UNIVERSITÀ DI PISA

Facoltà di Ingegneria

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

Progettazione e Realizzazione del Modulo di "Traffic Engineering" nell'Ambito della Piattaforma e-learning del progetto EuQoS (EU)

Tesi di laurea

di:

Luca Luigetti

Relatori:

Prof. Luciano Lenzini

Prof. Cosimo Antonio Prete

ANNO ACCADEMICO 2006-2007

Table of Contents

1 Introduction

The phenomenal growth of the IP network, and the convergence of other networks, such as radio, telephone and television to the internet, set up a new kind of problems, especially the technical features to provide the offered service completely usable. In fact, it is necessary to guarantee a good level of quality to this new real time applications and it is not possible by the actual telecommunication networks.

Of course, all these new factors are placing strenuous requirements on the internet, most of wich can hardly be achieved because they fall on the border or outside of the Net's origin design goals and resultant capabilities, so that, the problems related to the Quality of Service (QoS) in the telecommunication field, are actually object of intense study and research.

Every network based on the Internet Protocol (IP), like the Internet, is able to provide only best effort delivery of data.The advantage of this kind of architecture is that the core of the network remain simple (IP routers have only to perform a single table lookup to forward the packets and if it is congested, packets may be delayed or even dropped). This simplicity allows the network to be scalable to future growth and partly explains the Internet's success.

Unfortunately, this policy has sufficed for typical Internet application (e.g. Email, file transfer and web surfing) but the new applications cannot adapt sufficiently to inconsistent service levels due to the variable delivery delays and data loss. Multimedia elements can be found in these new applications demonstrating the need for more bandwidth to carry audio and video and, in addition, some of them certainly have strict timing demands that the best effort service of the internet is not able to meet. An increase in bandwidth is a necessarily first step but is not definitely a complete solution because application traffic is frequently burstly, producing temporary congestion, and congestion means delays and data loss. Moreover, for certain application like telephony, the central issue is latency rather then bandwidth, more precisely, what the congested Internet cannot presently control.

The solution is that some intelligence must be introduced into the Internet so that it can differentiate traffic with strict timing requirements from those that can tolerate delay, so that , IP networks can support active management of their bandwidth resources. This is where QoS is involved. About this matter, the European project EuQoS was started in September 2004 as part of the EU Framework Programme 6, whose goal is to research, integrate, test, validate and demonstrate end to end QoS technologies to support infrastructure update for advanced QoS-aware applications over multiple, heterogeneous network domains, belonging to research, scientific and industrial communities. Among the partners of the project, there are different European telcos, SMEs and universities that cooperate to reach the final goals. To achieve its ambitious objectives, EuQoS involves several activities that runs from the commercial coordination and management to the software core programming and so that, the whole project is divided in 6 Work Packages; WP6 (Work Package number 6 called Dissemination, Standards and Training) is the EuQoS section which deal with the e-learning activities and focuses on delivering the project results to the public. This shall be achieved by four activities, namely development of training material, delivery of training, standardization contributions, as well as dissemination by demonstrations and publications. Within this context, a course based on distance learning technologies is being developed. This e-learning system concerns all the technology studied, developed and used in the EuQoS activities and works as a support for people involved in the project, networking students and in general for the dissemination of the EuQoS research. In the first EuQoS phase, work package 6 develops seven e-learning modules, all of them related to QoS and related areas.

The goal of this thesis work is to develop the Traffic Engineering e-learning course among the EuQoS project. The course platform provides the learning content, the quizzes, the logbook for the student's notes, and the discussion board of the EuQoS pilot course. University of Bern, wich carry out the coordination role among the WP6, operates the commercial course platform WebCT CE for this purpose.

The EuQoS e-learning system is composed by two main branches:

- Theory Section concerning know-how about the dealt technology. In this work the main aspect of the Traffic Engineering and of the MPLS protocol (Multiprotocol Label Switching) are discussed. This part has been developed based on the IRNSI platform (Internet Remote Network Simulation Infrastructure) and a lot of interactive animations have been integrated.
- Hands-on Session where the Theory Section just studied is applied to solve real problems. For this purpose a Network Simulator laboratory has been configured. Students are able to remotly use this lab (run simulations, analyse graphics results, ecc.); moreover, by the virtual machines system, a maximum of 4 students can use the laboratory at the same time.

The accomplishment of this work has required the participation to several international meetings in order to integrate the Traffic Engineering module inside the whole EuQoS e-learning architecture. Furthermore, the system developed has been used in the course "Advanced Networking Architectures and Wireless Systems" held by Prof. Luciano Lenzini at the University of Pisa, and in the course "Multimedia Communications" held by Prof. Torsten Braun at the University of Bern; the feedback received has allowed the continuous validation and the improvement of the obtained work.

This thesis work is organized as follow: the chapter 1 describes the actual status of the e-learning research; the chapters 2 is an overview of the EuQoS project to introduce the EuQoS e-learning system that is detailed described in chapter number 3. In chapter number 4 the specific Traffic Engineering e-learning module, that I have implemented during this work is illustrated, while the laboratory architecture, which is part my work, is more specifically described in chapter 6. The chapter 5 describes the authentication architecture of the EuQoS e-learning system and chapter 7 ends this work reassuming the main conclusions.

2 E-Learning

2.1 E-Learning Overview

Distance education can provide a richer and more engaging educational experience than is possible within the confines of the classroom. It requires creativity and innovation in the design and development of Internet-delivered materials, especially since materials may have to stand alone, as in the use of delivery technologies.

Online courses lack many well-known features of studying. Take for instance, text markers or the possibility to take notes in scripts. They lack also the contact between students and teachers and between peers. Another factor of somewhat lesser importance is that with conventional learning exists the ability to study almost anywhere. If you would like to keep the script, you would simply store it together with all your personal notes and probably along with the exam too. If, one day, the material were needed--maybe ten years later--you would simply open the cartoon box where it was stored and have it at your fingertips again.

Conventional learning has a lot of advantages and one of the most important is; you are used to it.

But studying online is getting more and more popular. Tutors can, for example, address a bigger audience without a loss of teaching quality. There are many advantages for you too:

You study whenever you like to, the EUQOS course is open 24/24h, 365 days a

> year, it offers interactive content where you apply and increase your skills, you get pointers to additional lecture and content and are able to access it at once, many useful tools are integrated, such as a glossary or a discussion board.

Distance education existed long before the Internet, but it has become more prevalent and has changed significantly through technological advances. All sectors, especially higher education, corporate training, and continuing and professional education, want to take advantage of Internet technologies. Their interests are: to provide education, training, and collaboration capabilities to geographically dispersed populations to enhance educational experiences and increase enthusiasm for learning.

Comparing conventional and online learning, there is still a lot to improve in online learning. But already now, online learning offers a rich environment with many useful and interesting contributions.

Generally, E-learning is going to consolidate its importance in teaching and will be matured to the point that it should no longer be considered as an independent initiative, but rather one of many tools used for instruction and information distribution.

2.2 Benefits

The growth of e-learning and its destined change will be seen through information systems, as well as, through the communication infrastructure. This in turn will consent to the experimentation and the concentration of the communicative model rendering it more sophisticated and capable of offering greater learning opportunities both through the fronts of economic standard and quality.

The never-ending increase of *Internet* use non only produces the simple realization of diverse technologies but also modifies the speed and the habits of the people as they work. For this reason, the concept of *e-learning* does not limit the transfer of informational content over the internet, but is a method that will nurture the didactic process thus increasing the value of traditional learning with the integration of the communications technologies.

E-learning, as we know, it has been around for ten years or so. During that time, it has emerged from being a radical idea—the effectiveness of which was yet to be proven—to something that is widely regarded as mainstream. It's the core to numerous business plans and a service offered by most colleges and universities.

