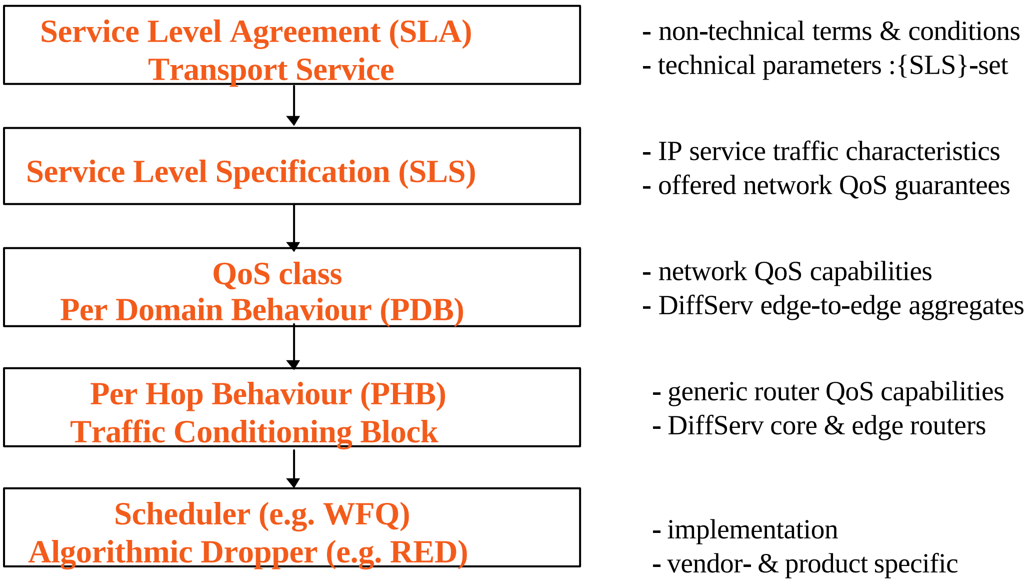

Service Level Agreement (SLA)
Transport Service
Service Level Specification (SLS)
QoS class
Per Domain Behaviour (PDB)
Per Hop Behaviour (PHB)
Traffic Conditioning Block
Scheduler (e.g. WFQ)
Algorithmic Dropper (e.g. RED)
- non-technical terms & conditions
- technical parameters :{SLS}-set
- IP service traffic characteristics
- offered network QoS guarantees
- network QoS capabilities
- DiffServ edge-to-edge aggregates
- generic router QoS capabilities
- DiffServ core & edge routers
- implementation
- vendor- & product specific

Figure 2-8: *Service Level Specifications in a layered DiffServ Service Approach.*

- An IP connectivity service is a contract between two parties (only), i.e. a *provider* and a *customer*, TEQUILA is not developing a complete (end-user) application service framework taking into account the business-related aspects and the different roles of the Internet stakeholders such as access providers, wholesalers, application provider, etc.
- One of the main features promoted by the TEQUILA architecture is a two-phase approach for service negotiation, i.e. service subscription and service invocation, assuming different time scales. This allows for a corresponding two-level based service admission control, which ensures hard QoS-guarantees to individual flows, while still maintaining scalability for large IP networks. For example a company may subscribe to an IP VPN service offering, which might then be used by its employees for conveying videoconferencing traffic (hence the invocation of multimedia services within the IP VPN). Another example is a voice over IP service provider, leasing a mesh of Virtual Leased Lines between Trunking gateways (subscription) and uses this virtual overlay network for offering voice over IP services to residential users (invocation of voice calls).

For more information about the TEQUILA service architecture, see [TE-04-SM]

Service Assurance and SLS Monitoring

SLS monitoring is an essential part in providing QoS and service assurance. It encompasses the in-service verification of traffic and performance characteristics of value-added IP services. The next figure shows the TEQUILA monitoring architecture as it is currently under implementation.

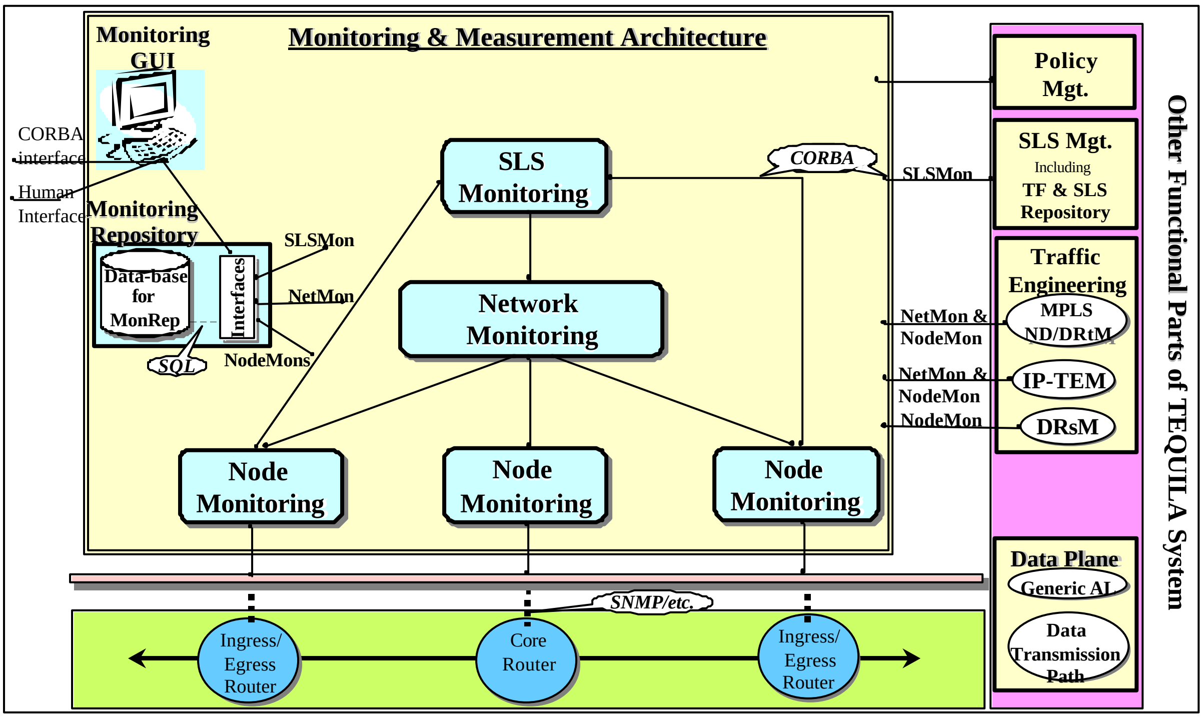


Figure 2-9: *TEQUILA Monitoring Architecture and its interactions with other parts.*

Service assurance and in-service verification is realised by the inter-play of several components.

Node Monitoring is responsible for node related measurements. A diverse variety of measurement data is needed in order to perform network and customer service performance and traffic monitoring. The variety of data, the magnitude of the raw data and the necessary processing of data near its source make a distributed data collection system more practical. Hence, the Node Monitoring is distributed across the network i.e., one Node Monitor per Network Element. **Network Monitoring** is responsible for any required network-wide post-processing of measurement data using statistical functions. It is in general, centralised and it utilises network-wide performance and traffic measurements collected by Node Monitors in order to build a physical and logical network view. **SLS Monitoring** is responsible for customer related service monitoring, auditing and reporting. SLS Monitoring is centralised, since it must keep track of the compliance of the level of service provided to the customer SLS instances, by analysing information provided by Network and Node Monitors. **Monitoring Repository** consists of two major parts for data cataloguing, a "data store" having a database functionality for storing the large amounts of data for monitoring components and an "information store" for storing smaller amounts of configuration type information. **Monitoring GUI** is used for displaying measurement results and can be used in a Network Operations Centre.

In general, the monitoring functions are split into four phases:

- ***Request***: Every component that requires monitoring information must register to one of the monitoring components (Node, Network, or SLS).
- ***Configuration***: Monitoring clients or Network Monitoring specify which Node Monitors are needed to be at the basis of any measurements and configure them.

- ***Execution***: Node Monitors perform the measurements based on these configurations.
- ***Reporting and exception***: The analysed measured data and events are sent back to the registered components.

More information on the TEQUILA monitoring approach can be found in [TE-06-MM].

2.3.4 Resource Management

The main objective of TEQUILA is a service-driven resource optimisation and traffic management for MPLS-based and (purely) IP-based networks. MPLS-based traffic engineering (TE) relies on an explicitly routed paradigm, whereby a set of routes (paths) is computed off-line for specific types of traffic. IP-based TE is a quite new area of research and relies on a 'liberal' routing strategy, whereby routes are computed in a distributed manner, as different routing options are discovered by the routers themselves. Although route selection is performed in a distributed fashion, the QoS-based routing decisions are constrained according to network-wide TE considerations made by the (logically centralised) network dimensioning component by calculating (and manipulating) the cost metrics used by the routing algorithms for route computation.

The main research work of TEQUILA and contributions is twofold. First, the inter-working between service and resource management and – second – the relationships between long-term (off-line) TE and short-term (on-line) TE. The TEQUILA architecture provides a framework for the interworking between service and resource management through the concept of the *resource provisioning cycle*, i.e. the interworking between service subscription, traffic forecast (forecasting the traffic based on the SLSs) and long-term, off-line traffic engineering (called network dimensioning).

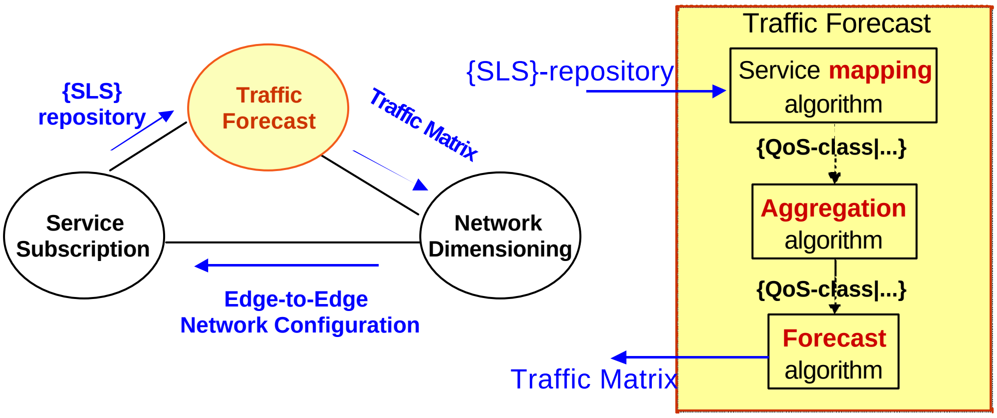


Figure 2-10: *The resource provisioning cycle in TEQUILA.*

The resource provisioning cycle enables a clear distinction between the customer (SLS) aware components and the resource (QoS class) aware components. The required "service mapping" of SLSs onto QoS classes is done by Traffic Forecast. The Service Management system has knowledge about all customers but is agnostic for the internal network details. The Resource Management system knows about all network resources but only acts on (aggregate) QoS classes. The QoS-classes in TEQUILA are parameterised edge-to-edge packet behaviours, comparable with the (recently) defined DiffServ *Per Domain Behaviours.*

Parameter	Comments
Ordered Aggregate	The allowed values are: Expedited Forwarding (EF), Assured Forwarding 1-4 (AF1, AF2, AF3, AF4), Best Effort (BE)
Delay	The *delay* is the maximum *edge-to-edge* delay that the in-profile packets of a certain IP stream should experience. It is a continuous parameter that may be worst case (deterministic) or a percentile (probabilistic).
Packet Loss	The *packet loss* is the upper bound of the *edge-to-edge* packet loss probability that in-profile profile packets of a certain IP stream should have.

Table 1: *TEQUILA DiffServ QoS class parameters.*

A finite number of QoS-Classes is obtained by discretising the number of allowed delay and loss values. The delay and loss ranges are determined by provider policy and gives flexibility to the operator for defining its own (finite number of) QoS classes. A network supports certain QoS classes by implementing dedicated PHBs in the core routers, appropriate Traffic Conditioning Blocks at the edge routers and an overall resource management capability implemented within the TEQUILA system.

The inter-working between the logically centralised off-line TE and distributed on-line TE is modelled by the interactions between Network Dimensioning (ND), Dynamic Resource Management (DrSM) and Dynamic Route Management (DrTM).

- Basically *Network Dimensioning* calculates the overall long-term network configuration and sets the guidelines (or boundaries) within the dynamic distributed components may operate. More exactly, ND is responsible for mapping the traffic onto the physical network resources and provides network-provisioning directives in order to accommodate the forecasted traffic demands. In an MPLS-based approach ND will e.g. calculate the explicit paths, while in an IP-based approach, the ND dynamically calculates the IGP traffic engineering metrics
- *Dynamic Route Management* is responsible for managing the routing processes in the network according to the guidelines produced by ND on routing traffic according to QoS requirements associated to such traffic, i.e. the contracted SLSs. DRtM is instantiated at all network edges and may e.g. load-balance the traffic over several explicit paths. *Dynamic Resource Management* has also distributed functionality, with an instance attached to *each* (core and edge) router. This component aims at ensuring that link capacity is appropriately distributed between the PHBs sharing the link. It does this by setting buffer and scheduling parameters according to ND directives, constraints and policy rules; and taking into account actual experienced load as compared to required (predicted) resources.

2.3.4.1 Policy-based Resource Management

Policy-based Management in TEQUILA provides the flexibility to the administrator to dynamically guide the behaviour of the components of the architecture resulting in configuration of the network as well as admission control decisions that reflect the business objectives of the operator. Policies are defined in the Policy Management Tool, which provides a “policy creation environment” using a high-level language, are translated to object-oriented policy representation (information objects) and stored in the policy repository (Policy Storing Service). After the policies are stored, activation information may be passed to the associated Policy Consumers, which are responsible for interpreting and enforcing the policies on the fly. In the TEQUILA architecture there exist many Policy Consumers, associated with particular functional blocks of the hierarchical management structure. Every time the operator enters a high level policy, this should be refined into policies for each layer of the TEQUILA functional architecture forming a policy hierarchy that reflects the management hierarchy.

For example, the functional blocks that are influenced by the enforcement of resource management policy, are Dimensioning and Dynamic Resource Management. Assuming a strict management hierarchy in the Tequila functional architecture, any function of the Dimensioning functional block will operate on managed objects of the Dynamic Resource Management functional block. Consequently, high-level resource management policies will be decomposed into dimensioning and dynamic resource management policies. In this architecture, the policy consumers will be probably tightly coupled with their respective functional blocks (Figure 2-11).

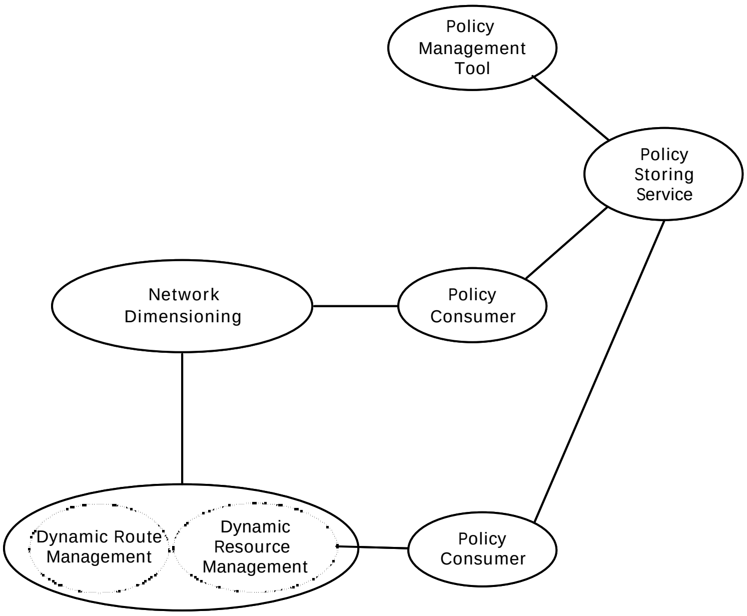


Figure 2-11: *Enforcement of the resource management policy at each level of the TEQUILA functional architecture.*

For more information about TEQUILA traffic engineering, see [TE-03-TE].

2.3.5 TEQUILA Summary

In summary, the following gives the main innovative strengths of the TEQUILA project

- A formal definition of an SLS template, which will aim at conveying QoS-related information for the provisioning of a guaranteed level of quality associated to the subscription of an IP service offering. This investigation work is currently promoted within the IETF community. A clearly defined mapping of service QoS requirements (through SLSs) and network QoS capabilities (through QoS classes)
- Holistic view for operational service & resource management and the related functional decomposition of a complete system. Scalability is obtained through:
  - A *Two-level based* service negotiation and admission control.
  - The *Resource Provisioning cycle*, allowing for a clear separation of the customer (SLS)-aware components and the resource (QoS-class)-aware components.
  - Well defined interactions between the long-term, centralised off-line TE and dynamic, distributed on-line handling of traffic fluctuations for MPLS- as well as IP-based networks
  - A Service assurance & SLS monitoring framework enabling an in-service verification of the service QoS requirements.

Further information on the TEQUILA project can be found at [TE-HOME].

3 POSITIONING OF AQUILA, CADENUS & TEQUILA

3.1 Common Goal

The three IST projects AQUILA, CADENUS and TEQUILA investigate IP Quality of Service support in large IP networks. The main objective of the projects is the same: providing Premium IP services over the Internet as a basic step towards the Next Generation Networks (NGN) of tomorrow. All the partners involved in these three projects consider that having this common goal is a very positive fact (since the acceptance of three projects shows that this is one of the most important concerns of today's research in IP services and networks) and an excellent opportunity to investigate the technical feasibility of different approaches for addressing this shared concern. The common goal and, by consequence, the unavoidable overlap of some of the technical areas being investigated by the three projects, is judged as a *strength and opportunity* of the IST Premium IP cluster and not at all as a threat or a weakness. More specifically, now that all three projects are running for more than two years, the following considerations and conclusions can be put forward:

- It is currently agreed upon in the international research community that Premium IP support over large IP networks (including the Internet itself), is a **very complicated technical issue** and **one of the biggest challenges** for today's operators and service providers.
- A wide and difficult technical area like IP QoS requires a broad community of researchers and identifies different tracks to be investigated. Therefore, these three IST projects involved in the IP QoS area are a promising means for obtaining significant research results that will promote and consolidate the importance of the European Commission funded research within the international community. One needs a critical mass for dealing with these difficult problems.
- The existence of three projects within the same (IP Premium) cluster gives the opportunity to tackle the problem from different angles and to highlight different aspects. This gives the opportunity to:
  - **Investigate different aspects of the same global problem**, e.g. service creation by CADENUS, operational service and resource management interworking by TEQUILA, and resource optimisation by AQUILA.
  - **Investigate different solutions for the same problem**, e.g. MPLS (off-line) traffic engineering in AQUILA, both MPLS and IP TE in TEQUILA and MPLS and DiffServ in CADENUS.
  - **Work together on the same problem and enhance the proposed solution of one particular project**. For example, the definition of the IP Connectivity Service Level Specification was first proposed by TEQUILA and then discussed and improved by inter-project collaboration.
  - Learn from each other.
- Apart from the technical inter-working mentioned above, the projects have proven to be perfectly capable to collaborate together on a broader scale and within the international research community. For example, they have worked together:
  - for organising an IETF SLSU working group
  - for workshops like in Amsterdam, January 2001, Capri in April 2001, Dresden in November 2001, and Maastricht in May 2002.