In general, where we are now in the online world is where we were before the beginning of e-learning. Traditional theories of distance learning, of (for example) transactional distance, as described by Michael G. Moore, have been adapted for the online world. Content is organized according to this traditional model and delivered either completely online or in conjunction with more traditional seminars, to cohorts of students, led by an instructor, following a specified curriculum to be completed at a predetermined pace. In general, the idea that e-learning will completely replace the ordinary teaching procedure is going to fail, but it is indeed that the integration of e-learning courses using new technology will upgrade the traditional system.

Another analysis to understand the e-learning development concerns people who use it. As we approach the halfway mark of the new millennium's first decade, the nature of the Internet, and just as importantly, the people using the Internet, has begun to change. These changes are sweeping across entire industries as a whole and are not unique to education; indeed, in many ways education has lagged behind some of these trends and is just beginning to feel their wake.

One trend that has captured the attention of numerous pundits is the changing nature of Internet users themselves. Sometimes called "digital natives" and sometimes called "n-gen," these new users approach work, learning, and play in new ways.

They absorb information quickly, in images and video as well as text, from multiple sources simultaneously.

In learning, these trends are manifested in what is sometimes called "learner-centered" or "student-centered" design. This is more than just adapting for different learning styles or allowing the user to change the font size and background color; it is the placing of the control of learning itself into the hands of the learner.

With *Web Based Training* one may be able to define a strategy orientated for and to give the “students” the possibility to digest the material and learning experience in a ubiquitous manor that may serve their every need. Another benefit is gained by the augmentation and possibility of integration in a flexible manor with all available informational material, i.e, the support of the internet alongside the actual “distance educational course. All of this is an advantage brought to the “classroom” through the introduction of innovation and organisation through the online atmosphere.

The changing demographics of the student population and the more consumer/client-centered culture in today's society have provided a climate where the use of student-centered learning is thriving".
Another big problem to tackle is that concerning the rapidity of content becoming obsolete. The material matures before its’ time thus imposing a huge effort and flexibility concerning the response to this problem. To be able to properly govern the informational processes the solution given by the experts is to be as dynamic as possible adapting and integrating new technologies without haste. This is accomplished in part by informational services being inserted into the working and business environments, whereby, limiting the down-time associated with changing educational needs. These are some of the motives

why the *e-learning* solutions are becoming standard, and more importantly, a success at every level of organisation.

2.3 Application Field

At the moment there are two principle fields of application of *e-learning*; on one side there are the schools and universities, where *e-learning* is being applied for distance learning courses and for those who are disadvantaged, on the other side there are the businesses, they create the richest (biggest) piece of this market. At this point in time, public administration is in its` infancy with respect to integration, there is only a marginal role. (This is even considering the fact that, commonly speaking, *e-government, including all branches, judicial and the like,* are at the frontier of P.A) But it wont be long before the public will be directed toward *e-learning* to form the new professional figures asked for by the market. Many businesses fall back on this as a means to save time, space, and money. Others instead, have found it to be extremely useful means to communicate throughout the workplace, to put out work related circulars. These two models are very close between themselves, but the tendency seems to be for the second to be the dominant model. Here, the technologies are applied in the best manor, access is graduated with respect to the internal structure of each professional environment.

E-learning is one the sectors of *ICT* with the major margins of growth; it is the sector where there is a concentration of hope and an expectation of investment opportunities. For some it is a bet worth winning, for others, it is the future knocking at the door. Even if the tone and optimism seems to resemble what was characterized as the *New Economy* during the bi-annual 1998-1999, the *e-learning* represents a new flight, synonymous with what is now called the "*Net Economy*". Actually, between the two different phenomenon there are many similarities even if the initial presumption is better.

Far away from aggressively accusing, at the point of tears, asking for stratospheric financing, *e-learning* from the other shore, has individualized a simple track to surpass the obstacle: to develop the offer in the segment of "*Business*" (in particular, businesses and academic institutions, two subjects that are adequately connected).

Analyzing the situation from the other shore, the panorama is generally comforting, and as evidence there is an analysis of *e-learning* compiled by the Brandon-Hall Studio. Within their research it was found that 49,9% of the businesses in the USA have already implemented a information platform based on *e-learning*, while the major part of the rest intend to initiate one shortly. Even with the business approach, as can be seen with this sensus between employees and the majority. In particular, 90,4% of Americans businesses consider *e-learning* an efficient means to satisfy the needs of their employees.

In Europe, *e-learning* is still in a fase of infancy, but for this reason in particular, it is ready for a substantial growth. It is important, above all, to create a strong cultural base on information technologies and the internet (*online training and knowledge*), putting more weight inside businesses, using developments through the new and evolving technologies.(Even if said technologies aren't been approved)

As a testimony to the fact that Distance Learning is alive and well consider these recent facts from the most prestigious and authoritative society of research, the IDC (International Data Corporation) and the Gartner Group. The research is different only in terms of actual numbers, but the analysis shows, without a doubt, a definite *trend* in the growth of the sector. This can be seen not only with the operators of the "*the stars and stripes*", but more importantly in Europe where the waters have remained stagnant as of to date.

The opinions of experts at high levels, like -- Lester Thurrow, principle of the Sloan School of Management of MIT--*e-learning* has transformed quickly into a true and real competitive advantage or what has been sustained by the theories on intellectual capital, information transmission will become e real business (Thomas Stewart).

E-learning is already one the growing factors and has been affirmed by the business sector. The transmission of knowledge through methods and instrument technologies, in fact, not only allow the optimization of presentation of single dependents, but above all, creates un hypothesis of success. The diffusion of the role of *e-learning* is growing with respect to managerial positions, as can be demonstrated with the interests and the attention supplied by the manifestation of the thesis.

2.4 Technical Environment

One of the first problems that the organizers of an online information activity must face and resolve is related to creating the technological infrastructure that is carry out said goals. The selection and goal of a system online activity is geard at being completely user-friendly and adequately supported due to the various implications; economic order, methodology, didactic, and of course, organization. Generally speaking, the infrastructure problem may be confronted with two different alternative solutions.

The first of the these solutions consist of being equipped with a minimum technological infrastructure, pointed more in the direction of an interactive interpersonal *tutor*—student to student. In this manor, the student, consequently, is capable of managing said interactivity which would best suit their specific needs. This solution tends to be used at a greater frequency, with online teaching and resources where everyone actually is involved in the online environment. Keeping in consideration that at times, the introduction of various instruments and ambient software be introduced to resolve problems as they would be encountered. For all intensive purposes, this hypothesis may be termed *weighted solutions*.

The second solution consists in the adoption of real and true technological platform structured to specific parameters to the informational experience. This in turn stabilizes certain criteria be chosen for the specific platform thus utilizing a regimented successive process for the interaction of the—tutor—student to student—student to resource— or student inserting other means into the process, like the realization of operational analysis, monitoring, or archiving data, simply put, valuation of the complete process.

About the technical environment, the dominant learning technology employed today is a type of system that organizes and delivers online courses—the learning management system (LMS). This piece of software has become almost ubiquitous in the learning environment; companies such as WebCT (used also in the EuQoS e-learning system), Blackboard, and Desire2Learn have installed products at thousands of universities and colleges and are used by tens of thousands of instructors and students. The learning management system takes learning content and organizes it in a standard way, as a course is divided into modules and lessons, supported with quizzes, tests and discussions, and in many systems today, integrated into the college or university's student information system.

The future trends of may be played through a simulation of reality through a virtual simulator. The power of the multimedia technology has been developed, acknowledged for its ability to utilize and integrate various media for information distribution: working papers, dynamic and statistical imagery, sound, in the end, everything necessary to simulate the situation in real time.

But what are the real environments that informational solutions may be applied for the goals required for distance learning?

At this point in time, it is possible to classify at least three:

1. Informational packets constructed of examples that coincide with theoretical knowledge; online books being based on the hierarchal process;

2. Training instruments geared to the working process; this is the case where the computer not only is the medium information transmission but also becomes the daily instrument of work;

3. Instruments based on virtual reality;

The first applicable goal, that which is more diffused, is the anticipation of distance learning information where the didactic material is constructed by information available online. This of course is periodically reviewed within the informational services for distance learning offered online by universities or businesses within the managerial knowledge and/ or knowledge related to technological theory.

A very important side to this ambient is constructed by the application of *knowledge management.* Throughout the written texts it can be seen and localized the results and developments of the local *expertise* in the organizations.

The second applicable environment looks more to the opportunity of putting forth new ideas or informational strategies, topically associated with *learning by doing* within the simulated context. This is already possible within those working environments where the computer has been adapted for both work and a medium of communicative knowledge.

In general e-learning may be used by a variety of complex functions and thus will bring about a proliferation and diversification of the instruments already in circulation.

There has always been two tendencies in vigor that are at opposite ends of the spectrum. The one is oriented at the integration of the greatest possible number of functions within a single platform, a stand-alone software that is sophisticated and very complex. The other is more focused on the production of a specific environment specialized or partially specialized to a goal oriented method.

Together, one speaks of more than 500 platforms and integrated environments in circulation today for the diffusion and application of online information activities. And, within that number there already have been valuated those systems different between themselves, for instance; the big platforms of client-server to objects for quiz production and interaction for distance education. This can be seen to be a significant number when one considers the different types of software that are on the market today.

Two reasons stand out as to why there are some many different types:

1. First, there is an enormous quantity of investments in this direction. This can be seen by how online information is considered one of the businesses of the future. The "market" has of yet to reflect this change as can be deducted by the fact that there still is not a standard;

2. The emphasis is greatly on personalization and specialization rather than on the small quantity of requests to make the online distribution more smooth. Instead, there are much more research on the study of solutions to resolve problems associated with the *single experience*.

In reality the tendency of the proliferation of the platforms one may be able individualize the motives for the general order; the information online is an argument that can be easily circumnavigated. This implies different approaches and strategies be used, very diverse between themselves. There is a multitude of variables on the table that bring one to confront the problems with alternative solutions. One comes to the conclusion that it is impossible for a universal solution to exist and therefore can never be created.

3 EuQoS Project Summary

3.1 EuQoS Overview

As already introduced, the main objective of the EuQoS project is to find a solution for assuring QoS in the multi-domain and heterogeneous network environment.

The solutions to this kind of problems and the network restructure will allow Internet to support the new network applications and at the same time this will allow the ISP, network operators and other service providers to promote new kind of services.

The provide QoS guarantees, EuQoS propose a three sequential phase solution:

- The first phase involves the neighbors domain to define commercial contracts. The aim of this contracts is to agree about the inter-domain resources allocation for each class of service
- During the second phase, called *provisioning*, the inter-domain resources will be allocated belonging to the commercial agreement. At the end of the provisioning phase, each domain has assigned some guaranteed resources for each class of service but these resources are not allocated to some user flows. In fact, each domain has still to know which destinations are reachable throughout the domains that have agreed a commercial contract during the first phase. These informations will be exchanged by the inter-domain routing protocol, which will select also the best path, if alternative paths are available.
- After that the provisioning phase is done and after that all the informations about

the reachable resources have been exchanged, the *invocation* phase will starts each time that any user wants to establish a new connection. During this last phase, the user sends a connection request to the AS he is connected to. The AS which receive the request, verifies if any path is present to reach the destination and also if sufficient inter-domain resources to manage the connection are available. If these conditions are satisfied, the resources are effectively allocated to the new connection.

In the EuQoS architecture, the inter-domain Traffic Engineering management adequately drives the inter-domain routing protocol choosing the best path to reach the destinations. Choosing to use a network path rather then an other, at the network layer, implies to use some resources rather then others. So that, an optimal choose of the network path will allows to maximize the amount of traffic that the domain can manage.
Once that the paths to use have been selected, the domain is ready to manage the users traffic flows.
After describing the QoS solution adopted in this project, the global architecture end-to-end will be described focusing on an overview on the Traffic Engineering application.

3.2 QoS in EuQoS

The approach EuQoS uses to achieve its objective, follow the concept, proposed by both ITU and IETF, of establishing in the network a number of, so named, *QoS Classes of Service* (CoS) differing in QoS objectives and types of handling traffic profiles. The CoSs are visible by the end-users (end-to-end CoS) and are maintained via the multiple domain network, even different network technologies are on the way, and this CoSs are translated to specific actions at the network level (dimensioning, admission control and equipment configuration); this allows a scalable approach to the QoS services distribution.

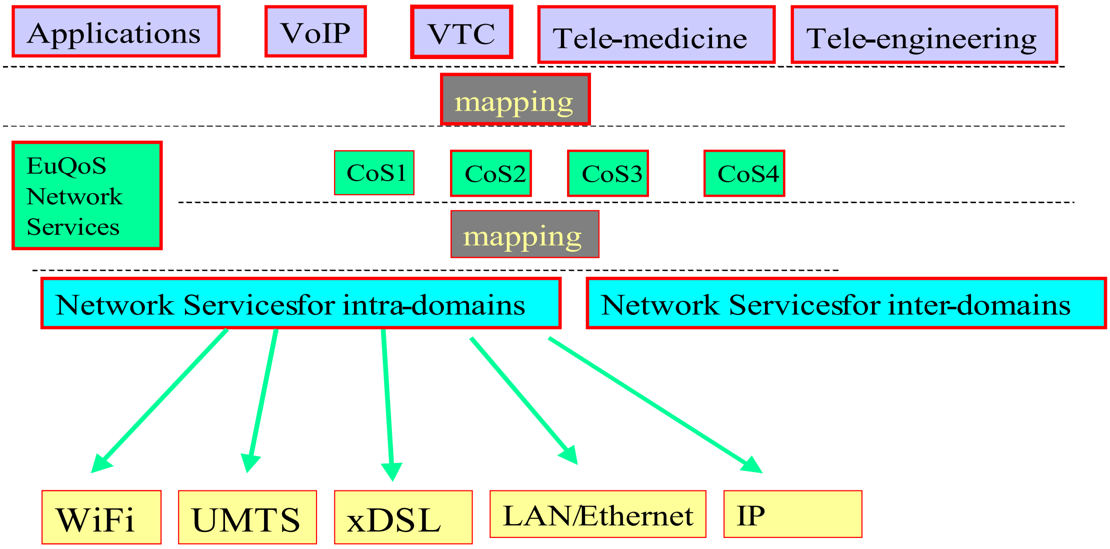


Figure 1: The Role of Classes of Service in EuQoS

The importance of each parameters among the CoS, depends on its importance to influence the quality of service perception of the user. More precisely, a CoS parameter has a limitless value associated when it doesn't influence at all the quality of service's supply and this values are indicated as *Unbounded* or *Undefined (U).* All the others parameters have got a ceiling limit to assure the quality of service.

Aggregate Classes of Service	End-To-End Class of Service	QoS Objectives		
		IPLR	Mean IPTD	IPDV
RT	**Telephony**	10^{-3}	100 ms	50 ms
	RT Interactive	10^{-3}	100 ms	50 ms
NRT	**MM Streaming**	10^{-3}	1 s	U
	High ThruPut Data	10^{-3}	1 s	U
Best Effort	**Standard**	U	U	U

Tabella 1: phase 1 EuQoS CoS.

As you can see in Table 1 structure, two traffic CoS aggregation levels are defined in EuQoS:

- Aggregate CoS
- End-To-End CoS

In the lower aggregation levels (end-to-end CoS), the traffic flows are grouped based on the application type:

- “Telephony” class involves the VoIP applications traffic flows.
- “RT Interactive” involves the video phone or video conference applications traffic flows.
- “MM Streaming” involves audio streaming or video streaming applications traffic flows like TV or radio.
- “High Throughput Data” involves big data transfer applications like FTP or p2p.
- “Standard” involves all the traffic flows related to applications that doesn't require

special QoS guarantees.