Other IST projects, which are known to be active in the Premium IP area, are: M3I, QoSIPS, DePAuDE, GCAP, FORM, MOEBIUS and SEQUIN.

- *M3I* is designing, implementing and trialling a next-generation system, which will enable Internet resource management through market forces, specifically by enabling differential charging for multiple levels of service. Offering this capability will increase the value of Internet services to the customers through greater choice over price and quality, and reduced congestion.

- *QoSIPS* (Quality of Service and Pricing Differentiation of IP Services) is developing innovative technologies for supporting QoS management, service differentiation and price setting of Internet Protocol Network Service Providers. QoSIPS will participate in the IP QoS cluster "open session" in Dresden (November 2001), with a view to determining whether this proje ct should work closer with AQUILA, CADENUS and TEQUILA.
- *DePAuDE* (DePendability for embedded Automation systems in Dynamic Environments) includes the design of a new architecture for dependable dedicated (intra-site) and IP (inter-site) mechanisms. DePAuDE will participate in the IP QoS cluster "open session" in Dresden (November 2001), with a view to determining whether this project should work closer with AQUILA, CADENUS and TEQUILA.
- *GCAP* is defining and evaluating a new end-to-end multimedia multicast transport protocol for supporting dedicated or specialised applications having guaranteed QoS requirements. The new QoS architecture will be based on IPv6 and DiffServ, and use an active network based technology.
- *FORM* is developing an exploitable set of services, systems and components that aims to manage outsourced, co-operative, inter-enterprise („interprise") facilities.
- *MOEBIUS* is integrating an IP-based, mobile Extranet platform, exploiting state-of-the art technologies in the telecommunication and information technology areas. The platform will be used for applications in different sectors, i.e. health care, and remote control, in order to demonstrate the benefits for end users in public health, business and residential environments.
- *SEQUIN* is defining and implementing an end-to-end approach to Quality of Service that will operate across multiple management domains and will exploit a combination of IP and ATM technology. SEQUIN will ensure that researchers across Europe have access to networking facilities that can be tailored to the requirements of individual groups and which will offer predictable and stable quality across multiple underlying management domains and networking technologies. The resulting VPN will be based on the GÉANT network.

The followin g diagram attempts to show where all these projects concentrate their efforts:

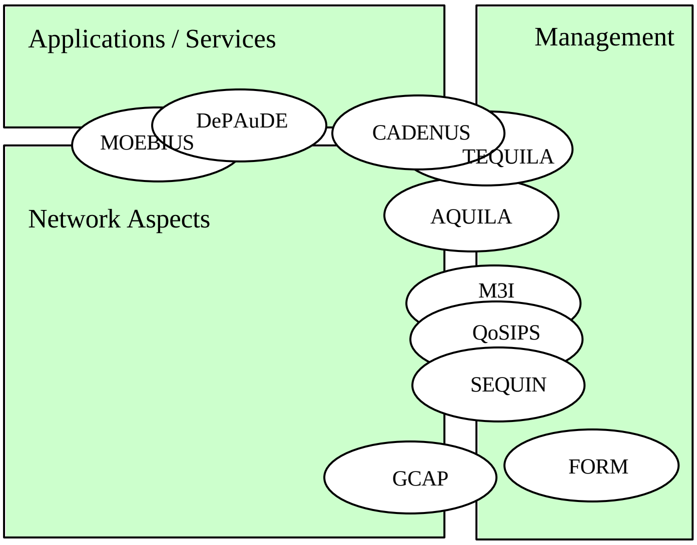


Figure 3-1: *Positioning of IST project concerning applications/services, management and network aspects.*

IST Project	Project Number	Keywords
AQUILA	IST-1999-10077	Network architecture, QoS, DiffServ, Resource Control Layer
CADENUS	IST-1999-11017	Premium IP service architecture, QoS, SLA/SLS
DePAuDE	IST-2000-25434	Embedded automation systems, new architecture for dependable dedicated (intra-site) and IP (inter-site) mechanisms
FORM	IST-1999-10357	Enterprise management and QoS
GCAP	IST-1999-10504	Network architecture, Multicast protocols, IPv6, QoS, Active networks
INTERMON	IST-2001-34123	scalable inter-domain QoS, monitoring, modelling, simulation, visual data mining, distributed QoS database, policy-control
M3I	IST-1999-11429	Resource management, charging, QoS
MOEBIUS	IST-1999-11591	Mobile IP platform, Healthcare application, trials
QoSIPS	IST-1999-20033	Quality of Service and pricing differentiation of IP services
SEQUIN	IST-1999-20841	IP QoS through a combination of IP and ATM technologies, GÉANT
TEQUILA	IST-1999-11253	QoS, traffic engineering

Table 2: *Keywords of QoS related IST projects.*

3.2 Project Differences and their Complementary Approaches

This subsection gives an overview of the technical research areas of the projects. The projects are "compared" by means of tables, which allow the reader to easily assess complementary approaches and the (main) differences between the projects. More technical information about each project can be found in the technical annexes and the reference list.

3.2.1 Project Service and Resource Management Comparison

Within Table 3 the Service Management approaches of AQUILA, CADENUS and TEQUILA are compared, while Table 4 offers an overview about Resource Management investigations. Some of the facts are not applicable to all three projects.

Service Management	**AQUILA**	**CADENUS**	**TEQUILA**
Business Layer aspects: SLAs, Business processes, billing, etc	Not the main focus of AQUILA. SLAs are seen as the subscription of the network services. No charging/billing but accounting of usage data.	CADENUS maps its architecture to the TMF business processes. The automation of SLA production, and the translation to SLSs is a strong focus of CADENUS	TEQUILA investigates operational service management (service subscription and invocation). The business management layer is not a TEQUILA research area.
Different stakeholder roles (access, service, wholesaler)	No	CADENUS considers the overall environment (access, service, wholesale), including residential- and business end systems. A fundamental aspect of the CADENUS architecture is the separation of Service Providers from Network (resource) Providers. “Access Mediators” and user profiling are also included	TEQUILA makes abstraction by considering ‘customer-provider” relationships. The provider is a network provider and the customer may be a company, a residential user, an application provider, another provider, or any other legal entity subscribing for a (network) service.
IP Service concept	The End-user Application Toolkit (EAT) offers the AQUILA's network services towards the end-users and applications via different GUIs and the EAT API, and allows reservation requests on them.	Full end-user IP services and user-provider interfaces are considered	IP connectivity services characterised by a set of SLSs (QoS-related traffic aspects) . TEQUILA considers as well long-term IP services such as leased lines and VPNs as short-term “multimedia” services. Combinations of both are possible such as using a VPN for voice services amongst the company employees.
Service creation process (definition of end-user services by providers)	AQUILA provides a set of predefined network services and allows their modification as well as the creation of new ones by using the QoS Management Tool (QMTool).	Yes, including a Service Directory for listing services, and the capability to have a Service Authority, where services can be classified (similar to a hotel star-rating system)	TEQUILA investigates resource-related aspects of policy-based service definitions. Services can be created to explicit service subscription (by e.g. a web-based interface) or direct service invocation by a well-defined UNI interface and protocol (e.g. RSVP).
AAA & user-profiles	The EAT allows the identification of end-users towards the RCL and subscriber database. Moreover it holds information on end-user's reservation history.	Security concerns between all the players in the CADENUS architecture are addressed.	TEQUILA makes distinction between “customers”, subscribing for the service and “users”, invoking the service. There is a 1:N-relationship in the sense that e.g.; several employees make use of the (same) company VPN

Service Management	**AQUILA**	**CADENUS**	**TEQUILA**
Interworking service & resource management service driven traffic engineering resource-based admission control	Yes	Yes, the Service Mediator – Resource Mediator interface. service driven resource management, through policies admission control at subscription and invocation time	Essential research area of TEQUILA service driven resource management & TE Resource Provisioning Cycle admission control at subscription and invocation level
Service Assurance (monitoring and measurement)	Yes, see chapter 5.1 and 5.2	Monitoring and measurement will be performed at all of the interfaces between the Mediators. Collaboration with INTERMON for joint experimentation is being investigated	An area of increasing importance in QoS research and therefore also in TEQUILA. A QoS measurement architecture goes beyond the diagnostic role of current monitoring functions in best-effort networks. TEQUILA investigates a monitoring architecture for: assisting traffic engineering in allocating resources efficiently and dimensioning the network for any short or long term changes in-service verification of the traffic and (QoS) performance characteristics by monitoring customer-specific SLSs.

Table 3: *Main Service Management research areas.*

Resource Management	**AQUILA**	**CADENUS**	**TEQUILA**
QoS capabilities of the routers	IP DiffServ light	IP DiffServ (use of IPv6 flow label, and load-balancing) and MPLS	IP DiffServ, MPLS and QoS-based routing (OSPF intra- & BGP-inter-domain) and IntServ (considering the RSVP usage)
QoS Architecture	Resource Control Layer, (see Figure 2-1) a distributed architecture for bandwidth control and Admission Control Layer	The CADENUS architecture (see Figure 2-5)	TEQUILA functional Architecture (see Figure 2-7)
Long-term, centralised TE-approach	Resource Control Agent MPLS-based (calculation of explicit paths)	A resource repository (database) is accessible from the Resource Mediator	Network Dimensioning (ND) calculates the long-term network configurations MPLS-based (calculation of explicit paths)

Resource Management	**AQUILA**	**CADENUS**	**TEQUILA**
			IP-based (calculation of TE OSPF routes)
Short-term, distributed TE, handling of traffic fluctuations	Hierarchical structure with resource pools at the network edges	Use of load balancing is expected to provide benefits in this area	Dynamic route & resource management, i.e. the edge and core routers operate within boundary conditions set by ND
Service and Resource interworking. Admission Control (AC)	separated from resource management per-flow based executed by Admission Control Agent	The Service Mediator and Resource Mediator interoperate via a well-defined interface. Admission control is used at the time of registration and invocation, as appropriate for the service	Main TEQUILA concept of the *resource provisioning cycle.* Admission control characteristics Part of the service mgmt system (separated from resource mgmt) Two-level based AC for service subscription and service invocation
Inter-domain TE	BGRP elaboration BGRP software design BGRP implementation, see also [AQ-BGRP]		QoS-enhanced BGP, see Internet drafts [TE-05-BGP]
Policy-based TE		A “policy-based” scheme using concatenated SLAs is under consideration	High level policies can drive the way ND and DRtM/DRsM algorithms work [TE-07].

Table 4: *Main Resource Management research areas.*

3.2.2 QoS Approaches

All three projects focus on Quality of Service, but their level concerning this issue is somewhat different. The same is true for the time scale. Figure 3-2 tries to place the three projects in relation to each other. Together they address a wide area of the QoS field. The three arrows indicate how common topics like SLA/SLS, BGRP/BGP and measurements are touched. As it is always difficult to integrate all information into one figure, it has to be mentioned that for example the BGP – BGRP activities apply to AQUILA & TEQUILA only.

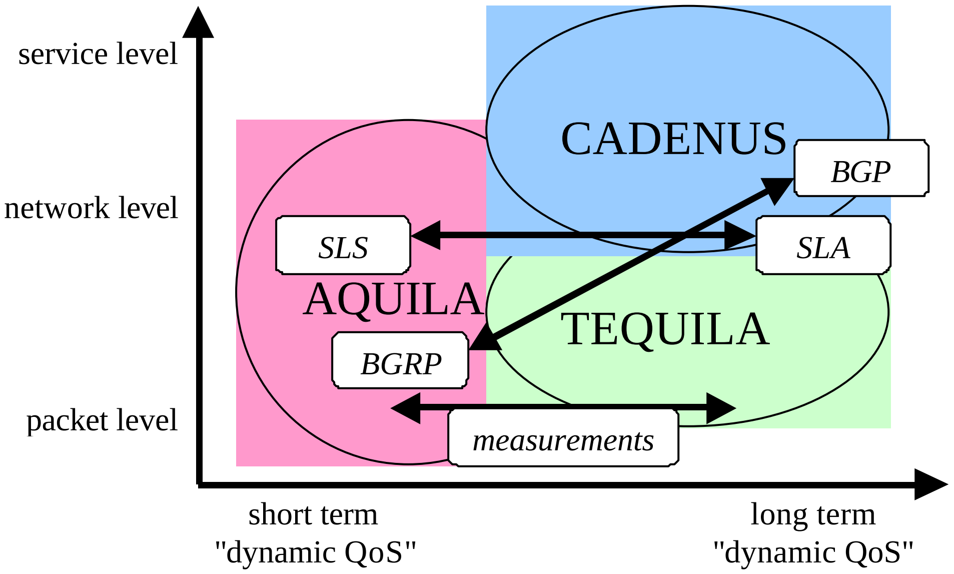


Figure 3-2: *QoS focus of the AQUILA, TEQUILA and CADENUS projects.*

3.3 Interoperation of the Projects

Being at the higher level of the service provisioning architecture, it would be interesting to map the service creation, presentation and registration features of CADENUS onto the lower level resource management schemes from AQUILA and TEQUILA. However, the timing of the three projects was not sufficiently well co-ordinated, nor were resources available within the projects for this opportunity to be exploited.

CADENUS has nevertheless shown that it is possible to invoke services through the CADENUS SM onto commercial devices (acting as RMs and NCs), using the SLS interface as the boundary. There would be, however, further scope for communicating the data received during the registration/subscription phase to the resource management processes for the longer-term network planning scheme within TEQUILA.

CADENUS has a proposal for determining how the QoS values in SLSs should be distributed across RMs for the inter-domain case. This is work that is being shared with MESCAL.

4 PROJECT RESULTS

4.1 Comparison between Measurement Facilities in AQUILA, TEQUILA and CADENUS

Measurement functions are used in the three projects to test QoS/SLA specifications of the developed network/service architecture in the projects. The measurement functions for the different European projects are designed to study the specific features of the QoS/SLA concepts developed in the architectures:

- Adaptive Resource Control for QoS Using an IP-based Layered Architecture - AQUILA
- End-User Services in Premium IP Networks - CADENUS
- Traffic Engineering for Quality of Service in the Internet, at Large Scale - TEQUILA

Dependent on the specifics of the QoS architecture (AQUILA, TEQUILA and CADENUS), there are differences in the

- kind of measurement traffic data, QoS parameter and metrics for resource utilisation
- used measurement and monitoring techniques and approaches.

The measurement facilities of the different projects are designed to solve complex measurement and analysis tasks concerning QoS and traffic. Thus, they are similar in approaches such as:

- Usage of databases and common measurement data repositories
- Focus on metrics which are standardised or are on the way for standardisation
- Focus on common measurement methodologies, technologies and techniques
- Interaction of different measurement tools
- Advanced graphical user interfaces to use measurement facilities

Measurement and monitoring procedures are used in the three projects to analyse QoS and SLA mechanisms of the developed architectures. Although the measurement facilities have some common features, there are differences concerning measurement tool selection and interaction.

- AQUILA measurement architecture integrates active and passive QoS measurement tools interacting based on common measurement database. The focus are end-to-end and paths QoS performance measurements and their inference to resource usage for QoS/SLA analysis and validation.

- TEQUILA collects traffic measurement data for SLA analysis using policy based traffic monitoring facilities.
- CADENUS collects measurements on technical SLI for QoS and SLA validation of IP Premium services (CADENUS put some effort on mapping between the SLS and the different kinds of SLIs (user SLI-and technical SLI).

Measurement facilities are discussed in the following chapters in a more detailed fashion in order to emphasise on specific and general measurement tool design techniques.

4.1.1 Comparison between Monitoring and Measurement Architectures in AQUILA and TEQUILA

The AQUILA and TEQUILA projects rely on similar monitoring and measurement facilities. The two approaches are detailed evaluated in tabular form. This allows the reader easily to assess both common things and the main differences between the two. More detailed technical information about each architecture can be found in the technical deliverables and published papers given in [AQ-DMA], [AQ-MU], [TE-MMA] and [TE-PAS].

The tables of comparison of the AQUILA and TEQUILA measurement approaches address the following subtopics:

- general principles (see Annex A, Table 7),
- design and implementation (see Annex A, Table 8),
- measurement data & methods (see Annex A, Table 9),
- metrics (see Annex A, Table 10),
- features (see Annex A, Table 11),
- assessments (see Annex A, Table 12).

4.1.2 Monitoring in CADENUS: Service Level Indication

The CADENUS project assumes that Premium IP services will include the feature of being able to choose between different levels of QoS that best meet a user’s application and pricing constraints. The service and its delivery quality will be negotiated through a contract, named a Service Level Agreement (SLA), between the user and a service provider. Such a service provider is expected to be an entity capable of assembling service contents and server side resources (e.g. the CADENUS Service Mediator).

The QoS issues are twofold:

- the auditing of the actual satisfying of the current SLA with the service provider
- the dynamic re-negotiation of the service agreements.

As far as the first aspect is concerned, we can reasonably forecast that as soon as communication services with QoS or other service-related guarantees (e.g. service availability) are available - and as soon as users start to pay for them - it will be required to verify whether or not the conditions specified in the SLA are being met by the provider.