The benefits that comes out from the low level aggregation CoS are:

- The advantage to directly aggregate applications traffic flows which use a particular CoS.
- The traffic profile and the QoS objectives are well defined.

This kind of classification guarantees to allocate the necessary network resources to each kind of application that has the QoS requirements defined in one of the end-to-end CoS.

The high aggregation level CoS (Aggregate CoS) joins different kinds of applications wich have similar QoS traffic flows:

- "RT class" (Real Time) join the end-to-end CoS "Telephony" and "RT Interactive" which differs essentially for the bit rate needed.
- "NRT class (Non Real Time) joins the end-to-end CoS "MM Streaming" and "High Throughput Data". Both this kind of applications require a minimum information loose in big data transfers.
- "Best Effort class" contains only "Standard" end-to-end CoS.

Each high level CoS has to satisfy the following features:

- Each Aggregate CoS has to satisfy the more tightening quality of service parameters among the contained end-to-end CoS.
- All the Aggregate CoS have to be projected to manage the most similar traffic flows.

The Aggregate CoS have been developed to optimize the resources allocation in the core networks. This means a better band allocation management to the end-to-end CoS, belonging to the customers request variations. More particularly, let' s suppose that a 300 Mbit bandwidth has been allocated to the aggregated COS "RT", on an inter domain link, and let's suppose to having configurate the border router as to assign a third part of that bandwidth , in a dedicated way, to the end-to-end COS "Telephony", and another third part, still in a dedicate way, to the end-to-end COS "RT Interactive".

With this resources distribution within the "RT" class, we obtain a minimum allocated bandwidth for both the end-to-end COS, while the remaining part can be used indifferently for both classes belonging to the users connection requests.

3.2.1 Provisioning

As far as the end-to-end path establishment is concerned, two options named *loose* and *hard* have been envisioned. In the EuQoS phase 1 the *Loose option* solution is adopted: this means that each AS allocates the resources for each CoS rather then grant resources for each end-to-end path.

The intra-domain resource allocation is implemented according to the internal resources management process. The resources allocation will depend and change according to certain factors like the quality of traffic that each CoS manages, the technology used, the infrastructures updates and variations, or partner commercial agreement variations.

Concerning the inter-domain resources allocation, it is based on commercial agreement between neighboring domain. More exactly, some domain that need to forward its own traffic with special CoS requirements, stipulates a special contract with the border domain and the contract bind the former domain to manage this traffic as agreed. The change or variation of these commercial agreements, involves new intra-domain resources allocation of the interested domain.

As already pointed out, both the intra-domain and inter-domain resources allocation to the CoS is called *provisioning* phase.

In this way, the network resources are dynamically allocated to each flow along the end-to-end path only during the user connection *invocation* phase.

Therefore, when a new connection is started, there is no way to know, if sufficient resources are present in the end-to-end path to support the connection request.

For this reasons, it's necessary to implement a special mechanism in all the crossed domain to:

- Verify the availability of sufficient resources to start the connection.
- Allocate the required resources until the end of the connection (this resources are no

more available for others flows).

In the EuQoS architecture, this operations are made by the CAC module (Connection Admission Control).

The final end-to-end path calculation among all the AS involved is worked out by the inter-domain routing protocol. The inter-domain routing protocol used in the EuQoS architecture is called EuQoS-Border Gateway Protocol (EQ-BGP) and it is a variation of the BGP-4 protocol. The aim of this protocol is to notify the presence and availability of the path for the *destination* and *CoS* pair according to the commercial agreement of the domain.

The EQ-BGP absolutely doesn't know the resources allocation status along the path calculated. The resources presence verification to handle the new connection is made only when the new connection request is done.

3.2.2 SLS

Concerning the matter related to inter-domain service providing with QoS requirements, the actual trend is based on commercial agreements between neighboring domains.

This agreements are called *Service Level Agreement* (SLA). These SLA specify the services characteristics and also the mutual responsibility of the domains involved in the service supplying/utilization.

The *Service Level Specification* (SLS) instead denote the technicals characteristics of the service supplied by SLA.

In the EuQoS context, the SLS concept is used to denote the domains trade agreement to manage the inter-domain resources and the *peering Service Level Specification* (p-SLS) concept defines the unidirectional trade agreement.

More precisely, each p-SLS is a contract stipulated by two domain: one of the two is the service supplier and the other one is the service utilizer. The supplied service provide the correct forward of the traffic flows proper to a specific CoS.

In the EuQoS context as depicted in picture number two, the two involved domains are called *provide AS* and *customer AS*. The provider AS is the service supplier while the customer AS is the service utilizer. The traffic flows run from the router A, of the customer AS, to the router B of the provider AS, and from there the flows are forwarded to the final destination.

The trade contract starts its validity from the router B interface that connects the provider AS to the customer AS and ends its validity in one of the exit which connects the provider AS to others upstream domains.

This means that the incoming traffic from the customer AS could be forwarded and exit in all the the inter-domain links of the provider AS.

The p-SLS stipulated completely describes the traffic profile that the customer AS is authorized to forward to the provider AS throughout the router B , and especially the class of service, the traffic band-width and others details.

The picture 2 shows a p-SLS extension in the customer and provider AS domains.

This descriptions highlights that the p-SLS is an unidirectional agreement because it describes the traffic flows from the customer AS to the provider AS but not the contrary flow. To obtain a full-duplex agreement it is necessary to agreed two p-SLS, and both the AS will be provider and customer.

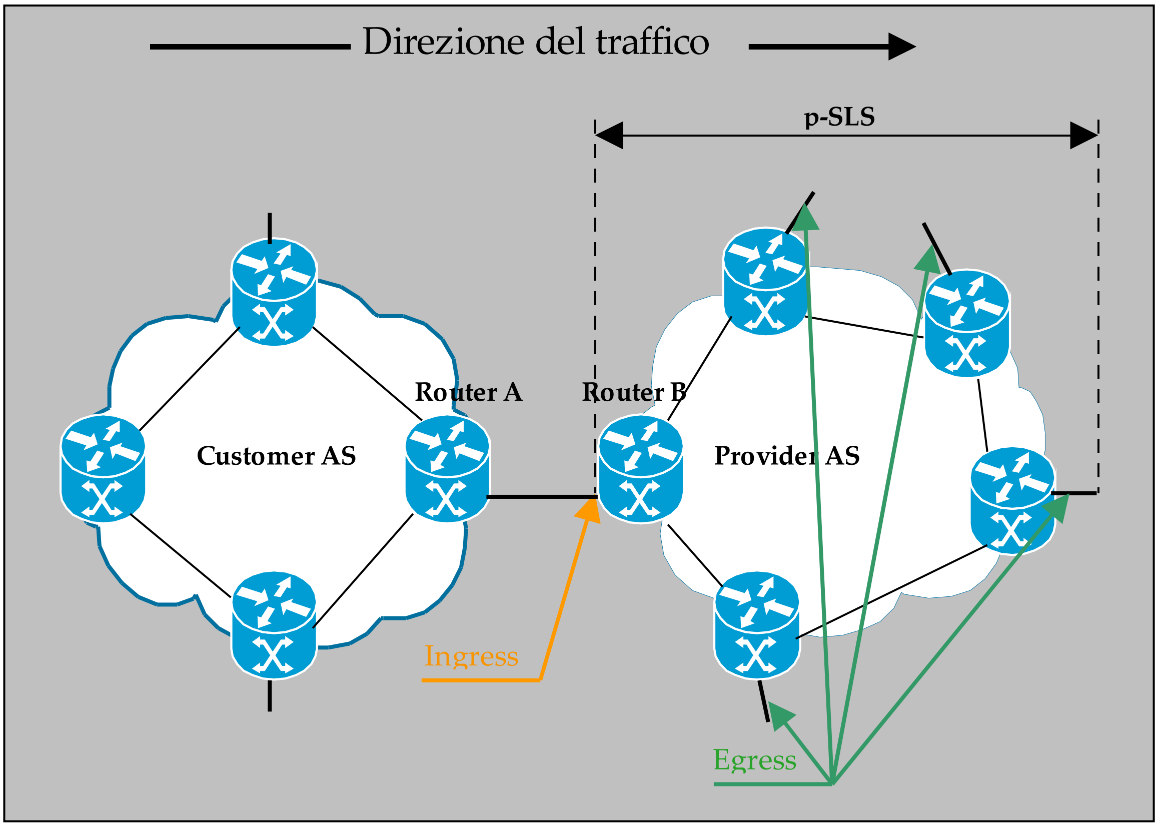


Figure 2: p-SLS Extensions

The main informations described in the p-SLS are:

- The appropriate class of service, and this specify the traffic that the p-SLS could forward.
- The maximum amount of traffic that could be handled.

Therefore, the p-SLS stipulation requires to the provider AS, the inter-domain resources allocation and these will be reserved to the customer AS traffic management belonging to the profile described in the p-SLS.

So that, each domain complete the inter-domain resources provisioning phase for all the handled class of service according to the p-SLS stipulated.

Using the p-SLS concept for the inter-domain resources allocation, a layered logical view of the network substitutes the real physical view.

In the network's physical view, there is only one network topology, according to the presence of the physical link that connect the domains among the Internet.

In the network logical view there are several virtual networks disposed in several parallel layers. Each layer handle the traffic related to a specif CoS.

The network topology associated to this logical network is just a virtual topology and it is generated by the p-SLS domains agreements. Each virtual network topology is associated to a CoS. The picture number three, shows the differences between the physical topology and the new logical view, in the EuQoS architecture.

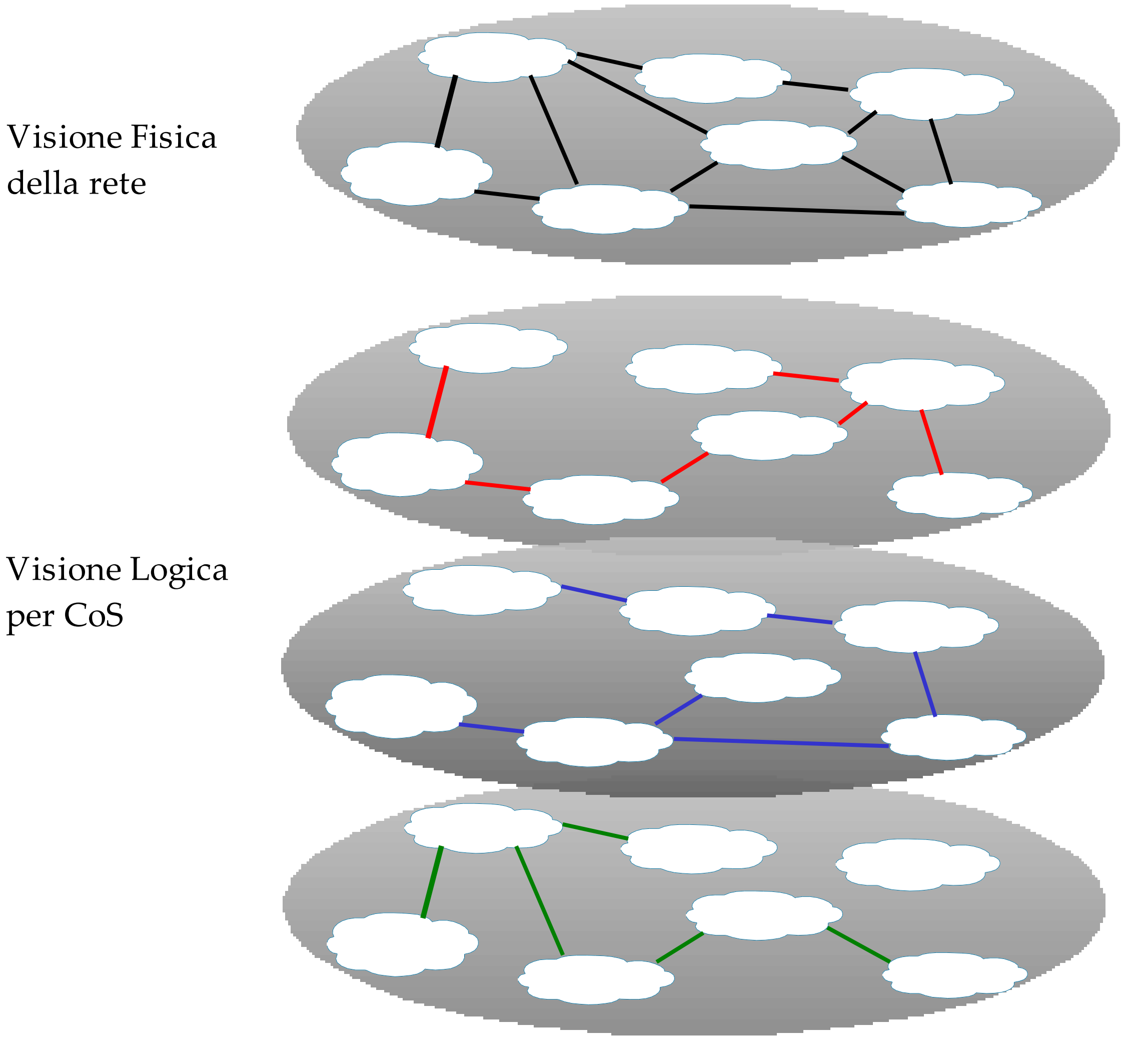


Figure 3: Physical and Logical View of the Network

It worth to noting, that the logical links are a subgroup of the physical links. This can be easily deduced considering that the logical link is just an abstract concept based on the presence of a p-SLS between two domain. The p-SLS depict the kind and the quality of the traffic that could pass between two domain, but to effectively send the traffic a physical link is needed.

3.3 EuQoS End-To-End Architecture

To manage the quality of service, EuQoS develops a distributed architecture.
Each Internet domain implements certain functionality and the concatenation of all the internet domain along the path allows an optimal management of the required connection. The EuQoS end-to-end architecture has two views: a network deployment view across a number of Autonomous System (AS) domains and a software view within an AS. The network deployment view is shown in the Figure four below. The software view, overlaid on the network view is shown in Figure five.