With reference to the second aspect, the re-negotiation of QoS has been always accepted as an important service in performance-guaranteed communications. Nevertheless, implementations are rare since the judgement is qualitative; generally linked to user-expectations related to changes in the perceptive satisfaction for the delivered service. However, re-negotiation can also be related to different issues, strongly connected to critical problems such as the efficiency of network resource allocation, the end-to-end application level performance, and the reduction of communication costs. For example we might consider a scenario where the QoS received by a distributed, client-server application is influenced by several factors: the network performance, the server load and the client computational capability. Since these factors can be varying in time, it is logical to allow applications to modify Service Level Agreements on the basis of the QoS effectively achievable and perceivable at the application layer.

We therefore believe that the possibility to modify the existing QoS based agreements between a service provider and the final user will assume an important role in future Premium IP networks. Furthermore, applications can impose additional requirements to Premium IP networks because of this possible dynamic re-negotiation of SLAs.

Currently, applications wanting to monitor the received QoS must be capable of collecting performance data, e.g. by on-line measurements of the communication performance achieved during the data exchange. This can be done by inserting software probes in the application code, or by using feedback information made available by specific protocols such as RTP (RealTime Protocol). This approach, however, is quite problematic, since i) it requires specific development of code dedicated to such on-line measurement; and ii) it is capable of only a high-level identification of possible end-to-end performance problems, with no detailed information on their original causes.

The fundamental idea behind the CADENUS proposal for monitoring is based on the definition of an information document, that we have defined as a *Service Level Indication* (SLI). The SLI is produced with the co-operation of all of the CADENUS Mediation Components in order to obtain a detailed picture of the level of service that is currently being offered.

Inside CADENUS, service provisioning is the result of an agreement between the user and the Service Mediator (SM), and it is regulated by a contract. The SLA is the document resulting from the negotiation process and establishes the kind of service and its delivery quality. The service definition stated in the SLA is understood by both the user and the SM, and it represents the service expectation which the user can refer to. Such an SLA is not intended to give a technical functional description of the service deployment. Therefore, a more technical document is needed: the Service Level Specification (SLS). This is derived from the SLA and provides a set of technical parameters with the corresponding semantics, so that the service may be appropriately modelled and processed, possibly in an automated fashion. The SLS can also be used by different providers, in order to co-operate in the fulfilment of the service: this issue, which is mainly related to the inter-domain scenario, requires that a thorough definition of the protocols and mechanisms involved in the exchanging of information between each pair of peering entities along the service delivery chain is provided.

In order to evaluate the service conformance to specifications reported in SLA and SLS documents, we introduce a new kind of document, the *Service Level Indication* (SLI).

By mirroring the hierarchical structure of the CADENUS architecture, it is possible to distinguish between three kinds of SLIs (Figure 4-1):

- *Template SLI*, which is contained inside the Service Directory and provides a general template for the creation of the documents containing the monitoring data associated with a specified service. This is in line with the definition of the SLA template as the very first step in the service creation process [5];

- *Technical SLI*, which contains detailed information about the resource utilisation and/or a technical report based on the SLS requirements. This document thus pertains to the same level of abstraction as the SLS. The Resource Mediator (RM) is in charge of preparing such a document on demand so as to allow the SM to check whether an SLS is actually fulfilled;

- *User SLI*, i.e. the final document forwarded to the user and containing, in a friendly fashion, information about the service conformance to the negotiated SLA. The User SLI is built under the responsibility of the SM on the basis of the SLS, the Template SLI and the Technical SLI.

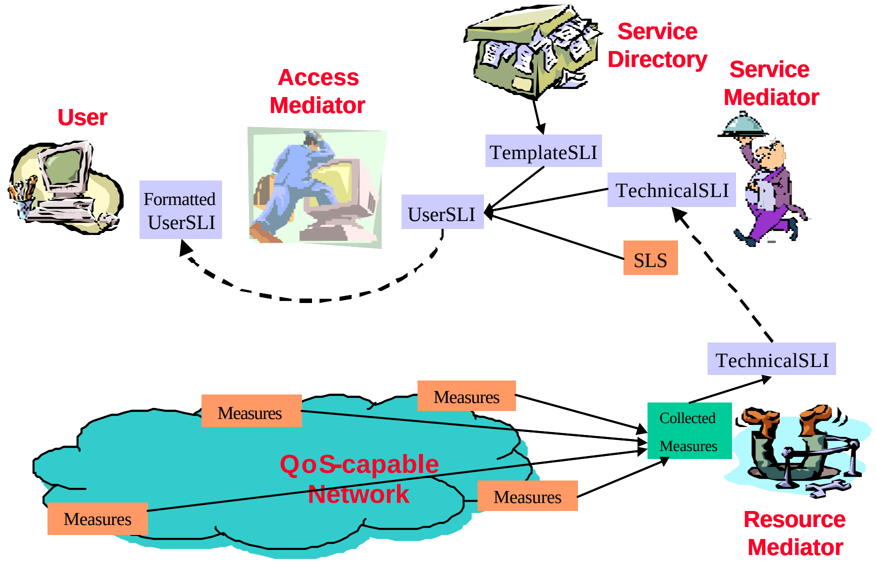


Figure *4-1: The CADENUS Monitoring Architecture: information passing.*

At the request of the SM, the RM builds the Technical SLI document on the basis of data collected by the measuring devices. The fields it contains are directly derived from those belonging to the SLS and are filled with the actual values reached by the running service. The resulting document is sent to the SM.

By means of the Technical SLI received by the RM, the SM is able to evaluate the received service quality conformance with respect to the requests formulated through the related SLS. It can be interested in such information both for its own business, and in order to gather data for the compilation of a complete report in the case that a user requests one.

At the user's request, the SM, exploiting data contained in a Technical SLI, produces a further report indicating the QoS level as perceived by the end user. The document it prepares is derived from a template published in the Service Directory at service creation time (the so-called SLI Template), which provides an abstraction for the measurement results in the same way as the SLA Template does with respect to the service parameters. Such a document, hereby called the User SLI, is delivered to the Access Mediator.

The Access Mediator receives the User SLI from the SM, puts it in a format that is compliant with both the user's preferences and the user's terminal capabilities and forwards it to the end-user.

SLA monitoring can be considered as a "metaservice", i.e. a "service about a service", that may be bought by users, bounded to a Premium IP service instance. Therefore, clarifying how the negotiation of such a metaservice can be included in the existing business framework is necessary.

An SM can add to the service offer the monitoring option. If this is the case, two different strategies are possible. In one scenario, the SM evaluates the resource usage for monitoring service as a fixed cost. Such a cost will be taken into account when the quotation is prepared. This strategy does not modify the business process related to the specific service since the user's request to monitor its own SLA implies uniquely a fixed add-on to the service quotation. Such an add-on depends upon the business strategies of both the SM and the RM.

In the second case, the SM shows two different quotations to the user: the first one related to the service instance selected by the user, the second one regarding the monitoring activity. This solution introduces a scenario in which the negotiation of the SLA monitoring metaservice is considered, and interactions between the Access Mediator and the SM can be formalised through the same business process as that describing the CADENUS services, such as VoD, VPN, and VoIP. Such a business process includes the following business transactions:

- checking the service availability,
- submitting a quotation request,
- accepting a service quotation,
- issuing the purchase order.

The definition of business processes can benefit from the availability of a standard proposal coming from the electronic business research community, named ebXML.

Details of the roles of the CADENUS components in the creation of models to export the measurement data can be found in Deliverable D2.2: "Resource Usage Monitoring in SLA Networks".

4.2 Service Level Agreements

A definition of the term "Service Level Agreement" can be found in [RFC2475]:

> "*…a service contract between a customer and a service provider that specifies the forwarding service a customer should receive. A customer may be a user organisation (source domain) or another DS domain (upstream domain)*".

Apart from this somewhat general statement, no specific work exists inside the IETF related to the definition of SLAs for particular classes of service. More precisely, most of the efforts have focused on the Diffserv framework (see next subsection), thus taking into account the definition of Per Hop Behaviours (PHBs), more than end-to-end service specifications.

The TeleManagement Forum has defined SLAs as*:*

> *"... a formal negotiated agreement between two parties, sometimes called a Service Level Guarantee. It is a contract (or part of one) that exists between the Service Provider and the Customer, designed to create a common understanding about services, priorities, responsibilities, etc. (TMF 701 modified). An SLA or Contract is a set of appropriate procedures and targets formally or informally agreed between Network Operators/Service Providers (NOs/SP's) or between NOs/SP's and Customers, in order to achieve and maintain specified Quality of Service (QoS) in accordance with ITU (ITU-T and ITU-R) Recommendations. The SLA may be an integral part of the Contract. These procedures and targets are related to specific circuit/service availability, error performance, Ready for Service Date (RFSD), Mean Time Between Failures (MTBF), Mean Time to Restore Service (MTRS), Mean Time To Repair (MTTR) (ITU-T Rec. M.1340)".*

CADENUS is of the opinion that a clear understanding of what an SLA looks like is a must for Next Generation Networks. In their view, an SLA is a contract between the customer and the provider of a specified service. Such a contract is signed upon subscription to the service itself and is prepared from templates specifically conceived for the available services. SLA templates are used during customer negotiation to define the required level of service quality.

As a general remark, an SLA should give the user the possibility to negotiate a certain type of service, among those offered by the network. A generic user might ignore the details of the service he is willing to demand from the network (especially those concerning the traffic characterization), either because such information is not available at all, or because he lacks the necessary technical skills required to understand their semantics. To ease the process of filling the contract template, a number of different SLA models might prove useful: the contract would become easier to understand, being focused on the actual needs expressed by the user. These SLAs may be considered as formed by two different parts, one containing information that does not depend on the particular application (e.g. user authentication module, information about availability/reliability of the service, encryption services, etc.) and the other containing application-specific data.

Given the general definitions above, CADENUS has made some work on the Service Level Agreements needed to support the correct operation of Premium IP Networks, including the introduction of the terms *retail* SLA and *wholesale* SLA. With the term *retail* SLA they refer to the agreement between an end-user and a service provider. The end-user might be either a single person or a users' organization. Such an end-user could be induced to establish an SLA with his provider in order to support different kinds of applications. SLAs trigger the negotiation of hierarchical agreements between different contractors. In the case of multi-domain scenarios, service providers may need to create inter-network agreements in order to support their end-user SLAs. *Wholesale* SLAs are inter-provider contracts. A *wholesale* SLA takes into account traffic aggregates flowing from one domain to another. In general, there is no direct connection between r-SLAs and w-SLAs. In particular, w-SLAs might not be based on parameters related to a single service but rather focus on statistical indicators related to the grade of service of the entire bundle provided by one provider to one of its neighbours.

4.3 Service Level Specifications

The three projects have worked together on the topic of Service Level Specifications, i.e. the technical part of the Service Level Agreement. The joint collaboration has been focused on common activities towards the IETF. Also the definition of the SLS (two years ago, by the initial SLS TEQUILA draft) has been a basic component for the TEQUILA system as well as the CADENUS system. The following section briefly summarises the definition and use of the SLSs, as been used by the projects.

4.3.1 A Layered Service Model for IP Differentiated Services

One of the basic DiffServ QoS concepts is the PHB, exposing, in a generic way, the QoS capabilities of a router. PHBs may be implemented by a range of scheduling and buffering mechanisms such as Priority Queuing, Weighted Fair Queuing and algorithms for implementing packet dropping policies such as Random Early Detection. The PHB is the basic building block for supporting value-added IP services, previously negotiated between the provider and its customers through SLAs. However, there is a missing link between the low-level data-plane concept of a PHB and a high-level IP transport service such as VoIP. This is illustrated in Figure 4-2.

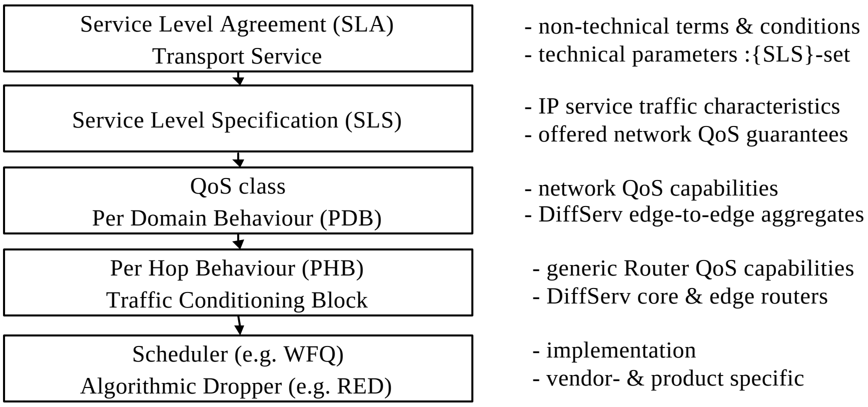

Service Level Agreement (SLA)
Transport Service
- non-technical terms & conditions
- technical parameters :{SLS}-set
Service Level Specification (SLS)
- IP service traffic characteristics
- offered network QoS guarantees
QoS class
Per Domain Behaviour (PDB)
- network QoS capabilities
- DiffServ edge-to-edge aggregates
Per Hop Behaviour (PHB)
Traffic Conditioning Block
- generic Router QoS capabilities
- DiffServ core & edge routers
Scheduler (e.g. WFQ)
Algorithmic Dropper (e.g. RED)
- implementation
- vendor- & product specific

Figure 4-2: *A DiffServ layered service model.*

4.3.2 Service Level Specifications

The upper two layers of Figure 4-2 describe the interface between the IP transport provider and the customer. According to the IETF DiffServ working group, a Service Level Agreement (SLA) is "*the documented result of a negotiation between a customer and a provider of an IP service that specifies the levels of* availability*, serviceability, performance, operation or other attributes of the transport service*". The SLA contains technical and non-technical terms and conditions. The technical specification of the IP connectivity service is given in Service Level Specifications (SLSs). A SLS "*is a set of technical parameters and their values, which together define the IP service, offered to a traffic stream by a DiffServ domain*". SLSs describe the traffic characteristics of IP flows and the QoS guarantees offered by the network to these flows. Note that a SLA may contain a set of SLSs. Our definition of a SLS [TE-02-SLS] is uni-directional, thus requiring two symmetric SLSs to describe services such as a bi-directional Virtual Leased Line (VLL) or a telephone call.

The DiffServ working group does not intend to specify further the content of a SLS beyond the loose definitions given above. Nevertheless, the definition of a SLS is a key-step towards the provisioning of value-added IP services because it specifies the semantics of the interface between the provider and the customer, i.e. *the technical terms and conditions*. To this end, we have proposed a standard template for the parameters and semantics of a SLS [TE-02-SLS]. The basic parameter groups of the SLS template with a brief description are presented in Table 5.

Parameter Group	*Description*
Customer Identifier	Identifies the customer or the user for Authentication, Authorisation and Accounting purposes (AAA)
Flow Descriptor	Identifies *the packet stream* of the contract by e.g. specifying a packet filter (DSCP, IP source address, etc).
Service Scope	Identifies the administrative region *where* the contract is applicable by e.g. specifying ingress and egress interfaces.
Service Schedule	Specifies *when* the contract is applicable by giving e.g. operating hours of the service on a per-day, per-month, etc. basis
Traffic Descriptor	Describes the traffic envelope through e.g. a token bucket algorithm parameters, allowing to identify in- and out-of-profile packets
QoS Parameters	Specifies the QoS network guarantees offered by the network to the customer for in-profile packets including delay, inter-packet delay variation, packet loss and throughput guarantees.
Excess Treatment	Specifies the treatment of the out-of-profile packets at the network ingress edge including dropping, shaping and re-marking.

Table 5: *SLS parameter groups.*

4.3.3 Network QoS Layer

The third layer in Figure 4-2 is the "network QoS layer" mediating between the customer-specific SLS-based services and the elementary PHBs supported by the routers. The notion of the QoS-class is introduced to substantiate this mediation. QoS classes expose the network-wide QoS transport capabilities and they are bound to the specific technology employed and capabilities provided by the network. For example, a Virtual Wire (VW) QoS-class could be defined to denote an edge-to-edge transport capability with a guaranteed maximum packet delay and a guaranteed throughput for an aggregate IP packet stream marked as Expedited Forwarding (EF). QoS-classes should be seen as specifications of a Per Domain Behaviour. We have adopted the following specification of a QoS class.

Parameter	*Description*
Ordered Aggregate	The allowed values are: Expedited Forwarding (EF), Assured Forwarding 1-4 (AF1, AF2, AF3, AF4), Best Effort (BE)
Delay	The *delay* is the maximum *edge-to-edge* delay that the in-profile packets of a certain IP stream should experience. It is a continuous parameter that may be worst case (deterministic) or percentile (probabilistic).
Packet Loss	The *packet loss* is the upper bound of the *edge-to-edge* packet loss probability that in-profile profile packets of an IP stream should have.

Table 6: *Specification of a DiffServ QoS class.*

A finite number of QoS-Classes is obtained by allowing only a discrete number of possible delay and loss values. The delay-loss ranges are mainly driven by the corresponding performance parameters of the services offered (expressed in the SLSs) and they are subject to the capabilities and characteristics of the network including its topology. Furthermore, they may be policy-influenced, changing from time to time as service and network policies warrant so.

A network supports certain QoS dasses through deploying dedicated Traffic Conditioning Block (TCB) at the edge routers, PHBs throughout the network, and an overall resource management system). Supporting customer specific SLSs boils down to a “service mapping” of the SLS to a QoS class and SLS admission control, while the network should be suitably engineered to gracefully sustain the traffic of the admitted SLSs.

4.4 Resource Management

4.4.1 Inter-Domain Issues

Resource reservation schemes are considered extremely critical since scalability depends on their performance particularly when taken into account the rapidly growing size of the Internet. An edge router may be responsible for simultaneously handling hundreds of reservations, but when a core router is considered, the case is completely different. Even if in general a core router has more CPU than an edge router and can possibly handle tens of thousands of simultaneous reservations [AQ-BGRP], it cannot definitely handle hundreds of thousands, and certainly not millions.

In the research community it is well know that the RSVP protocol does not scale well in large networks due to per-flow reservation state management, since its overhead can grow like O(N2), where N is the number of Internet end hosts. The introduction of the IntServ over DiffServ architecture [RFC2998] seems to be a promising solution to provide end-to-end QoS in a scalable way. The basic idea is to use the DiffServ approach in the core network and the RSVP/IntServ in the access network. This architecture allows at least two different possible deployment strategies. The first is based on statically allocated resources in the DiffServ domain while the second is based on dynamically allocated resources in the DiffServ domain, which can be done using RSVP-aware DiffServ routers. However, this approach has most of the RSVP drawbacks, since per-microflow state information is kept in the intermediate routers.