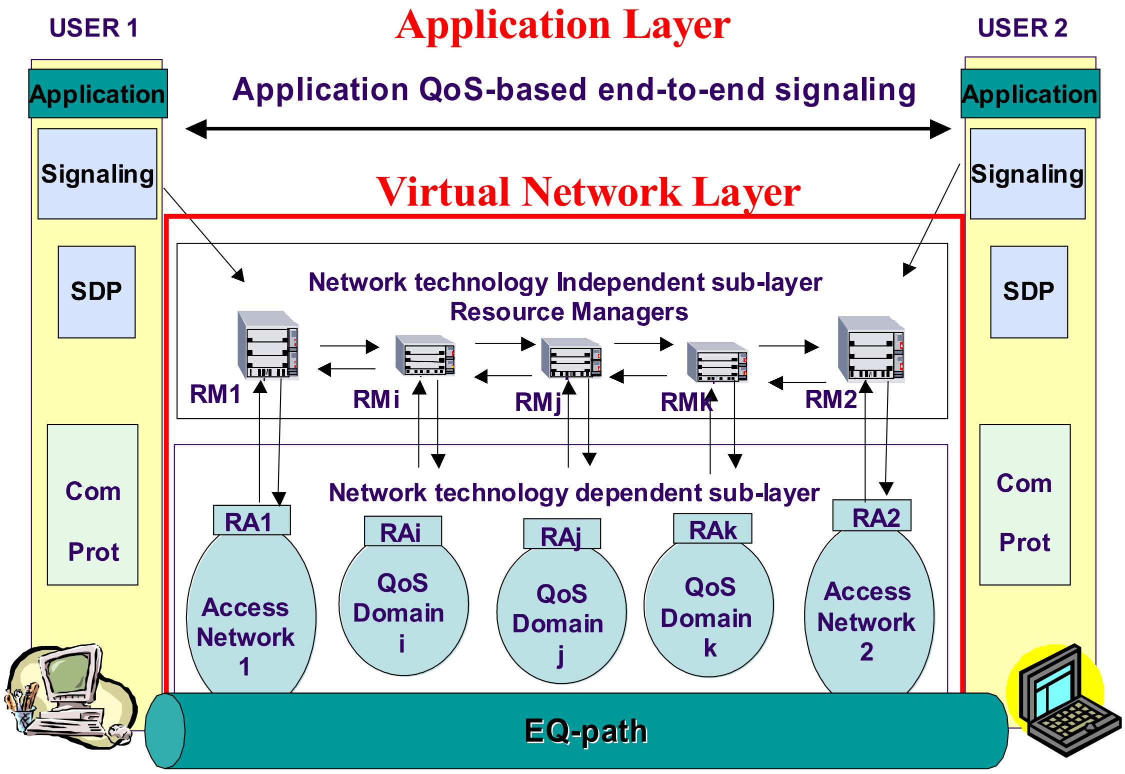


Figure 4: Network Deployment View

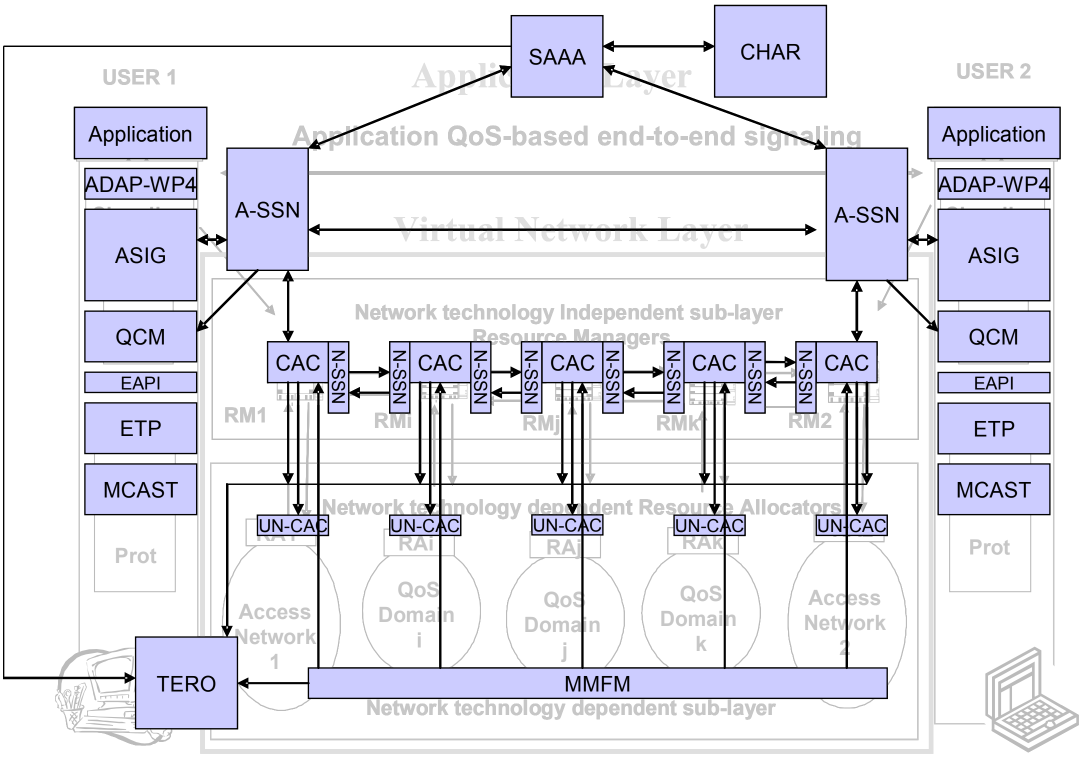


Figure 5: Mapping between the EuQoS and the functional architecture

The EuQoS architecture approach to the manageability challenge is the standard “divide and conquer” approach of reducing the size of problem by splitting it into smaller parts. From the horizontal view (i.e. the different Planes), this implies a clear separation between the Service and Control Plane from the Network Plane. The Control plane is furthermore divided into a technology independent layer (*Resource Manager*) and a technology dependent layer (*Resource Allocator*). From the vertical view (i.e. the different network partitions), this “divide and conquer” approach implies a clear separation between the various access technologies and the different core networks involved in the end-to-end connection.

The aim of the EuQoS architecture is not to provide end-to-end QoS for all applications, which is a significant challenge for large scale, but rather to provide QoS only for the applications which need them and only when they are needed. For this reason, the EuQoS system is based on the *session* concept. When an application sets up a session, this triggers the corresponding network QoS setup. This has the advantage to perfectly synchronize the QoS requirement / setup and the usage of the QoS resources by the application. A furthermore problem which is solved by the session concept is the graceful release (i.e. synchronisation) of QoS resources at the end of their usage by the application. For this purpose, the EuQoS system uses an enhanced version of *Session Initiation Protocol* (SIP), named EQ-SIP, which allows QoS negotiation within the session establishment.

3.4 Traffic Engineering in EuQoS

The optimal resource allocation research, allows the network administrator, to maximize the available resources use and then to maximize the consequent profit.

Moreover, a deep knowledge of the traffic course characteristics among the network, allows to determine some data parameters like medium delay or delay variation and these informations are useful to solve the quality of service management problems in Internet.

Therefore, Traffic Engineering regards the domain behaviour phenomena analysis, related to the traffic flows that pass through it or around it. TE can be divided in two main branches:

- Intra-domain traffic engineering
- Inter-domain traffic engineering

The intra-domain traffic engineering concerns the optimization of the network resources that are all contained within an autonomous system (only one administrative domain), while the inter-domain traffic engineering concerns to manage the resources among an autonomous system and the autonomous systems connected (more then one administrative domain).

Concerning the intra-domain traffic engineering solution in the EuQoS project, there is not sensible difference from the ordinary traffic engineering approach based on MPLS diffserv, intserv ecc. and. In fact, this problem is easiest to solve because only one administrative entity has got the domain control, and it perfectly knows the internal network topology, the amount and the kind of traffic that pass through the domain. In this way the administrative entity can independently decide which are the best technological solutions to better manage the domain.

The inter-domain traffic engineering, instead results harder to be managed because to the already large problems about the lack of technological instruments and datas to appropriately manage the traffic engineering, it adds commercial and political likely problems due to the relationships between the various neighboring domains and in this

direction it has been developed the TERO platform adopted by euqos
Traffic Engineering and Resources Optimisation (TERO) is the module located in the Resource Manager (server side) that takes care to allocate and optimize the inter-domain resources belonging to the commercial agreement defined by the domain.
TERO builds the EQ-path at the provisioning process. More specifically, it controls the interdomain routing process, so as to steer the traffic through the AS in the most effective way, optimizing interdomain resources (i.e., bandwidth and buffer space on the interdomain links) based on QoS requirements.
Furthermore, it configures queues and policers at interdomain links so as to provision the necessary resources to allow traffic to flow across neighboring domains.

The TERO module has the following objectives:

- ***Resource Provisioning***. This entails the provisioning of network resources to different classes of service, according to specific network requirements. Provisioned resources may be either inter-domain or intra-domain. This function is based on the establishment of Service Level Specifications between peering domains (p-SLS), and the task of TERO is to provision resources for supporting p-SLSs (and thus inter-domain CoSs), i.e., to appropriately configure ingress and egress routers for, e.g., traffic policing and scheduling. TERO contributes also to support the p-SLS establishment decision process, by means of traffic analysis and forecast.

- ***Traffic Engineering***. In EuQoS this means controlling the inter-domain routing process, by supporting the decision process of EQ-BGP with appropriate configuration, so that an end-to-end data path is setup for each class of service.

TERO takes advantage of the possibility to influence the EQ-BGP decision process, to finally get its objectives. In this way, TERO can change the traffic forwarding decision throughout the p-SLS of the domain. More precisely, when the domain installs a new p-

SLS, TERO have to configure the EQ-BGP to manage the update associated to the new p-SLS.

Thus, TERO can support the decision process to select the right path by the intelligent management of these parameters. The aim of this support is to maximize the p-SLS utilization in the domain. To manage this functionality and really improve and optimize the traffic management, the allocation state of the resources associated to the p-SLS have to be regularly monitored and TERO can use these informations to change the used QoS Preference Parameters. In consequence of the variations, the configurations have to be updated, but the routers are not directly accessed. TERO manage this work by the functionality provided by the RA-SSN module present inside the RM and the RA-SSN module just send the configuration method and its parameters to the RA.

The Resource Administrator is the only module that knows the network technology used in the domain and then it is able to generate the appropriate configuration commands to implements the TERO rules. This architecture allows TERO to independently work from the network technology of the physical layer.

In the same way TERO interacts with border router through RA-SSN, and not directly. This way TERO need not be aware of the specific router technology.

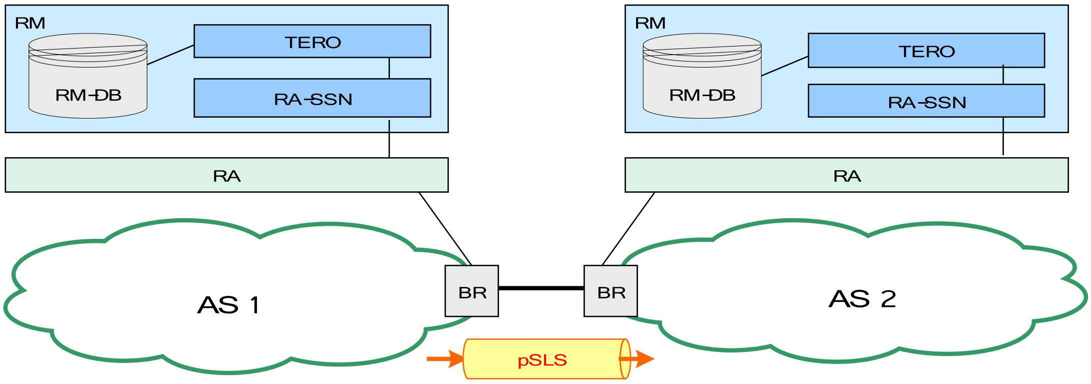


Figure 6: Format of TERO policies

4 EuQoS E-Learning Course Description

4.1 Overall Architecture

The European Quality of Service project (EuQoS) e-learning course is a hands-on sessions' oriented Internet-based course framework. The audiences are computer sciences learners, learners from technical universities and industrial learners such as users and engineers. Each EuQoS module introduces one or more concepts, which have a relation to the Internet and to Quality of Service (QoS). The most important aspects are discussed and introduced with theory, exercises and at least one hands-on session scenario using simulations, emulations or real hardware. EuQoS provides knowledge through trial-and-error approaches and the content will be designed according to certain didactics guidelines.

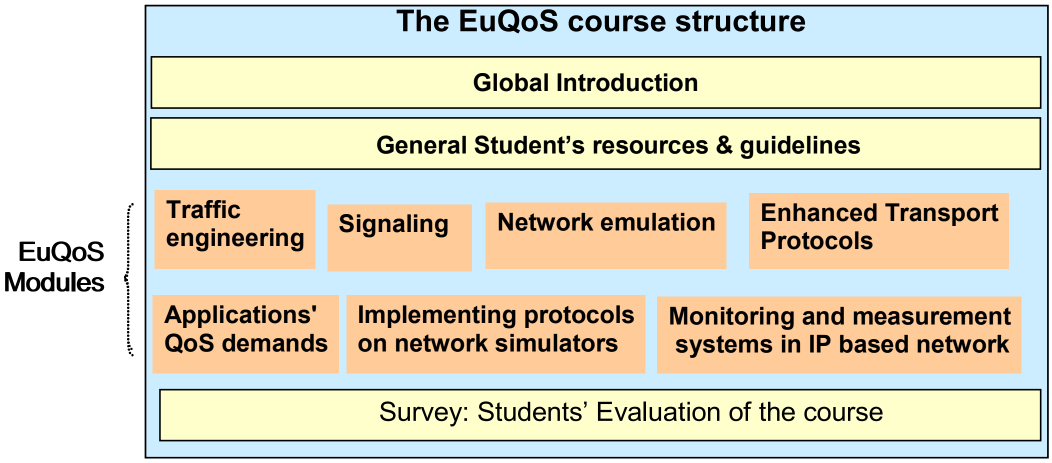

The EuQoS course structure
Global Introduction
General Student's resources & guidelines
EuQoS Modules
Traffic engineering
Signaling
Network emulation
Enhanced Transport Protocols
Applications' QoS demands
Implementing protocols on network simulators
Monitoring and measurement systems in IP based network
Survey: Students' Evaluation of the course

Figure 7: EuQoS course structure

The EuQoS course is a framework of in itself closed modules and the modules can be visited independently from each other.

All EuQoS course modules are similarly designed to allow easy navigation and orientation. Each of the learning units is sub divided in four Chapters and the modules' structure with short explanations is listed below:

- **Introduction:**
  - Welcome
  - The Goals and How to Reach Them
  - Module Vicinity
  - My Goals
  - Tips
  - FAQ

Section 1 introduces learners to the module topic with a very brief abstract and subsequently explains the goals of the module, and how to reach them. The module is placed into the course context with its many other modules. A first learner task is to formulate own learning goals for the respective module.

- **Basic Knowledge Acquisition:**
  - Theoretical Basics (supplementary content possible but marked as described above)
  - Readings
  - Personal Synthesis
  - Self Test (formative evaluation) with links to sections related to wrong answered questions
  - Quiz (success required to access laboratory)

Quiz (success required to access laboratory). The basic knowledge acquisition section is the place where students have to study theory. Students start with theory and interactive exercises. Another part of this section is scientific reading, which gives to the user an insight in the scientific notation of the module's topic. The Self Test helps to minimize the theoretical work by giving the answers immediately and additionally pointing to further readings in case of wrong answers. The Self Test is also a place to check if students have to read through the whole theory or not. In a personal synthesis students identify what is learned and can make links with the personal goals. Learners may as well use this task to build connections between the newly acquired knowledge (theory) and the previous knowledge in order to go further in the understanding of the topic. Additionally, students may organize your knowledge in concept maps to better prepare the quiz and to re-use it more easily during the following activities. This section ends with a quiz that is graded by a tutor.

– **Knowledge Application/Exploration:**

- Introduction
- Hands-on Session (Laboratory work can be simulation, emulation or real supplementary content possible but marked as described above. Automatically tracking exercise data is desired, else exercise results should be saved by learners. Possible teamwork to solve/discuss the task)

Knowledge application and exploration is the place to apply the previously acquired skills. This is the section with the hands-on session scenarios. The situations in the hands-on session can be simulated, emulated or real. This is also the section where students can work in a team during the hands-on session. It is not forbidden to discuss the understanding of the results/explorations with other learners. Finally students use the same results for your individual interpretation in the final quiz.

All EuQoS course modules have the same structure, although it is possible to split up the hands-on session and thus to repeat step b several times.

- **Evaluation of Acquired Knowledge and Skills:**
  - Personal synthesis
  - Final Quiz
  - Survey

A first task is to write another synthesis about the whole module topic and express in their own words what they have learned by using the personal notes. This helps learner to prepare the final quiz. This section ends with a final quiz that lets the tutors see if you have met the goals listed in the introduction section of the module.