Another step towards end-to-end QoS provision is the Bandwidth Broker (BB) mechanism, which has been introduced from the early stages of the DiffServ model. The QBone bandwidth broker architecture defines a model for the BB and specifies an inter-domain interface between peering BBs. For communication between the BBs, the Simple Inter-domain Bandwidth Broker Signaling (SIBBS) [AQ-BBA] protocol is proposed, forming a single layer of bandwidth brokers, which control the resources within each domain.

QoS signaling capabilities are indeed needed to extend the provisioning of QoS in IP networks from a static model towards a dynamic one. The IETF WG NSIS [AQ-NSIS] has been specifically chartered to address the signaling aspects of QoS in IP networks. The Border Gateway Resource Protocol (BGRP) framework emerges as a scalable answer to this need, which is largely compliant to the requirements for the QoS signaling under definition by NSIS WG. Moreover, it appears to be a more scalable solution with respect to the "RSVP-aware DiffServ region", which is proposed in [2].

4.4.2 BGRP Concepts

The BGRP approach, introduced by P. Pan et al. [1], proposes the aggregation of reservations on the basis of the destination domain. This functionality is closely related to the property of the BGP routing protocol that enables the creation of sink trees while domains trace their route towards a particular domain. Consequently, reservations are aggregated along the sink trees created by the BGP protocol, thus limiting to a great extent the number of active reservations maintained at the routers to a factor of O(N).

Accordingly, the BGRP Plus (BGRPP) protocol, described in [AQ-BGRPP], is introduced as an enhancement of the BGRP protocol. It operates between BGP-capable border routers of each DiffServ domain, namely the BGRPP agents. On providing the desired communication, three messages are mainly used in the BGRPP framework: the PROBE, GRAFT and REFRESH messages. Figure 4-3 depicts a reference network where the BGRPP framework can be applied.

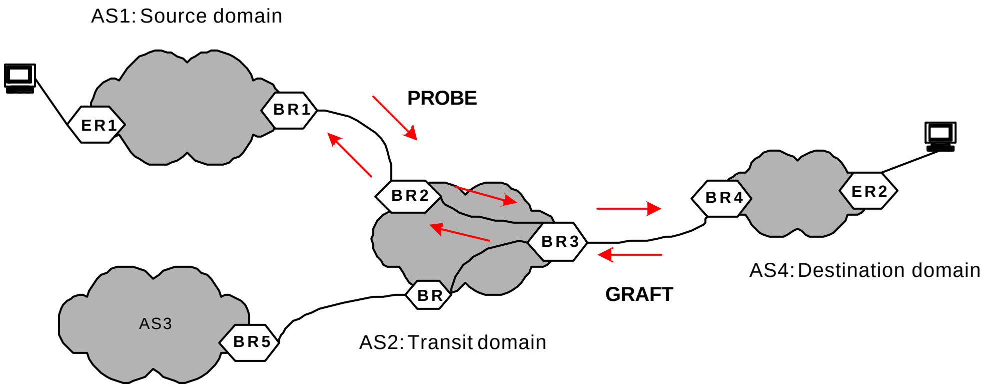


Figure 4-3: *A reference network for the appliance of the BGRPP concepts.*

The BGRP is an inter-domain protocol, which tries to tackle the scalability problems by reducing the amount of state information for each resource reservation as well as the processing of resource reservation messages. However, in order a resource reservation request to be successfully established in the network, signaling messages have to travel the full path from the source to destination increasing the signaling overhead and utilizing a significant amount of bandwidth. Aiming at reducing the signaling overhead, the quiet grafting mechanisms are introduced. The quiet grafting mechanisms should provide an intermediate BGRP agent with the necessary functionality to successfully answer a PROBE message, before the latter arrives at the destination domain.

The Quiet grafting solutions proposed at [AQ-BGRPP] include the network layer reachability information (NLRI) Labeling for early sink tree identification, the resource cushion algorithm for implementing a delayed resource release procedure and an enhancement of the information carried in the GRAFT message for informing the last domain at the end-to-end path for new reservation requests. A detailed analysis and performance evaluation of the quiet grafting mechanisms can be found in [AQ-QG].

Policies may be used to achieve better scaling in network management by describing common attributes of groups of objects, typically associated with the "role" of that object instance in the network. Policies may also be used to express the behaviour of objects - typically expressed as rules. Rule based policies enhance the scalability of network control by:

- facilitating the distribution of common control algorithms, and
- enabling control functions to span multi-vendor networks through common abstracted information models.
- Specific policy sets may be applied to automate network administration tasks including configuration, performance, security, fault and restoration, service provisioning including QoS, and traffic engineering.

4.4.3 Policy-based Resource Management

In CADENUS, once the subset of information contained in the SLS has been received by the Resource Mediator, the Network Controller translates it into a set of policy rules and, acting as a Policy Decision Point (PDP), sends policies to the underlying Policy Enforcement Points (PEP), by exploiting the COPS protocol. Upon the reception of a new policy, the PEP forwards it to the Device Controller, which produces configuration commands for the network device as well as rules enabling it to distinguish the traffic flow to be measured. Then, the Device Controller is able to appropriately configure the traffic control modules (e.g. allocation and configuration of queues, conditioners, markers, filters, etc.) and to perform the measurement activities.

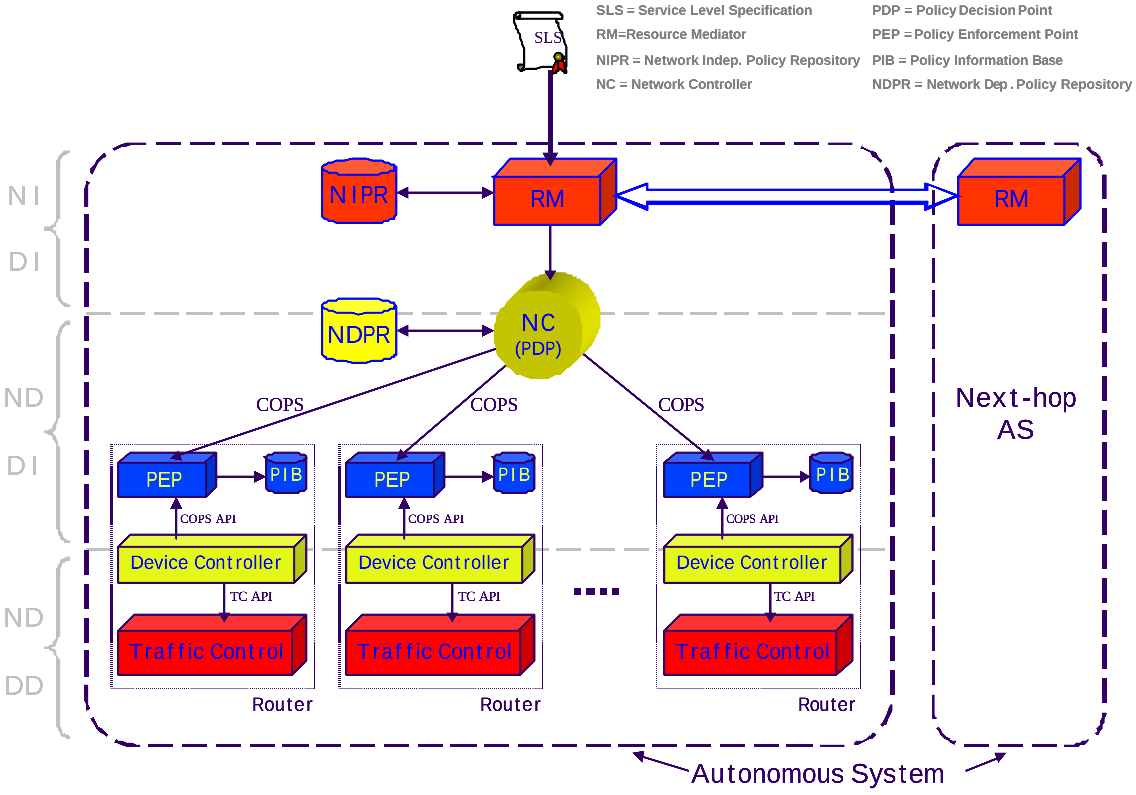

SLS
SLS = Service Level Specification
RM=Resource Mediator
NIPR = Network Indep. Policy Repository
NC = Network Controller
PDP = Policy Decision Point
PEP = Policy Enforcement Point
PIB = Policy Information Base
NDPR = Network Dep. Policy Repository
NI
DI
ND
DI
ND
DD
NIPR
RM
RM
NDPR
NC
(PDP)
COPS
COPS
COPS
PEP
PIB
COPS API
Device Controller
TC API
Traffic Control
Router
....
Next-hop
AS
Autonomous System

Figure *4-4*: *Overview of the CADENUS policy framework components.*

4.5 Security Issues in CADENUS

From the CADENUS security architecture point of view, there are two conceptually different critical communicating paths that need to be protected (see Figure 4-5).

1. Communication links between user and Access Mediator,

2. Communication links that connect Mediators to each other, using SLAs or SLSs.

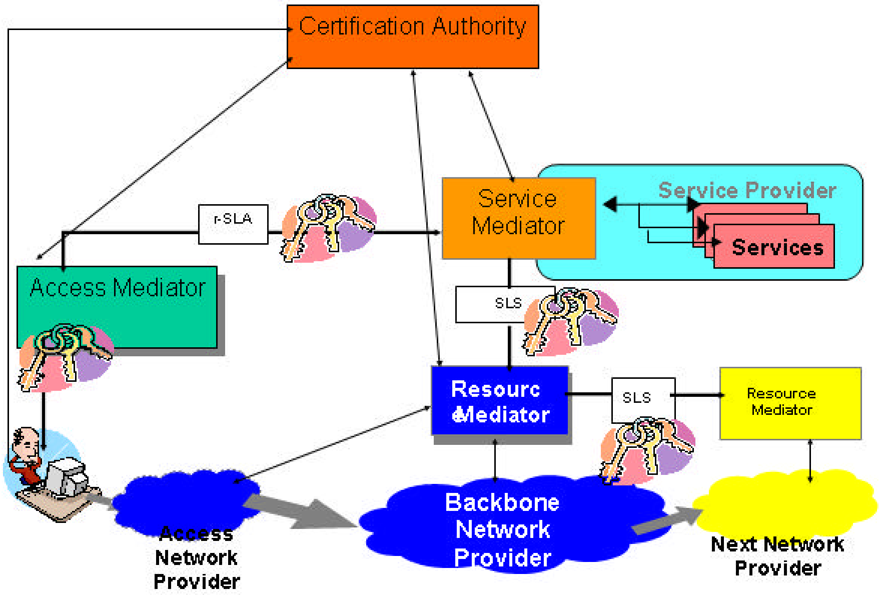


Figure 4-5: *Global security architecture in CADENUS.*

Authentication is the most important security service in the electronic world. It is defined as the corroboration that the source of data received is as claimed, or that a peer entity in an association is the one claimed. Identification and identity verification of a user connected to the AM enables the safe building of a user's profile, controlled access to user's information, tailoring of services to the user's needs and charging for a service. On the other hand, authentication of an AM gives users an assurance that they are really using genuine AM services. Mutual authentication is also a basis for key distribution and establishment of a secure channel that provides for the safe transfer of data between the user and the AM. In this way, the secure session prevents the abuse of the user's privacy and provides confidentiality and integrity of exchanged and stored data.

Secure channel establishing procedures include several cryptography based security mechanisms for data protection, for example symmetric and asymmetric encryption algorithms, and digital signature algorithms. Symmetric algorithms are primarily used for the encryption of exchanged data between a user and a server, and require for their use a common encryption key. To put security on a higher level, and to prevent abuse of keys for encryption/decryption, asymmetric (public-key) algorithms are used for key distribution as well as for authentication. Two distinct keys are used in public-key algorithms, one for encryption and the other for decryption. Anything encrypted with the first key can only be decrypted with the second key. Although both keys are mathematically related, it is computationally infeasible to derive one key from the other without additional (secret) information. One of the keys can thus be published, e.g. on LDAP servers or in the X.500 Directory, allowing everyone to perform encryption or signature validation, while a user only has to know the corresponding private key to decrypt or sign a message. For the establishment of a secure channel, several security protocols are available. As described later, SSL (Secure Sockets Layer) or its enhancement TLS (Transport Layer Security) is the basis for security provision in CADENUS secure user <-> AM access.

Authentication of users can be done in different ways. A user can, for example, demonstrate his identity with something he/she knows (e.g. password), something he/she posses (e.g. token) or with his/her personal characteristics (e.g. fingerprint). Authentication with passwords has several drawbacks and is therefore not appropriate for secure electronic services. A more safe and reliable way is using public-key cryptography based protocols and digital signatures.

4.5.1 Security Mechanisms

Asymmetric cryptography is the basis for authentication and data integrity. Each user possesses a pair of keys (private/public key) and identifies himself/herself with digitally signed data that is produced with his/her own private key. The private key is unique to the user and should therefore not be accessible to other users. With a private key, a user can digitally sign his/her message and the recipient can authenticate the user's identity with the user's public key, which corresponds to the user's private key.

Public keys are stored on public key servers and accessible to everyone. Since a public key is generally just a string of bits, it is essential that one can verify to which particular entity the key belongs. The problem of public key authentication is solved with public key certificates, which are issued by trusted entities, known as Certification Authorities (CAs). For the CADENUS project, a special CA needs to be set-up. A public key certificate is a digitally signed data structure that includes all relevant user's data and his/her public key. The de-facto standard certificate format is defined in the ITU-T Recommendation X.509 v3. X.509v3 certificate, which has been used in the CADENUS service. It contains the following mandatory data:

- Version of certificate format,
- Serial number,
- Subject's (user) distinguished name,
- Distinguished name of the CA, that has issued the certificate,
- User's public key,
- Signature algorithm identifier,
- Validity period,
- Subject public key information.

Optional extensions which provide additional information about the public key and its owner, certificate the issuer, certificate policies and possible constraints on the use of the key and certificate can also be specified. The amount of included data depends upon the system needs and abilities. At the beginning, only *Basic Constraints* and *Certificate Policies* extensions will be populated. After the initial test, other extensions, such as *Alternative Names* or *CRL (Certificate Revocation List) Distribution Point* can be added. This depends upon the overall performance of the CADENUS services.

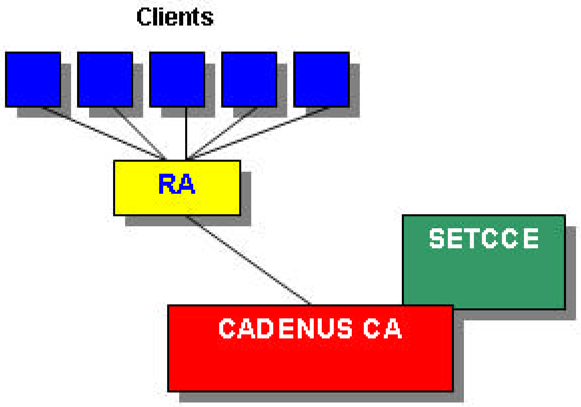


Figure 4-6: *CADENUS PKI*

Figure 4-6 shows the CADENUS Public Key Infrastructure (PKI) needed if public-key-based technologies are used on a wide scale. A PKI is a system of certification authorities with supporting registration authorities and other agents and servers. The CADENUS PKI will consist of a single CADENUS CA that will be established and operated by SETCCE. The core services of the CA will be certificate issuance to end-users and Mediators, directory service provision, certificate distribution, revocation of certificates, and publishing of certificate revocation lists. OCSP (On-line Certificate Status Protocol) service for on-line checking of certificate validity is also envisioned later in the project, if necessary. One of the most important issues in PKI is the certificate applicants registration and identification. Before a user receives his public-key certificate, he/she must be identified and his identity verified. Verification procedures generally depend upon the type of users (individuals, organisations), the intended use of certificates and cryptographic keys, and the level of assurance that a certificate purports to provide. In such services, the physical appearance of a certificate applicant is widely recognised as important. User authentication will therefore be performed in their personal presence on the basis of official documents, such as personal ID cards. User identification and registration will be done by a local registration authority (RA), physically close to the user community. A close distance between the RA and end-users will speed-up the registration and identification process and provide a higher level of security. The detailed identity verification procedure will be further defined in the CADENUS CA certification practice statement.

4.5.2 Operations

As mentioned before, the security component enables authentication and, through the establishment of a secure channel, confidentiality and data integrity. The basic secure protocol is TLS, which provides privacy and data integrity between two communicating applications.

The identification of a user (as well as of the AM) is part of the protocol and is performed in two steps. After connecting to an AM, a client is requested by the AM to authenticate itself. In the next step, the client sends a digitally signed response message together with his certificate. The AM then checks the digital signature and validity of client's public-key certificate. Figure 4-7 schematically shows the procedure of client's authentication.

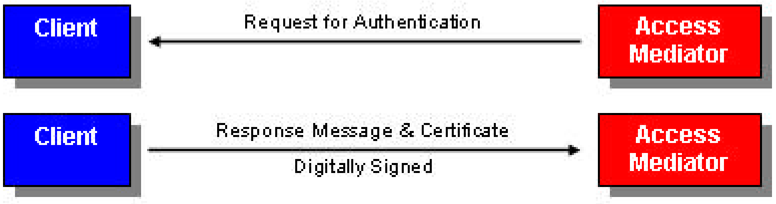


Figure 4-7: *Authentication of CADENUS's client.*

The mutual authentication of a user and a AM is part of the procedure (TLS protocol) for setting up a secure channel. The authentication of users is optional in TLS, but it will be used in CADENUS. Figure 4-8 shows this procedure. The TLS protocol consists of two parts (sub-protocols):

- Record protocol
- Handshake protocol

The record protocol defines the basic format for all data items sent through a secure channel and provides data integrity and confidentiality. This is the foundation for setting up a secure channel for transferring public-key certificates with client's and AM's public keys. In the handshake protocol, a client and an AM authenticate each other, negotiate on cryptographic parameters that will be used later for data protection, and establish a common symmetric session key for encryption. Firstly, the client contacts the AM by sending a Hello message. The AM responds with a message that includes also its certificate.

After receiving the AM's certificate, the client checks the validity of its certificate. The validation procedure involves checking a revocation list that includes the numbers of all revoked certificates. A certificate becomes invalid in case of abuse, loss of private key or other reasons. Revocation lists are updated regularly, such as hourly, daily or weekly. OCSP can also be used later in the project to check on-line the current status of the certificate.

In a third step, the client generates a session key. This key is generated for each session, and is encrypted with the AM's public key (received by the client in the second step) before it is send to the AM. This way the session key is securely transferred to the AM.

In the fourth step, the secure connection between the client and the AM can be established using the session key for symmetric encryption.

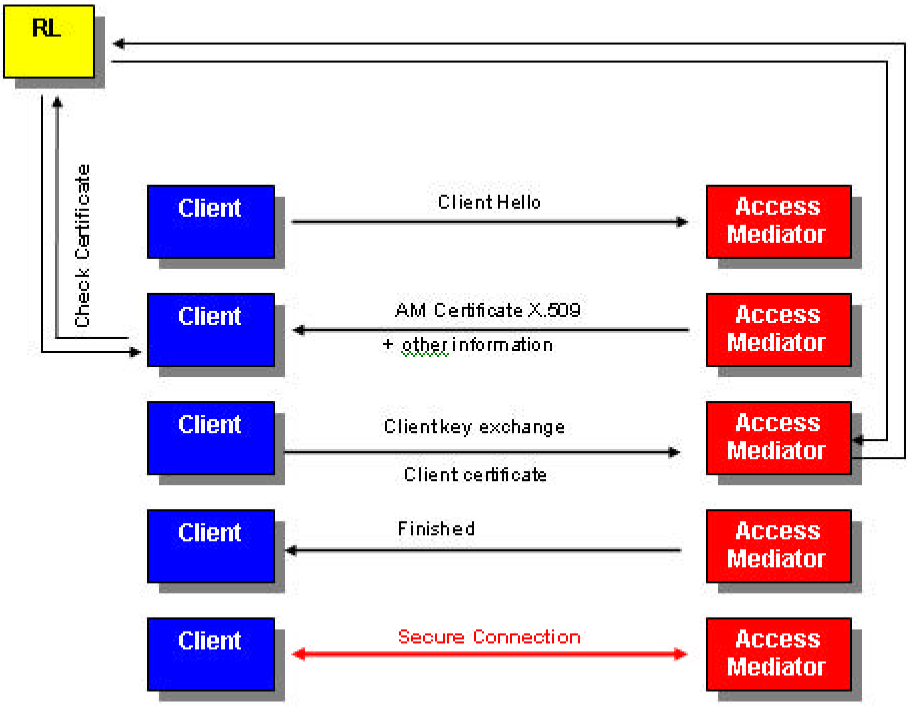


Figure 4-8: *Setting up a secure connection*

4.6 Trials

In general the trials are carried out in order to prove and evaluate the functionality of the proposed architectures and mechanisms. Furthermore, the applicability on the existing networks is investigated and the benefits and constraints that the given framework introduces are identified. Therefore, the planning and the evaluation of the trials are of great importance.

During the design phase of a project several assumptions and simplifications are made. Moreover, the mechanisms that will be implemented introduce additional constraints and points of investigation. Additionally, advanced theoretical work is made in each area in order to provide the formulas that are going to be used (e.g. for admission control). It is consequently crucial to first validate the main functionality of the proposed architecture and then to identify the requirements that the given approach has from the system. Also scalability issues should be taken into account and be further studied. Finally, the project objectives should be fulfilled, which in the case of the three projects AQUILA, CADENUS and TEQUILA is the provisioning of Quality of Service in networks.

More specifically the goals and the objectives of the trials should be to:

- Validate the main functionality of the system components. This task can be achieved by defining basic functional scenarios that will be carried out at the trial sites and by which the concept of the proposed architecture will be proved.

- Certify the assumptions and simplifications that are made during the specification and design phase as well as the proposed formulas. Concerning this issue the input from the network operators is required mainly for two reasons: to confirm the reasoning of those assumptions and to provide the trials with as realistic scenarios as possible. Additionally the results from the trials should be compared with the theoretical results in order to validate the correct implementation of the defined mechanisms and formulas. A common example is the admission control functions.
- Evaluate the QoS offered. As all three projects have as the main objective the provisioning of QoS this is one of the most important issues. There are mainly two possible approaches to evaluate it. Firstly, by giving simple demonstrations of the system to “real” users the QoS offered as this is perceived by the user can be determined. However, in order to obtain a more reliable and accurate feeling of the offered QoS, the actual QoS metrics (i.e. delay, jitter, packet loss, etc) should be measured by using measurement tools. If such tools are not available, the development should be considered at least in the case where the required effort is not high.
- Check the scalability factor of the framework. One of the main considerations in each QoS architecture is the scalability of the proposal. The signalling mechanisms that are usually introduced aggravate the network with additional load. Additionally the currently used equipment (i.e. routers, switches, and workstations) has constraints concerning the performance of the system on high load situations. Therefore the analysis of the problem is of great importance. This can be decomposed in three areas
    - The trials should realise scalability tests mainly concerning the performance of the equipment (e.g. by making multiple reservations or introducing multiple users) since there is not possible to build large-scale network in trial test beds. Additionally, the signalling load can be measured as well as the requirements of the system components (in terms of memory usage and processing power).
    - From the trial results and with the help of simple calculations, an estimation of the scalability of the system could be produced.
    - Furthermore, with the use of simulation tools, a more detailed picture of the performance of the system, especially concerning large-scale networks, could be obtained.

After the realisation of the aforementioned tests and simulations, the benefits and the constraints of the proposed architecture will be revealed. In this way, not only a well functioning prototype is produced but also the field of appliance is identified and the advantages that are arising form its use are determined and justified beyond doubt.

4.6.1 Distributed Trial in AQUILA

Important aspect of trials performed in the AQUILA project is to validate the QoS in the inter-domain scenarios. In order to create a testing environment as close as possible to the real conditions, the testbeds located in Polish Telecom (Warsaw) and in Telecom Austria (Vienna) were inter-connected via the European GÉANT network, especially built for the purpose of the European Research Projects. The Premium IP service available in the GÉANT network supports reliable service with guaranteed QoS. The capacity of the connection established between the testbeds is 2 Mbps. The inter-connection was set-up with active support from the SEQUIN project and from national research networks POL34 and AcoNet.

The multi-domain network scenario (see Figure 4-9) closely resembles the conditions in the real Internet and has been used for testing the inter-domain resource management architecture developed within the AQUILA project. The main focus of the inter-domain trials was to validate the ability to request QoS in multiple domains, as well as to validate the packet-level QoS provided for the user traffic traversing multiple domains.

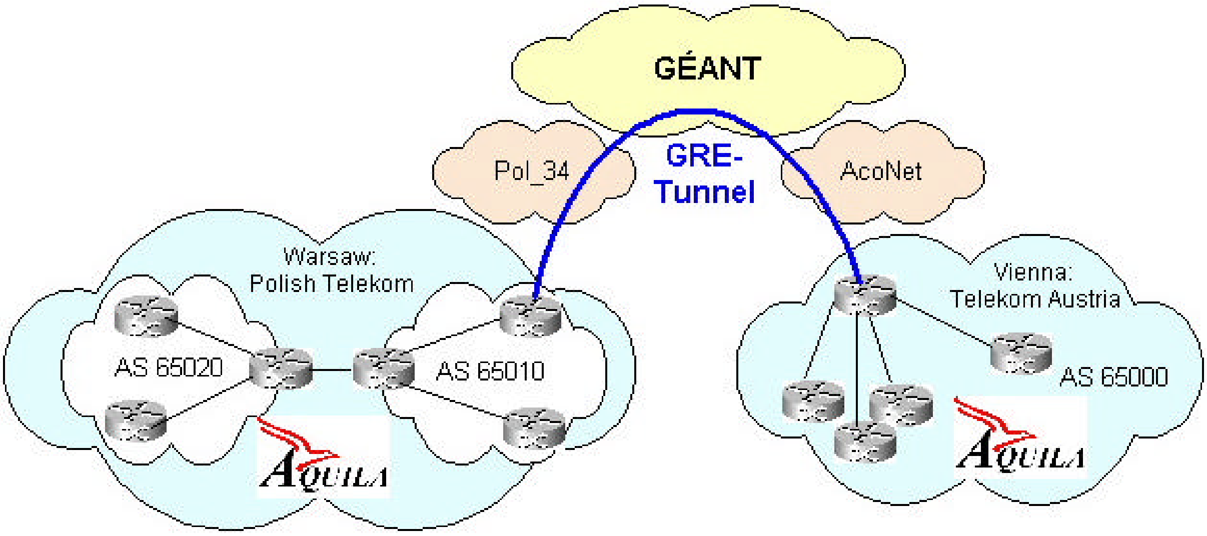


Figure 4-9: *Distributed trial sites in the AQUILA tests.*

4.6.2 Trials and Validation in CADENUS

For proof-of-concept purposes, the developments will focus on solutions for enhanced versions of the existing services and applications VoD, VoIP and VPN. The service configuration is provided in a dynamic way, through the appropriate mediation of user related service components (authorisation, service selection, QoS parameters, etc.) to network related components (resource control, monitoring, accounting, etc.). Two different network technologies have been trialled: MPLS and DiffServ.

The architecture must be generic, and sufficient service examples should be implemented to demonstrate that the architecture meets its requirements. The tests that have been performed are intended collectively to validate that the CADENUS approach:

- is easy to understand and install for users, network providers and service providers,
- blends seamlessly with novel, dynamic SLAs,
- meets the functional requirements for registering with – and invoking – services with different levels of QoS, SLA monitoring, and collecting data for subsequent billing,
- is network independent,
- is service independent.

Two Trials were made following a logical development cycle from a static Service Mediator and Resource Mediator functions for, respectively, a VPN service and an DiffServ network, to a system deploying dynamic service creation and configuration. This roadmap includes the introduction of more flexibility into the Service Mediator and Resource Mediator, the introduction of underlying commercial networks, an Access Mediator, multiple domains, roaming users (portable user profiles, etc.), composite services and much SLA work.

Trial 1 was a laboratory testbed implementation of the CADENUS mediator components being used to handle the introduction and configuration of end-user services selected from Video on Demand (VoD), Voice Over IP (VoIP) and IP-VPN, running on a DiffServ network.

Trial 2 was a laboratory testbed implementation of the CADENUS mediator components being used to handle the introduction and configuration of end-user services selected from VoD, VoIP and VPN, running on a DiffServ network. It incorporated commercial equipment, controlled by CADENUS mediation components.

4.7 Applications for Concept Verification

The AQUILA project assumes that four QoS network services [see chapter 3.1] are supported by the network, each designated for effective handling of specific type of traffic. Each service has been defined for guaranteeing predefined QoS objectives, adequate to the requirements of different types of applications. Traffic generated by applications in a multiservice network can be broadly classified into two groups, streaming and elastic:

- Streaming flows result from audio and video applications and require the network to preserve time integrity – usually an AC (Admission Control) is required
- Elastic flows are usually established for the transfer of digital documents (files, pictures) and for them there is a need to provide some throughput guarantees. In addition, some applications, which work in request-response regime, require fast and reliable transfer of information. For meeting the above requirements, an AC function is also required.

For concept verification in the first and second trial the set of applications for each network service were specified. In the trials the following applications were used:

- For PCBR service: WINSIP or Sigma (voice transfer), sending streaming traffic with constant bit rate and requiring low delay and low packet loss ratio;
- For PVBR service: NetMeting or Sigma (videoconference), sending streaming traffic with variable bit rate and requiring low delay and low packet loss ratio;
- For PMM service: Real Player and Server or Mediazine (data transfer using TCP and UDP protocol), sending TCP/UDP-controlled long-lived traffic requiring minimum throughput guarantees;
- For PMC service: Mediazine or games e.g. Unreal Tournament, Ultima Online (data transfer using TCP), sending TCP-controlled short-live traffic requiring low response time and reliable transfer.

The above set of applications represents all traffic types, which can be observed in a multi-service network and allows us for exhaustive verification of AQUILA network services concept.

4.8 Business Cases and Dissemination

For an appropriate dissemination of QoS project results of AQUILA the network and service market has to be considered as well as the according user requirements and Business analysis for these markets. The evaluation of meaningful Business models is a substantial part to exploit research and development project results within commercial products and services. Business plans for commercially promising cases should be based on market studies, on the evaluation of the project results and on the exploitation plans of the project partners. Such cases include Business-to-Business (B2B) relations and Business-to-Customer (B2C) relations.

Objectives for market research should be:

- State of the art studies of competitive network providers.
- Investigations of the information services in the Internet, which could obtain an increase of value by implementing QoS.
- Market relevant results of end user and Business user surveys.
- A Business model analysis containing the value chain for QoS applications and the description of relevant B2B models for network providers and B2B as well as B2C models for information service provider.

Analysis of market sizes and forecast summaries as well as updated company exploitation plans (as quantitative as obtainable) will allow to estimate a possible success of QoS based products / services for alternative Business models more in detail. A financial analysis should detail the anticipated nature of the costs incurred in the creation and delivery of QoS based applications, and also the expected revenues to be obtained from the use of the services. It will detail the sensitivities of a Business model to variations in certain parameters to reach a break-even point.

It is recommended to evaluate following Business models more in detail:

- Subscription-based Business model
- Pay-per-view and revenue sharing Business model
- Advertising based revenue model.

Dissemination recommendation for the involved market participants will be given after a brief summary of mentioned points.

4.8.1 Potential of the Network and Service Market

The market of information technology is already wide extended and continues to grow. The exploitation plans (in WP 3) showed that in the markets of western and eastern Europe a growing Internet infrastructure as well as Internet service and features providing. In eastern Europe customers adapt new services very fast. The growth of customer demanding broadband services will grow rapidly if QoS is more important for providers to attract their customers. In the Western European market Internet with its infrastructure and services is quite established and several service providers are competing. Offering services is not enough to attract customers. Western Europeans want good services in a good quality for low price. It is therefore more important for the network and service provider to offer a good QoS infrastructure. It has to be balanced if an over-provisioning fulfils the requirements or if QoS mechanism will be available to reach the aim more convenient and even cheaper.

The development of the broadband market is determined by the growth of Internet use and the consumers' wish for online services as well as technological offered possibilities. Two types of broadband providers will dominate the market: the cable service providers and the integrated telecommunication companies with DSL technologies. However - for all Internet Service Providers (ISPs) counts the further development for services in order to survive. They have to shape up in different directions and diversifying into new areas of the networked economy: application infrastructure provision, integrated communications services, e-commerce, new media and broadband. But two factors still slow down the universal acceptance of broadband Internet access: first the higher entry prices compared to the free dial-up Internet access and second the technical upgrades necessary to popularise the two access technologies, i.e. cable modem and DSL technologies. If the competition is growing, the prices will decrease and motivate a large group of people to opt this form of fast Internet access. QoS plays a big role in broadband environment characterised by higher bandwidth and "always on" feature that delivers basic technology services like audio/ video streaming, video-on-demand (VOD), Internet telephony, video conferencing etc. Three groups of participants have different major interests and needs in this context: consumers (information, entertainment, education, low costs and high quality), network operators (attractive network providing to increase penetration with attractive content, high quality and additional services), content providers (market their own content, gain high reaches, recycle content with multi-channel strategies). Providers can be divided in offering access AND content with direct Costumer Relationship (AOL, T-Online, Video Networks) and service provider only providing content with direct Customer Relationship (LikeTV, real Goldpass).

CADENUS also believes that as the number and range of services accessible via the public network infrastructure increases, the average bandwidth requirement of customers will dramatically increase from conventional narrowband to broadband levels. For many key service types good QoS will be imperative to attracting customers to using network-based solutions. Accordingly the widespread availability of broadband communications («broadband access for all») will be essential to deliver services at the quality required to maintain the attractiveness of the services offered to customers. The development of sustainable markets in high bandwidth services thus appears essential to the business case for investing in the replacement of conventional networks.

4.8.2 User Requirements

Due to the fact that at the moment users are not satisfied with the quality of stream-based services QoS is the important feature for Internet services, like multimedia content providing. With a higher quality of connectivity the market could grow in the more bandwidth consuming these services and QoS would also increase the market introduction to their customer acceptance. As seen in the user survey, a lot of participants are prepared to pay for future QoS enabled applications. Customer would necessarily subscribe to services, which are useful for their needs either via a subscription fee or via a pay per view model. The most claimed services are Internet telephony, video/audio streaming applications as well as mobile services. As mentioned these services and applications are currently not very well distributed. The main reason is that no QoS is guaranteed. Business customers expect revenue increase, if effective QoS tools are available in the near future. Without QoS a loss of customers is to be expected and as a consequence thereof the costs of the service provision would increase.

4.8.3 Dissemination Plan for the Market Participants

QoS is relevant for making companies competitive for the future and for increasing the usage of broadband services. If companies want to reach higher customer relationship with their new services, they have to provide a good quality for a low price.

There are three groups of market participants who have to disseminate following activities for QoS. AQUILA defines, creates, evaluates and implements an enhanced architecture for Quality of Services for IP networks and enables business models in business (B2B) and customer markets (B2C). Each dissemination of these Services needs different activities to achieve the wanted establishment.

- **Internet Service Providers (ISPs):** ISPs provide QoS equipped services either directly to end users (B2C) or business users (B2C). Business user can buy complete QoS apparelled Services or the revenues can be reached by advertisement clients. Dissemination for QoS based services for the end users can be done by building up a co-operation with an advertisement company and by providing a free test environment during a special timeframe. For Business users PR effects are also reached by implementing web services in the portal with integrated QoS functions, monitoring tools for IP platforms. For Service Providers quantitative issues are involved in selecting classes of services for fixing QoS requirements. Thus need to build a middleware solution for supporting their services. Together with network operators a common platform for SLAs management and QoS provisioning can be designed for the ISPs. This platform will rely on the providers’ workflow process in order to help the dynamic building of IP products and services, which meet then diverse customer needs.

Network Operators: At the moment Network Operators are not in the position to offer a satisfactory solution in the field of multimedia streaming. QoS enables better solutions for broadband services and possibilities to combine them and fulfils so the expectations of consumers regarding high-speed Internet and multimedia content, as they permit the real-time use of data-intensive multimedia services such as e.g. video-on-demand, interactive TV and gaming. Internet offers the mechanism for telecommunications, information-technology, media, entertainment and security sectors to come together and to form a converged value-chain to provide new/novel products and solutions. The greater the regional broadband access, the greater the relevance of the new value-chain steps. For dissemination the network operators should build up Business relationships with ISPs and operators as well as building up several prototypes for investigations in this directions. So the demand for IP multimedia services on the base of a QoS serving network can be analysed and the knowledge about these services can also be increased. Establishment of QoS revenues can be then reached by provision of QoS within their networks from Internet Service Providers for provision of QoS capable networks. The QoS technology providers are responsible for developing, setting up and running the QoS services in the networks. Other dissemination activity are in the product development by prototypes and enhancements in filed trials, customer test environment and future product releases. With established partnerships and co-operations every partner/company will gain a lot of new experiences in the area of IP QoS and receive an optimisation of products and services that can be offered to customers.

As the level of social and economic activity conducted on the network increases, the importance of access to the network will increase. Thus demand for mobility and portability in communications will increase. Accordingly the business case for investing in the complete overhaul of conventional networks suggests that Bandwidth on Demand (BoD) at broadband levels will be essential to the successful realisation of the market conditions which will justify the massive investments in NGN technologies proposed. In order to quickly develop sustainable markets in high bandwidth services it is similarly essential to the business case for investing in NGN technologies that the provision of broadband BoD be offered to customers at a reasonable cost from the outset.

The cost of providing network services will be reduced for all public network providers if access to unused capacity can be made available to rival networks for delivering service to customers.

Similarly if public customer access to unused private network capacity can be facilitated, then the cost to the industry of realising broadband BoD can be reduced.

This implies that roaming between all available networks such that maximum service access can be provided to customers at the lowest cost to the industry in general, will be important to meeting the traffic targets on which the Telcos business case relies.

- **Universities:** Dissemination can be pursued by exploiting results of the AQUILA project via scientific communities like participation in conferences and workshops, as well as publishing results in scientific journals. Furthermore pilot-projects driven by students together with market participants, like ISPs or Network Operators or technology provider can be initiated. Another possibility lies in the establishment of QoS in lectures and courses on software engineering methods and technologies. In this way students may get an impression of the complexity and the real problems of industrial projects. Also participation at international projects and conferences improves the public relations.

AQUILA is an activity that is an essential precursor to widespread deployment and use of such QoS networks. With the architecture of AQUILA a tailored approach where aggregated service elements are used in the core of a network, where scalability is a major design objective and users per flow service elements at the edge of the network, where accuracy of the service response is a sustainable outcome. Such qualities are not only important for network operators – also for an increasing knowledge base of universities as well as the quality of content and service providing together with the whole customer relationship management.

4.8.4 Market in unused Bandwidth

Markets are proven to be the most efficient means of dynamically rationing scarce resources. Accordingly in order that BoD can be efficiently and cost effectively implemented it is suggested that a dynamic market in unused network resources will have to develop in which the price of network capacity is determined by demand and availability, irrespective of the source of this demand.

In this context, QoS will assume great importance in the setting of the terms and conditions of network resource provision. Intuitively QoS will be one of the primary price discriminators for network providers as it has been in the markets for all manner of conventional goods down through the ages. For some services relatively high QoS guarantees will be an essential ingredient to their attraction to customers. For other services lower QoS standards may be acceptable. In all service cases different customer segments will have differing QoS requirements. It is suggested therefore that the ability to offer varying end-to-end service guarantees will be important to the rapid development of sustainable markets in a wide range of services. Thus network providers will seek to offer a portfolio of products, differentiated according to QoS guarantees that maximises the return from their network investments. The ability to reliably offer differing end-to-end QoS guarantees is therefore essential to the business case for re-engineering conventional networks.

4.8.5 Interoperability is essential

Just as in non-electronic based markets for services, customers will require interoperability and compatibility between the network and service offerings of the different network and service providers. As the importance of the network increases, the importance of interoperability between the various devices used to access fixed and mobile networks will also increase, so as to permit effective portability and mobility.

4.8.6 Market Efficiency

Achieving a high level of interoperability and intercompatibility will be important in optimising market reach and consequently maximising the level of network traffic growth realised, on which the business case for NGNs is dependent.

For ASPs and network operators alike, it will be important that they can maximise the sales potential of their services. Accordingly, they will seek to sell directly to the end-user and indirectly through brokers, discount resellers etc. The efficiency of the market in facilitating flexible sales mechanisms will be important to the success of the e-marketplace envisioned.

In the context of markets in dynamic network resource provision, portability of network and service access, and the delivery of services with QoS guarantees, market mechanisms facilitating reliable transaction between the various actors involved are essential. To this end the market enabling mechanism used must effect end to end management of services and ensure transparent compliance with the business and technology agreements negotiated with all parties in the service delivery chain.

The evaluation performed within CADENUS suggests that, assuming that the CADENUS solution is provided with the required functionality, it has huge potential as a key enabler for the successful evolution of e-commerce and IBC.

5 RELATED ACTIVITIES

5.1 Activities towards IETF

5.1.1 Service Level Specification (SLS)

The TEQUILA project initiated an IETF draft on Service Level Specification (SLS) template definition and Service Level Specification negotiation protocol requirements.

During an AQUILA project meeting extension in Salzburg, Austria, on October 12, 2000, joint activities were discussed and planned in order to gauge interest for the creation of work effort within the IETF on SLS, for a BoF session at the next IETF meeting in San Diego (December 10 - 15, 2000), and for the establishment of an IETF Work Group on these topics.

The Salzburg meeting was one of the first joint meetings of the Premium IP projects AQUILA, CADENUS and TEQUILA.

The BoF session took place at the 49th IETF meeting in San Diego on December 13, 2000, 15:30 - 17:30. Agenda, minutes, presentations and an e-mail list for SLS interest can be found at the Service Level Specification Interest Web Page [TE-SLS] or via the AQUILA home page [AQ-HOME].

Discussions were ongoing - privately organised - during the 51st IETF meeting, London, UK, August 5-10, 2001. Minutes are available.

For the charter and drafts see [SL-01] .. [SL-07].

5.1.2 Inter-domain Resource Control

During recent months the AQUILA workpackage 1.2 carefully watched the ongoing activities in the IETF regarding QoS signalling. Initial plans to launch a working group in this area started in April 2001. After the 52nd IETF meeting in November 2001 in Salt Lake City, the NSIS (Next Steps In Signalling) working group was established [AQ-NSIS].

From the charter: "This working group will develop the requirements, architecture and protocols for the next IETF steps on signalling QoS."

According to the charter of the NSIS WG, the topic of inter-domain signalling mostly correlates to the work of the AQUILA project. Workpackage 1.2 therefore prepared two Internet drafts addressed to this WG:

- **draft-aquila-bgrp-arch**
  This draft outlines the architecture of the AQUILA inter-domain signalling based on BGRP. It describes the basic architectural issues as well as the special implementation choices, protocol message content and message processing.

- **draft-aquila-bgrp**
  This draft presents the mechanisms used for inter-domain resource management and simulation results, which prove the scalability of this approach.

Both drafts will appear very soon at the IETF.

The workpackage members also actively contribute to the discussion on the NSIS mailing list to promote the AQUILA project's point of view and the submitted drafts.

5.1.3 Application Profiles

5.1.3.1 Application oriented Approach

With the concept of application profiles AQUILA proves that it is possible to supply legacy non-QoS aware applications with QoS. The solution is based on the assumption that we have a QoS enabled network offering network services and non-QoS aware Internet applications running on a host.

The working scheme is as follows: applications run stand-alone at the host in parallel to a so-called QoS web portal and protocol gateways.

The task of the web portal is to enable the identification of the running application (via manual selection by the end-user), to present the QoS offer in appropriateness with the running application (using the application profiles), and to request for QoS on behalf of the application toward the network.

The task of the protocol gateways is to identify control plane information of the running application in order to know which flows are to be supported with QoS.

The task of the application profiles is to describe information about application's QoS profile (what requirement does an application have), and so constitute a repository of concrete application profiles.

5.1.3.2 Application Profile Description

The description of the application takes place by means of the so-called ApplicationProfile.dtd and Servic eComponententProfile.dtd. This is a syntax for describing application and QoS at:

- network level
  - how to describe the AQUILA QoS request - implementation dependent
  - how to describe the QoS expectations / requirements - generic
  - how to describe the produced traffic - generic
- at application - control plane level
  - protocol used, port used...
- at application - data plane level
  - implementation issues of the different service components (e.g. audio, video) - different configuration options
- at end-user level
  - how to build metaphors - presentation of the possible QoS

5.1.3.3 Contribution to IETF

In our opinion we have the four following possibilities for a possible contribution to the IETF standardisation activities

- To propose the description syntax for standardisation. The current version is not completely implementation independent. It has a generic part and an AQUILA dependent one. It still has to be proven that the generic description syntax works with other QoS implementations than AQUILA. Moreover the IETF activities show that the working groups are dealing with much more concrete problems and are not so advanced to discuss cross-implementation issues.
- To propose the application profile repository for standardisation: but makes it sense to standardise application analysis? This information is subject to frequent changes and may be updated and extended by external parties. Therefore AQUILA is preparing a web-based public repository for this information.
- To propose the general approach for standardisation: this could be a possibility to contribute to standardisation activities. However the current status of the IETF activities shows that there is no working group dealing with such a problem. The working groups are dealing with much more concrete problems.

Preparatory work for future IETF activities and make the IETF aware of the AQUILA work: this seems to be the most adequate solution. The concrete steps are: to present the work done at a web page, to make the application profile repository public and to inform the IETF members e.g. mail to the relevant working groups mailing lists announcing the AQUILA web-resources.

5.2 Cluster Monitoring & Measurements (MoMe)

Monitoring and measurement has many facets. For example, all the players (users, service providers and network providers) need to be able to check that their SLAs are met, which requires that monitoring schemes are implemented. Network providers also need to be able to plan for network upgrading, which also requires that they measure and monitor the usage of their resources. The collection of the necessary data is a required task, but should not adversely affect the real traffic (neither during the monitoring process, nor during the transport of the data to the place where it will be processed). If requests for service are accepted/rejected on the basis of models of the underlying networks, then it is beneficial to be able to confirm the accuracy of these models from time to time, using the real network status.

5.2.1 MoMe Cluster Status

Within the MoMe cluster the following partners of the NGNI cluster are currently active:

- IST AQUILA (Salzburg Research, Telekom Austria, T-Systems Nova)
- IST CADENUS (University Naples, Fraunhofergesellschaft)
- IST INTERMON (Salzburg Research, NEC, Fraunhofergesellschaft)
- in discussion: NGNI-project (Waterford Institute)

5.2.2 Objectives of the MoMe Cluster

The objective of the MoMe cluster is to support the existing IST projects by know-how exchange:

1. Pre-competitive components of the IST projects with similar objectives and implementation concepts are candidates for knowledge transfer between the IST projects.
2. Joining the knowledge of the European projects will result in a better European position in the global competition.
3. All IP QoS related IST projects are implementation oriented (field trials). The modelling of the Internet is an open research topic but is needed for the implementation of QoS management algorithms. The cluster will give the possibility to get closer to the scientific (control theory) background of the projects and to improve the European contribution (e.g. IST INTERMON). On the other hand the field trials of the existing projects will generate interesting new measurement results - an unbeatable potential for further research, which will be used for contributions in the 6th framework.
4. MoMe should find out the “best practices” of the different IST project approaches in measuring and modelling:
   - Which tools were useful (accuracy of the measurement tools, load generators)?
   - Which methods were useful (active/passive probing, overhead)?

5.2.3 Planned Activities and Expected Results

The following planned activities rely on results of the current NGN projects:

1. Integration of AQUILA DMA into CADENUS trials
2. Integration of AQUILA DMA into INTERMON
3. Exchange of the trial measurement reports (October 2002)

First international workshop on Inter-domain Performance and Simulation (IPS 2003) February 2003, organised by MoMe Cluster and INTERMON in collaboration with industrial partners (Siemens Austria and Deutsche Telekom).

5.3 IST project INTERMON

In 2000/2001 the AQUILA consortium initiated discussions about missing monitoring/measurement components in the Premium IP Cluster. Especially the aspects of Inter-Domain QoS monitoring, modelling and visual data mining were identified to be candidates for necessary additional R&D activities in a new IST project. With the idea to develop advanced inter-domain QoS analysis architecture with integrated monitoring, modelling and visualisation components the INTERMON IST project has been started in April 2002. The INTERMON project (http://www.ist-intermon.org/) is a partner in the MoMe Cluster. In order to enhance the inter-domain Quality of Service (QoS) analysis in large-scale, multi-domain Internet infrastructures, the goal of INTERMON project is to develop and demonstrate a scalable inter-domain QoS architecture with integrated monitoring, modelling, simulation, and visual data mining components using common distributed QoS database with policy-controlled inter-working of components and automated processing of different kind of inter-domain QoS information (inter-domain QoS, traffic, resource, events).

5.3.1 Integrated QoS Monitoring, Modelling and Visual Data Mining

The INTERMON architecture [IM-IIS] is aimed at integrated QoS (Quality of Service) monitoring, analysis and modelling of application traffic in inter-domain environment using database and visual data mining facilities. INTERMON features address the automated measurement and modelling of QoS and border router traffic for different time scales as well as visual data mining relating statistics and models describing end-to-end and inter-domain QoS as well as border router traffic. Concepts like ”spatial composition” of inter-domain QoS and “policy-based” performance measurement and traffic collection at border routers are considered. The key points of INTERMON architecture are focussed on:

- Integration of tools for automated Internet structure analysis, monitoring, modelling and visual data mining using common database for the purpose of QoS monitoring and verification in an inter-domain environment
- Database design and data mining to support requirements for spatial composition of inter-domain QoS and automated producing of monitoring, modelling and analysis reports considering different aggregation intervals
- Open architecture concept with flexible import/export interfaces for measurement and modelling data (QoS, traffic).
- Tools for distributed measurement, modelling and visual data mining using relational database are integrated in the INTERMON toolkit. INTERMON architecture is intended to be used by ISP provider, operator and application user in an inter-domain environment especially based on QoS technologies (DiffServ, MPLS) for:
- inter-domain traffic engineering and network planning based on visual data mining of border router traffic flows obtained by IPFIX interface
- QoS/SLA monitoring and verification of applications in inter-domain environment based on the concept of spatial composition of inter-domain to end-to-end QoS.

The functional components of the INTERMON toolkit are integrated based on common database relating topological, measurement and modelling information for different kind of parameters (end-to-end QoS, inter-domain performance metrics, traffic) and Graphical User Interface (GUI).

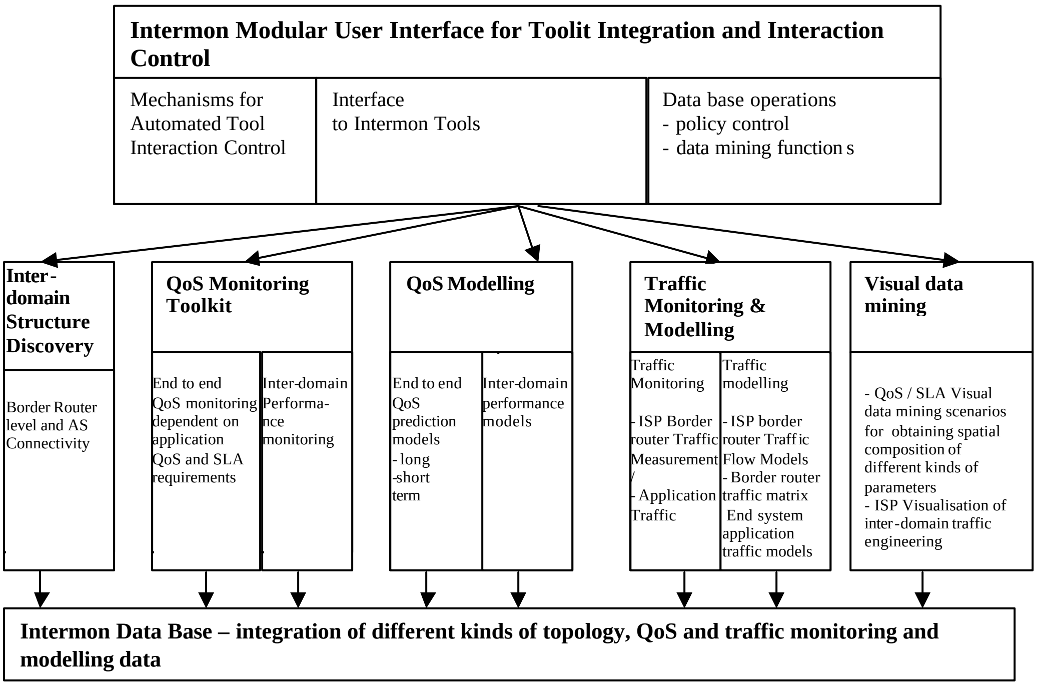

Intermon Modular User Interface for Toolit Integration and Interaction Control
Mechanisms for Automated Tool Interaction Control
Interface to Intermon Tools
Data base operations
- policy control
- data mining function s
Inter-domain Structure Discovery
Border Router level and AS Connectivity
QoS Monitoring Toolkit
End to end QoS monitoring dependent on application QoS and SLA requirements
Inter-domain Performa-nce monitoring
QoS Modelling
End to end QoS prediction models
- long
-short
term
Inter-domain performance models
Traffic Monitoring & Modelling
Traffic Monitoring
- ISP Border router Traffic Measurement /
- Application Traffic
Traffic modelling
- ISP border router Traffic Flow Models
- Border router traffic matrix
End system application traffic models
Visual data mining
- QoS / SLA Visual data mining scenarios for obtaining spatial composition of different kinds of parameters
- ISP Visualisation of inter-domain traffic engineering
Intermon Data Base – integration of different kinds of topology, QoS and traffic monitoring and modelling data

Figure 21: *INTERMON toolkit – integration of functional components.*

The INTERMON users may request the execution of functions for inter-domain structure analysis, monitoring, modelling and visual data mining through the GUI menus and parameters. The user interface includes management mechanisms for "policy based" data collection, interaction control, and specification of configuration and interaction parameters. The INTERMON database defines relationships between different kinds of entities which are stored and processed with the integrated tools.

The integrated measurement and modelling concept is based on relating of the modelling entities (derived per end-to-end QoS parameter, inter-domain performance metric and border router traffic flow) to the corresponding measurement statistics and result entities (describing aggregated statistics results) of the specific measurement scenario for a given time aggregate. The modelling entities, such as accumulative distribution, autocorrelation function, and Auto Regressive Integrated Moving Average (ARIMA) prediction models, are linked to the measurement results and statistics for a given measurement aggregation interval. INTERMON data mining functions are specified in order to obtain automated generation of modelling reports for a different kind of aggregation intervals (e.g. short term: inter-domain routing, long-term: network planning).

5.3.2 Inter-domain Policy based Data Collection

The inter-domain policy based data collection in INTERMON is open for interoperation with other QoS architectures and flexible to integrate different kind of measurements and statistics into the relational database.

INTERMON open architecture design is intended to support import/ export measurement and modelling interfaces between different INTERMON users and towards other QoS monitoring and modelling systems.

The INTERMON monitoring tools use remote meters and adapters for execution of measurement/monitoring scenarios specified with the monitoring tools. The remote meters are configured by the monitoring tools to filter their results and to parameterize adapters for the specified measurement scenarios in order to interact with the INTERMON database. The adapter concept allows to reuse the great amount of QoS monitoring data obtained by other QoS monitoring architectures developed in European projects and international activities.

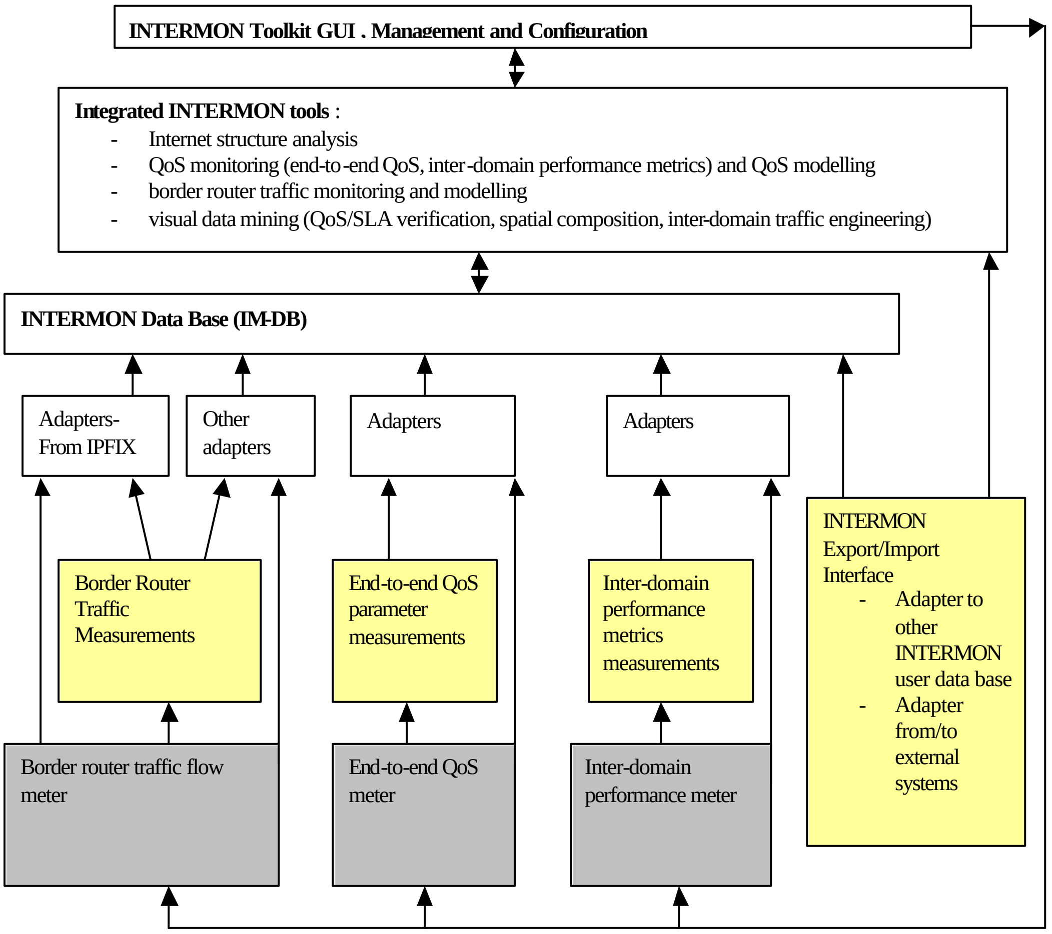

INTERMON Toolkit GUI . Management and Configuration
Integrated INTERMON tools :
- Internet structure analysis
- QoS monitoring (end-to-end QoS, inter-domain performance metrics) and QoS modelling
- border router traffic monitoring and modelling
- visual data mining (QoS/SLA verification, spatial composition, inter-domain traffic engineering)
INTERMON Data Base (IM-DB)
Adapters- From IPFIX
Other adapters
Adapters
Adapters
Border Router Traffic Measurements
End-to-end QoS parameter measurements
Inter-domain performance metrics measurements
INTERMON Export/Import Interface
- Adapter to other INTERMON user data base
- Adapter from/to external systems
Border router traffic flow meter
End-to-end QoS meter
Inter-domain performance meter

Figure 22: *Open and flexible architecture design with adapters for filtering of source measurement data and export/import interfaces.*

5.4 IST project MESCAL

MESCAL aims to propose and validate scalable, incremental solutions that enable the flexible deployment and delivery of inter-domain Quality of Service (QoS) across the Internet. This involves developing: templates, protocols and algorithms for establishing Service Level Specifications (SLS) between Internet Service Providers (ISP) and their customers, including their peers; scalable solutions for inter-domain Traffic Engineering (TE) based on enhancements to the existing Border Gateway Protocol (BGP) routing protocol and associated route selection logic. MESCAL will consider both unicast- and multicast-based services and ensure that the proposed solutions are applicable to both IPv4 and IPv6.

MESCAL started in November 2002 and will run until April 2005.

5.4.1 Project Rationale

In today’s Internet, there are numerous relationships between a multitude of stakeholders who are each responsible for part of the provision of end-to-end connectivity and value-added services. Service and content providers rely on connectivity services provided by what could be termed a loose federation of organisations, which together provide end-to-end connectivity across the global Internet. No single organisation is responsible for *vertical* integration, in terms of applications over service providers over network connectivity, or *horizontal* integration, in terms of global geographical coverage.

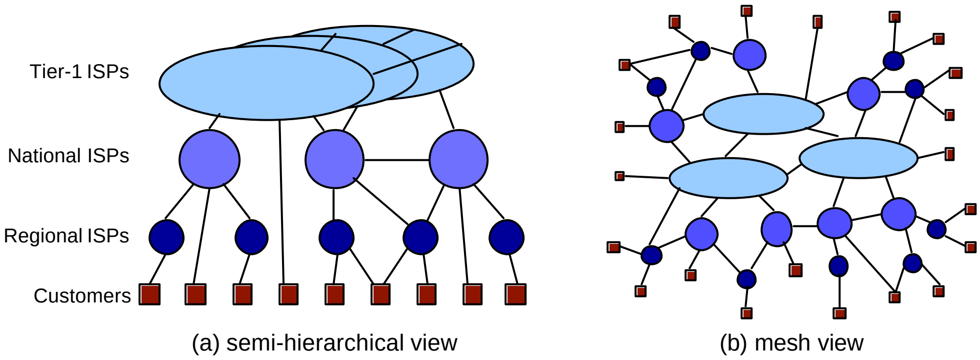


Figure 5-1: *Many autonomous systems are involved in end-to-end service provision.*

A major limitation of the Internet is its lack of service level guarantees due to its basic design for best-effort packet delivery. The introduction of the IP Differentiated Services framework and subsequent research and standardisation efforts, represent significant progress on solving the problem of QoS delivery in a single domain for unicast traffic. However, *inter*-domain communication and information access is the rule rather than the exception, and extensive deployment of QoS-based services will not take place unless they can be offered across domains. The provision of end-to-end QoS is a wide-open research issue whose solution will transform the Internet to the global multi-service network of the future.

MESCAL views two major aspects as essential to the deployment and delivery of inter-domain QoS-based IP services: the definition of QoS-based connectivity services to be provided by stakeholders; and second, the means to engineer network resources to meet agreed performance and capacity targets for the contracted services. Together, these two dimensions aim at providing the means for a dynamically configurable Internet, with service requirements driving traffic engineering to meet end-to-end service demands.

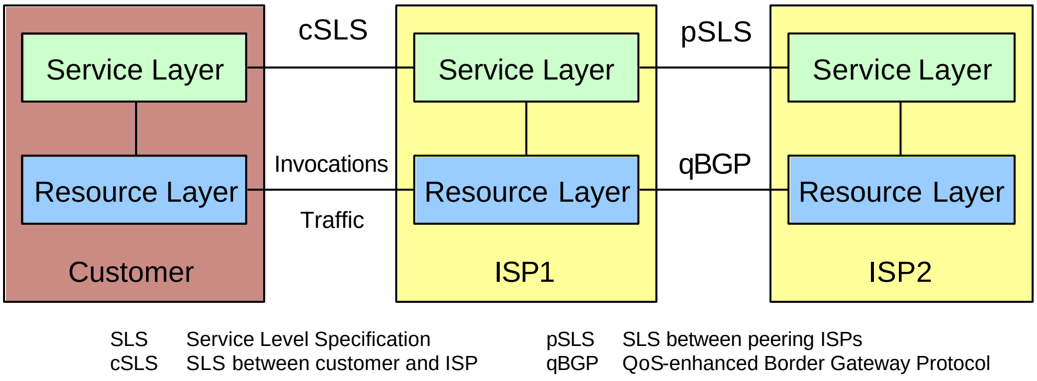
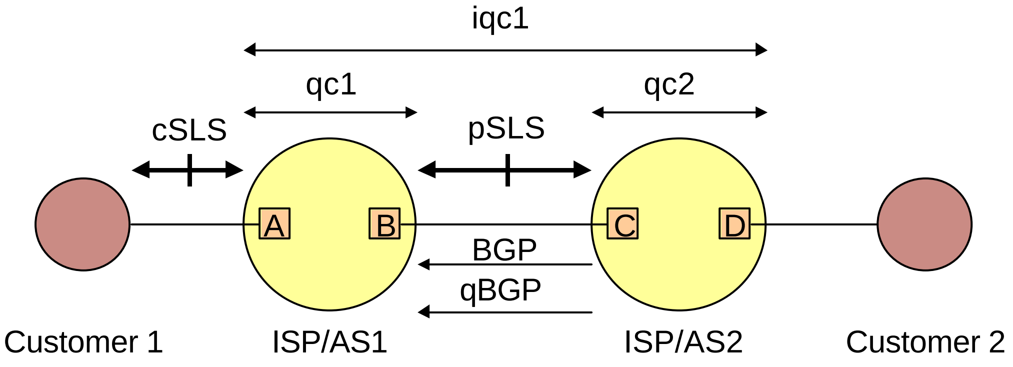

Service Layer
Resource Layer
Customer
cSLS
Invocations
Traffic
Service Layer
Resource Layer
ISP1
pSLS
qBGP
Service Layer
Resource Layer
ISP2
SLS Service Level Specification
cSLS SLS between customer and ISP
pSLS SLS between peering ISPs
qBGP QoS-enhanced Border Gateway Protocol

Figure 5-2: *Inter-domain interactions at service and resource layers.*

5.4.2 Project Objectives

- MESCAL's key objective is: to propose and validate scalable, incremental solutions, enabling flexible deployment and delivery of inter-domain QoS across the Internet at large, with the following sub-objectives:
- To develop business models, based on current commercial practice and emerging business scenarios, describing the roles of and relationships between the stakeholders involved in providing QoS-based services across domains.
- To specify a generic, multi-domain, multi-service functional architecture for the flexible deployment and delivery of inter-domain QoS-based services.

- To develop templates, protocols and algorithms for the specification, negotiation, subscription and invocation of QoS-based IP services between customers and ISPs and between peer ISPs.
- To enhance existing inter-domain routing protocols and algorithms and to investigate new approaches to convey QoS information to enable scalable inter-domain traffic engineering solutions.
- To examine the impact of:
    - IPv6 on inter-domain traffic engineering and to ensure that the TE solutions proposed by the project are applicable to both IPv4 and IPv6 infrastructures.
    - both unicast- and multicast-based services on inter-domain TE.
    - inter-domain aspects of SLS management and TE on corresponding intra-domain aspects, and vice versa, and to investigate the co-operation required between them.
- To adopt a policy-based approach to service provisioning and network operation and investigate policies for SLS negotiation, admission, and inter-domain TE.
- To evaluate and validate the devised algorithms and protocols through simulation and testbed prototypes.
- To contribute to international standardisation efforts, especially the IETF, and to participate in other consensus-forming activities in the IST programme.



SLS	Service Level Specification	qBGP	QoS-enhanced BGP
cSLS	SLS between customer and ISP	qc1/2	Scope of intra-domain QoS class 1/2
pSLS	SLS between peering ISPs	iqc1	Scope of inter-domain QoS class 1
BGP	Border Gateway Protocol		

Figure 5-3: *Building inter-domain QoS classes from intra-domain capabilities.*

5.4.3 Project Organisation

The project is structured around four Work Packages:

- WP0, Project Management and Co-ordination of External Liaison, is concerned with the administrative and technical management of the project, including liaison with other projects and co-ordination of dissemination and standardisation.
- WP1, Specification of Functional Architecture, Algorithms and Protocols, is responsible for defining a business model and a generic, multi-domain, multi-service IP QoS functional architecture for inter-domain QoS delivery. The main output will be the specification of algorithms and protocols for negotiation and establishment of inter-domain SLSs, inter-domain TE and routing, including the required interactions with intra-domain TE and route computation capabilities to achieve inter-domain QoS delivery.

- WP2, System Design and Implementation, will enhance experimental routers and simulators to support the inter-domain QoS requirements of the project. Based on the specifications from WP1, WP2 will design and implement the specified algorithms and protocols, as both testbed prototypes and simulation tools/models. WP2 will deliver prototypes and simulators to WP3 in an incremental way to allow experimentation activities to take place.
- WP3, Integration, Validation and Experimentation, is responsible for setting-up the required experimentation infrastructure and for performing validation and performance evaluation activities on the prototypes and simulators developed by WP2. The testbed experiments are focussed on proof-of-concept validation, while the simulation experiments aim at assessing the performance and scalability of the project's inter-domain solutions.

5.4.4 Comparison with TEQUILA

While TEQUILA focussed on intra-domain SLSs and TE, MESCAL concentrates on inter-domain aspects.

TEQUILA SLS templates and negotiation mechanisms were focussed on the customer-SLS interaction with the topological scope of a single domain. MESCAL will additionally specify ISP-ISP interactions and extensions required to the customer-ISP interactions for an end-to-end topological scope. Negotiation logic and SLS management algorithms including traffic forecast techniques will include the additional complexity arising from multiple peer ISPs.

TEQUILA TE solutions were mainly focussed on engineering a single domain through MPLS and IP-based TE techniques. Work was done on inter-domain TE from the viewpoint of extensions required to the BGP protocol for conveying TE related information between peers. This investigation was limited to the mechanisms for distributing TE information but the associated logic for determining how and when it should be propagated was not studied and the appropriate linkages with the intra-domain TE algorithms and SLS management were for further study. MESCAL will build on the results from TEQUILA and enhance the BGP protocol extensions in the context of a more comprehensive research project. Additionally inter-domain TE algorithms will be developed and the linkages required with a range of intra-domain TE algorithms and approaches (not just those developed by TEQUILA) will be in scope, including intrer-/intra-domain QoS route distribution policies and QoS-based inter-domain routing techniques based on enhanced path-vector EGPs and possibly an investigation of link-state inter-domain routing considering QoS characteristics. While TEQUILA's solutions were applicable to unicast IPv4 traffic, MESCAL will investigate the impact of IPv6 and multicast and explicitly support this traffic in SLS management and TE solutions.

Policy management was investigated in TEQUILA from the perspectives of an overall architecture and approach for policy-driven SLS management and TE to tailor behaviour to operational requirements and also on the use of policy-based protocols and information models for interactions with the underlying routers. Both dimensions will be studied further regarding the applicability of policy driven management on an inter-domain basis and on appropriate PIB specifications for interactions with the network.

While TEQUILA studied monitoring techniques and developed a monitoring system covering node, network and SLS levels this will not be investigated further in MESCAL. A number of other recently awarded IST projects including INTERMON and SCAMPI are studying monitoring as main objectives and MESCAL will liase with them as required.

6 REFERENCES

[AQ-BBA] QBone Bandwidth Broker Architecture, Work in Progress, URL: http://qbone.internet2.edu/bb/bboutline2.html

[AQ-BGRP] P. Pan, E. Hahne, H. Schulzrinne: "BGRP: Sink-Tree-Based Aggregation for Inter-Domain Reservations", Journal of Communications and Networks, Vol. 2, No. 2, June 2000, pp. 157-167

[AQ-BGRPP] Salsano, et. al, “Inter-domain QoS Signaling: the BGRP Plus Architecture”, Internet Draft, May 2002

[AQ-DMA] U. Hofmann, I. Milouchewa, "Distributed Measurement and Monitoring in IP Networks", SCI 2001 (5th World Multi-Conference on Systemics, Cybernetics and Informatics), Orlando, Florida USA, July 22-25, 2001.

[AQ-HOME] AQUILA, Project Home Page, URL: http://www.ist-aquila.org/, AQUILA consortium, April 2002

[AQ-MU] Felix Strohmeier, et al., AQUILA deliverables, “D2301, D2303: Report on the development of measurement utilities in the 1st/2nd trial”, URL: http://www.ist-aquila.org

[AQ-NSIS] Next Steps in Signaling (NSIS WG), URL: http://www.ietf.org/html.charters/nsis-charter.html

[AQ-QG] E. Nikolouzou, et. al, “BGRPP: Performance evaluation of the proposed Quiet Grafting mechanisms”, Internet Draft, July 2002

[CA-HOME] CADENUS, Project Home Page, URL: http://www.cadenus.org/, CADENUS consortium, April 2002

[IM-IIS] D. Hetzer, I. Miloucheva, U. Hofmann, J. Quittek, F. Saluta, “Integrated Information System for Inter-Domain QoS Monitoring, Modelling and Verification”, EURESCOM Conference, Heidelberg Germany, Oct. 2002

[RFC2998] Y. Bernet, et al., "Integrated Services Over Diffserv Networks", RFC 2998, IETF, November 2000

[SL-01] D. Goderis et al, "Service Level Specification Semantics, Parameters and negotiation requirements", draft-tequila-sls-01.txt, June 2001

[SL-02] Proposed Charter for SLSU WG (version 1) -- 23/02/01

[SL-03] S. Salsano et al, "Definition and usage of SLSs in the AQUILA consortium", draft-salsano-aquila-sls-00.txt, November 2000

[SL-04] R. Rajan et al, "Service Level Specification for Inter-domain QoS Negotiation", draft-somefolks-sls-00.txt, November 2000

[SL-05] D. Goderis et al, "Service Level Specification Semantics and Parameters", draft-tequila-sls-00.txt ,November 2000

[SL-06] Y. T'Joens et al, "Service Level Specification and Usage Framework", draft-manyfolks-sls-framework-00.txt, October 2000

[SL-07] D. Goderis et al, "Service Level Specification Semantics, Parameters and negotiation requirements", draft-tequila-diffserv-sls-00.txt, July 2000

[TE-01-ARCH] A Management and Control Architecture for Providing IP Differentiated Services in MPLS-based Networks. P. Trimintzios et all, IEEE Communication Magazine May 2001

[TE-02-SLS] Service Level Specification Semantics and Parameters. <draft-tequila-sls-01.txt> D. Goderis et all (July 2001). Work in progress: http://www.ist-tequila.org/ or at the IETF web: http://search.ietf.org/internet-drafts/draft-tequila-sls-01.txt

[TE-03-TE] Engineering the Multi-Service Internet: MPLS and IP-based Techniques. P. Trimintzios et all, Proc. of IEEE International Conference on Telecommunications (ICT 2001), Romania, Bucharest, June 4-7, 2001.

[TE-04-SM] A Scalable Service-Centric IP QoS Architecture for Next Generation Networks. D. Goderis et al. Paper accepted for NOMS2002 conference (Network Operations and Management Symposium, 15-19 April 2002, Florence). See TEQUILA webpage http://www.ist-tequila.org/

[TE-05-BGP] Providing Quality of Service Indication by the BGP-4 Protocol: the QoS_NLRI attribute (2001) C. Jacquenet et al. Internet Draft: Draft-jacquenet-qos-nlri-02.txt

[TE-06-MM] A Monitoring and Measurement Architecture for Traffic Engineered IP Networks, A. Asgari et al. To appear in proc. of IEEE/IFIP/IEE International Symposium on Telecommunications (IST2001), Tehran, Iran, September 1-3, 2001

[TE-07] Policy-based Extensible Hierarchical Network Management, P. Trimintzios et all, In Proc. of Workshop on Policies for Distributed Systems and Networks (Policy 2001), Spinger-Verlang LNCS-1995, Bristol, UK, January 2001

[TE-HOME] TEQUILA, Project Home Page, http://www.ist-tequila.org/, TEQUILA consortium, April 2002

[TE-MMA] A. Asgari, et al., "A Monitoring and Measurement Architecture for Traffic Engineered IP Networks", Proceedings of IEEE/IFIP/IEE International Symposium on Telecommunications (IST2001), Tehran, Iran, 1-3 September 2001.

[TE-PAS] Pim Van Heuven, et al., Tequila deliverable, "D1.3: Intermediate Results based Protocol and algorithm Specification (Public part)", http://www.ist-tequila.org/

[TE-SLS] TEQUILA: Service Level Specification Interest Web Page (http://www.ist-tequila.org/sls.html)

ANNEX A: MEASUREMENT FACILITIES IN AQUILA AND TEQUILA

Subject	AQUILA	TEQUILA
Scope	• Intra-domain QoS Monitoring Architecture for QoS-enabled IP networks [**AQ-DMA**], [**AQ-MU**]	• Intra-domain QoS Monitoring Architecture for traffic engineered DiffServ networks [**TE-MMA**], [**TE-PAS**]
Goals	AQUILA goal is the implementation of network services, resource reservation, and admission control mechanisms for QoS based applications. The distributed measurement architecture (AQUILA DMA) therefore is used for two main tasks: • To support network operation and resource control performed through the network operator. This is used to enable measurement based admission control (MBAC) and to give the operator a view on the current situation within the network. • To validate the implemented QoS architecture including the evaluation of the end-to-end QoS of network services and the validation of the admission control. This is used to support traffic engineering in the design of the algorithms and their parameters.	TEQUILA monitoring architecture goes beyond the diagnostic role of current monitoring functions in best-effort networks by becoming an important tool for providing real-time feedback information for: • Assisting both IP and MPLS traffic engineering in network provisioning and long-term planning • Assisting traffic engineering automatically in real-time in optimising the usage of network resources through performing dynamic resource allocation at node and network level as well as dynamic route management • In-service verification of QoS-related traffic & performance guarantees of value-added IP services negotiated between a customer and a provider and specified in Service Level Specifications (SLSs)
Scalability principles considered for the design of monitoring architecture	• For active measurements the user can decide either to request detailed per-packet information or to receive results aggregated over specified time intervals. • For probing large networks the master stations collecting the measurement information are distributed to remote network regions • The measurement server represents the central part of the measurement architecture. It can handle an arbitrary amount of measurement agents (limited by the performance of the server machine and the network), which are installed independently and which can either register themselves automatically at the server or are entered to the measurement database via the GUI. • While application-like measurement flows are used to stress the network with synthetic traffic, the additional load produced by probing flows is negligible	• Defining the monitoring process granularity at the aggregate level of PHB and LSP/IP route level (and not at packet level) for data gathering • Distributing the data collection system at node level for processing and aggregating data at source • Minimizing the measurement transmission overhead by employing event notification and summarization of statistics • Using aggregate *performance* measurements combined with per SLS *traffic* measurements by carrying out *performance* measurements at the LSP/IP route and *traffic* measurements at the SLS levels. This reduces the amount of synthetic traffic injection for carrying out the SLS *performance* measurements as several SLSs may use a single IP route/LSP.

Subject	AQUILA	TEQUILA
	in most practical cases. • Router monitors are distributed near the monitored routers (to keep the traffic between routers and their monitor local) and report only selected results to the measurement database.	• Reducing the amount of synthetic traffic by using hop-by-hop measurements and calculating edge-to-edge results for lower priority traffic in case of MPLS -TE where there might be a huge number of LSPs for monitoring • Controlling the amount of synthetic traffic by having a trade-off between the synthetic traffic load and sampling frequency

Table 7: *Comparison of the AQUILA and TEQUILA measurement approach (General Principles).*

Subject	AQUILA	TEQUILA
Monitoring System Components	• Distributed active measurement agents located near the end-user host for the generation of application-like measurement flows and within the providers network for the generation of aggregated flow load situations. • Active probes located at network edges of the providers network. • Central management station/s for QoS data collection and storage. • Traffic generators at the distributed measurement agents for generation of application-like flows. • Router monitors near the routers for collecting QoS relevant data from the routers (e.g. queue depth, conformed/exceeded traffic, packet drops, traffic rates per traffic class). • A QoS measurement database for storing and archiving configuration of measurement scenarios and measurement results from both active and passive measurements. • GUI for the configuration of measurement scenarios and the graphical display of measurement results. Monitoring of the measurement results during the running measurement flow and for performing data analysis afterwards is provided.	• Distributed active probes and passive monitoring agents attached to every router in the network • Distributed Node Monitors (i.e., one per router) for initiating, receiving, aggregating, and processing node-related measurements. Each Node Monitor can initiate active measurements between the router attached to it and any other node in the network and passive measurements on the router attached to it. • A centralised Network Monitoring for network-wide post-processing of measurement data. • A centralised SLS Monitoring for customer related service monitoring, auditing and reporting. • A Monitoring Repository for storing configuration and measurement information. • Monitoring GUI for displaying measurement results at node (PHB), network (LSP/IP route), and SLS levels.
Service Assurance	• Service monitoring is part of central management station/s. The measurement database holds the states of the distributed measurement agents.	• For scalability reason, a separate entity for in-service verification of the traffic and performance characteristics of customer-specific SLSs is provided.
Data Export Protocols	• CLI is used to get information from the routers, support for using SNMP is designated.	• CORBA interfaces used for communication of monitoring components with one another and with

Subject	AQUILA	TEQUILA
	• Proprietary protocols based on TCP are used for the communication between the distributed agents and their corresponding management station. • HTTP between measurement database and GUI.	external components. • COPS, SNMP, CLI, etc. used to export the data from routers to a Generic Adaptation Layer (GAL) which passes measurement results to the monitoring agents.
Technologies used for implementation	• Because of performance and accuracy reasons the distributed agents and the management stations are implemented using C++. • Router monitoring is implemented using Java2 connecting to the AQUILA architecture via CORBA. • The measurement database is currently based on MySQL. • The GUI (a standard web browser) accesses the measurement database via HTTP by using PHP and the Apache web server. • GPS in combination with NTP is used to synchronise the measurement agents to enable one-way measurements.	• All monitoring system components are implemented using the object-oriented approach, i.e., Java language on a Java 2 platform. No of the shelf monitoring component is used. • ORB (CORBA infrastructure), XML, Oracle and graphical libraries are used for implementation of the monitoring system. • Monitoring Repository is implemented using Oracle v 9.0.
Standards techniques Used	• IPPM, ITU-T, SNMP, HTTP, SQL	• IPPM, RMON, COPS, SNMP
Device drivers Implemented	• GPS-equipment is used for clock synchronisation. Device drivers are provided by the equipment manufacturer.	• for Cisco, Linux, IFT (IP fast Translator) routers

Table 8: *Comparison of the AQUILA and TEQUILA measurement approach (Design and Implementation)*

Subject	AQUILA	TEQUILA
Measurement data types	• Per-packet information ("raw data") • Statistics ("aggregated data")	• Statistics • Event notification: This method avoids overloading the network by reducing the export of large amount of data from monitoring nodes to management entities.
Measurement aggregation	• At the distributed measurement agents; time intervals are configurable by the users.	• At the node level in order to reduce the large volume of measurement data near the source for transmitting the data efficiently to the management entities
Threshold crossing notification	• currently none.	• Asynchronous notification of threshold crossing events in real-time from nodes (Node Monitors) to the registered clients
Data Export Mode	• Data is available in the measurement database and accessible e.g. by using	• "Push" the threshold crossing events to the clients by Node/Network

Subject	AQUILA	TEQUILA
	standard techniques like SQL and ODBC/JDBC. In addition the data can be exported via the GUI, which supports both graphical display of the results and comma-separated value (CSV) lists.	Monitoring • "Push" the statistics to the clients by Node/Network Monitoring
Measurement methods	• Active measurement • Passive measurement (router monitoring)	• Active measurement and passive measurement
Active Measurement	• End-to-end performance measurements at the traffic class levels (using DSCP field)	• End-to-end performance measurements at LSP level in MPLS-TE • End-to-end performance measurements at IP route level in IP-TE • Hop-by-hop performance measurements at PHB level
Active measurement Protocol Implemented	• The implemented proprietary TCP-based control protocol between the management station and the measurement agents is comparable to the IETF IPPM protocol draft "draft-ietf-ippm-owdp-03.txt"	• The implemented one-way delay and loss measurement protocol is generally based on the Internet-draft "A Framework for Synthetic Sources for Performance Monitoring: draft-cole-sspm-03.txt"
Passive Measurement	• Data gathering from the MIBs via CLI from selected routers. Support for SNMP is designated. • Monitoring of incoming traffic (input parameters) on edge devices per flow reservation, e.g. number of conformed/exceeded packets. • Monitoring of outgoing traffic (output queues) on edge devices and core routers per flow aggregates (traffic classes), e.g. number of total/dropped packets.	• Data gathering at every router • Sources of passive measurement data: MIBs, PIBs, metering information from traffic conditioners, and in case of Cisco routers MIB-2 information for LSP traffic measurements, CAR MIB for SLS/macro flow traffic measurements, and QOS MIB for PHB related measurements by using CLI.

Table 9: *Comparison of the AQUILA and TEQUILA measurement approach (Measurement Data & Methods).*

Subject	AQUILA	TEQUILA
Monitoring levels	• Single and aggregated flow monitoring at application level, node, and network level monitoring.	• User/customer flow monitoring, traffic aggregate monitoring at node and network-wide levels
Performance related measurements	• One-way delay, packet loss, packet loss patterns, IP packet delay variation (IPDV) and throughput at network service level (DSCP) and application level.	• One-way delay and packet loss at the LSP, IP route, and PHB levels
User traffic flow related measurements	• Per-flow measurement of user generated traffic is not part of the AQUILA DMA. The input parameters of the incoming traffic (see above) can be requested through the AQUILA EAT (end-user application toolkit).	• Throughput per SLS and macro flows at egress point • Offered load per SLS and macro flows at ingress point

Subject	AQUILA	TEQUILA
Network workload related measurements	• Measurements per traffic class at the output queues of routers (edge and core): • Packets/Bytes transmitted/dropped • Queue depth • Link utilisation in/out	• Bandwidth usage per PHB per interface • Throughput per LSP • Packet Discards per PHB per interface • Link utilisation in/out
Network diagnostic	• Path reachability/connectivity	• Link and device availability

Table 10: *Comparison of the AQUILA and TEQUILA measurement approach (Metrics).*

Subject	AQUILA	TEQUILA
Modularity	• The active measurement part can run standalone, i.e. independently from the AQUILA network. • For small probing scenarios (up to 10 measurement agents) no management station with the measurement database is necessary.	• The monitoring system is implemented as a standalone system in a modular fashion. The monitoring system can be used independently from Tequila system. It is also possible to use any component of the monitoring system without modifying the remaining part of the system.
Flexibility	• Measurement scenarios (i.e. load generators, aggregation times, measurement periods, etc.) can be specified by the user via a GUI or by directly entering. • For application-like measurement flows, a state-based flow generator that supports different distributions is implemented, which provides high flexibility in the parameterisation of application-like traffic. • For application-like measurement flows the possibility of using trace-files is provided. Traffic traces (packet sizes and packet inter-arrival times) from real applications can be recorded by using network sniffers (e.g. tcpdump) and reproduced by the measurement agents. • Measurement agents register themselves automatically at the management station with their IP address or netmask. • The web-based GUI can be viewed with a standard browser on any platform. • The GUI provides the results in comma-separated value (CSV) format, which can be imported into further software programs for post processing.	• The monitoring system is managed through policy based high level configuration at node level, network level, and monitoring parameter level (such as specifying synthetic traffic injection rate and packets sizes, etc). • Clients (i.e., any TEQUILA system component that needs measurement information) can request for one/more monitoring function to be initiated. • Clients can specify the monitoring metrics, the threshold parameters, and the time for receiving the periodical statistics. • Clients have the option of requesting one/more aggregation functions to be applied to the data chosen form a set of available statistical functions. • Network and SLS monitoring can provide current/historical longer-term in-depth statistical analysis requested by clients/manager/users. • GUI provides an interface through which users may request display of any measurement data at the node and network level extracted from the monitoring repository.

Subject	AQUILA	TEQUILA
Reliability	- Measurement data is reported via TCP. Lost connections and other failures during the measurement process are reported in the measurement database.	- A reliable data transport mechanism for reporting events and statistics is employed that ensures that the network must not become unstable as a consequence of losing measurement data.
Interoperability	- The DMA inter-operates with the AQUILA QoS architecture (automatic reservation for application-like measurement flows).	- This is not addressed.
Security	- Security is currently not addressed in the AQUILA DMA.	- Although the security is not yet addressed in the implementation of monitoring system, the CORBA Security service provides a security architecture that can support a variety of security policies including security of communication between objects. This requires trust to be established between the client and target, which may require authentication of clients to targets and authentication of targets to clients. If also requires integrity protection and (optionally) confidentiality protection of messages in transit between objects.

Table 11: *Comparison of the AQUILA and TEQUILA measurement approach (Features).*

Subject	AQUILA	TEQUILA
Accuracy	- For accurate one-way delay measurements, the measurement agents are intended to be equipped with GPS cards.	- One-way delay and loss measured by TEQUILA monitoring system are compared against the measurement results obtained from a hardware test equipment (e.g., SmartBits). - One-way delay and loss measured using two different approaches, i.e., edge-to-edge and hop-by-hop are compared.

Subject	AQUILA	TEQUILA
Benefit/cost	• Benefit is to get a view of the network under test, i.e. the path performance characteristics as well as the router state information. • Associated costs are the introduction of synthetic traffic for active performance measurements and the communication overhead introduced by the control traffic and result reports between the measurement agents the management station. • Regarding deployment costs: The implementation itself is based on hardware off the shelf (PCs possibly equipped with GPS) with Linux as operating system.	• Benefit is the improvement to the dynamic operation of network attributable to the monitoring system by detecting both congestion and under-utilization in the network. • Associated costs are the introduction of synthetic traffic and the communication overhead to transfer node/network level measurements to the related management entities.
Scalability	• To minimise the measurement data overhead transmitted over the network, result aggregation (i.e. calculation of statistics) can be done at the distributed agents, but on the other hand detailed information per measurement packet can be requested by the user. • The volume of synthetic traffic is configurable by the user. • The relational measurement database is designed to keep large amount of data in a compact form, so that also measurement results from a large number of measurement agents can be stored efficiently.	• Scalability of monitoring system, when there is a large number of edge-to-edge measurements (in case of MPLS-TE), is tested in terms of volume of synthetic traffic injected to the network. • Scalability of monitoring system, when ingress/egress Node Monitors have to do large operations in supporting multiple clients, is tested in terms of response time of Node Monitors. • Scalability of Network Monitoring, when it has to do large operation in concatenating hop-by-hop measurements and in supporting multiple clients, is tested in terms of its response time. • Scalability of SLS monitoring in auditing a large number of SLSs is tested in terms of response time.
Stability	• Measurement results from the DMA are not automatically imported to the resource control and can therefore not influence the network operation without user interaction.	• As the traffic engineering reacts to the measurement information provided by the monitoring system, the monitoring system must ensure that the network must not become unstable as a consequence of its function.

Table 12: *Comparison of the AQUILA and TEQUILA measurement approach (Assessments).*