4.2 EuQoS Course Didactic and Design Program

EuQoS is designed for persons that have already acquired a two year's knowledge in computer sciences or similar branches, engineers or persons who need a theoretical background in QoS but have a base knowledge in Internet technologies. This already existing knowledge provides the foundations for understanding each module's new lecture material. It also helps learners to develop the autonomy and initiative required by e-learning, more specifically during the exploration of the laboratory activities. Autonomy and initiative development is supported by providing guidelines and reflexive activities.

The EuQoS e-learning course framework is an extension to traditional teaching activities in universities and industrial further education. EuQoS course modules should help learners to go beyond traditional expository teaching. After the mastering of the basic knowledge, learners are asked to effectively analyze and solve problems from real existing situations. All those situations are taken out of the life of telecommunications and Internet experts. These hands-on sessions allow learners to apply their theoretical knowledge in a trial-and-error process. Hence, by learning in simulated, emulated and real network environments, learners can develop skills for self-directed problem-based learning which will help them throughout their life. To do so, each module includes at least one hands-on session scenario. The content of the modules, from the introduction to the tests is designed to fully integrate the hands-on session.

EuQoS' modules combine the delivery of basic knowledge and the exploration of real tasks in order to develop effective know-how. In addition, reflective processes, which permit to make sense of exploration and problem solving, are supported by note taking in a personal logbook throughout the modules' activities.

We have designed a generic didactical framework, which enables EuQoS course providers to increase the quality of e-learning courses compared to traditional courses described. In contrast to traditional laboratories, the audience of the EuQoS e-learning computer networks laboratories is global as learners can theoretically attend the laboratory wherever Internet access is possible.

We assumed that the didactics concept of this e-learning course must cover the education of computer science learners with finished basic studies, learners from related curricula and engineers.

The course structure developed reflects the intention to provide a common design to the e-learning course.

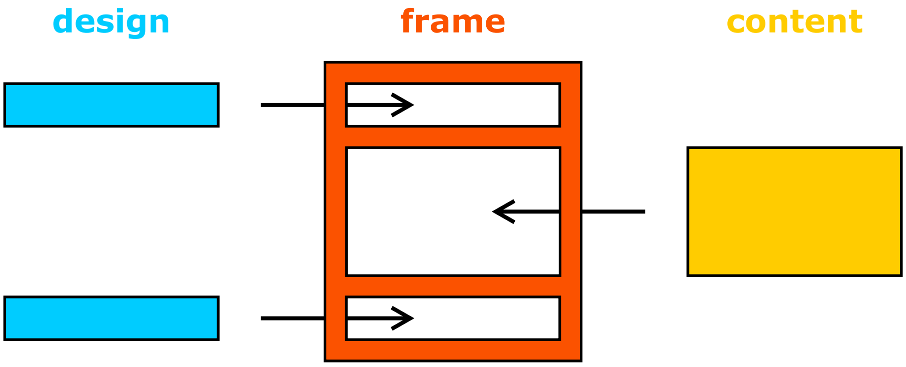


Figure 8: Page Style

Without a common design, learners loose too much energy with exploring each learning module's structure. Designers must avoid unnecessary repetitions; else, learners do not read the texts and skip important information. This has led to a course design with a common introduction chapter for all modules and an identical structure for each of the modules. The developed course structure with the didactic framework has found its way into a didactics and design guide for hands-on trainings oriented e-learning courses.

The common introduction chapter discusses the background and questions regarding the entire course. The following figure number 9 shows a house that represents the e-learning course under whose roof single modules are stacked. The base of the house is the common introduction.

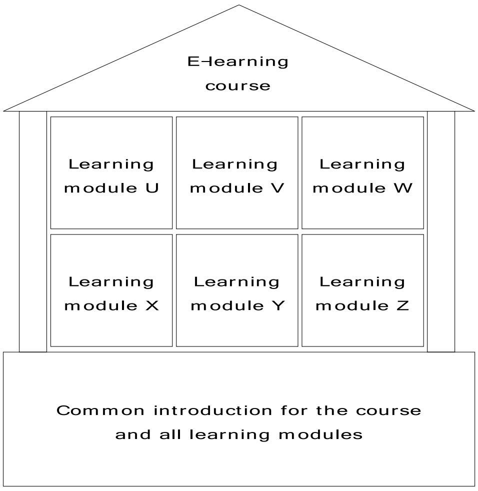


Figure 9: EuQoS E-Learning Course

In the first part, the common introduction explains the course's global objectives, the didactic approach, and the course structure for learners and tutors. The second part introduces studying online for beginners; explains the course management system with the laboratory reservation system (without technical details), indicates external resources useful for the whole course, explains the evaluation procedure, introduces discussion boards, explains the help system and the surveys. All this information is part of the didactic framework in which we intend to inform and prepare learners as well as tutors to the single learning modules.

The new didactic framework for hands-on training oriented e-learning courses comprises several well-known didactic methods, with a special emphasis on the knowledge association on Meta layers. Knowledge that has been memorized but not associated resides on Meta layers. The composition of these methods in a hands-on training oriented e-learning laboratory is new. We discuss the single didactics elements and their functions in detail:

Logbook

The logbook's task is to replace the real logbook that exists in traditional laboratories. The logbook is something like a notepad and used in traditional laboratories. Learners make all personal notes, calculations, remarks, and draws into the logbook. In this way, the logbook documents the personal learning procedure of each learner. In case of problems, tutors and learners can go through the logbook to search for the reasons of those problems.

Learning Goals

The learning goals' task is to define the learning activity and the goals to reach at the end of each learning module.

Learners need to have easy understandable but as well clear formulated learning goals. Without learning goals, learners do not know what exactly they have to learn and memorize for later. Learning goals also contain the evaluation procedures and the expected quality of the results.

Own Learning Goals

The own learning goals' task is to activate existing knowledge prior to start with the main knowledge acquisition section.

In this didactic framework, learners have only read the learning module's abstract and the learning goals when they have to write down their own learning goals. With this task, learners reactivate and remember already existing knowledge and re-associate it with the information they have about the module. Writing down the own goals helps memorizing the new associations and prepares the start in the knowledge acquisition section. At the end of a module, learners can verify if the have learned what they have expected before. For tutors these self-formulated learning goals show what learners expect from the module topic.

Module Vicinity

Module vicinity’s task is to locate a learning module in the context of the other learning modules.

The e-learning course lists its single modules in a certain order on an overview page but without numbering the modules. Each of the modules is a in itself closed learning unit that can be used inside or outside of the entire course. To provide an order for learners that work through the whole course, we introduce a vicinity map. This map shows the recommended modules sequence for learners who want to work through the complete course. An icon represents each learning module and the icon of the module in which the learner is located at the time colorized.

Mindmap

The Mindmap’s task is to initiate learners for a self-association of existing knowledge. In Mindmaps, learners find the module topic in the centre and from there leave branches with theory (green) and practical (red) topics. Neighboring modules are depicted in yellow balloons to show the close relation to the module topic in the centre of the Mindmap. Learners are animated to draw own Mindmaps or to further develop the proposed map. By adding and labeling own branches, learners draw in a way they think, i.e. they write down how their knowledge is associated in their mind. By watching their own associations they can create new associations. Mindmaps help to recall knowledge within a short time, for example before an exam, because they reflect their designer’s knowledge.

Scientific Readings

The scientific readings task is to introduce learners in scientific writing.

Scientific readings are a didactic method used to accustom learners to the way scientists communicate their results. With the integration of such readings in each module, a part of each module’s knowledge acquisition section is imparted in that way and the understanding evaluated in the quizzes. Besides the required readings, there are also recommended readings, representing a collection of text references, and base as well as higher-level readings to the module’s topic.

Personal Synthesis

The personal synthesis' task is to associate knowledge recently studied in the knowledge acquisition section.

The personal synthesis is a didactic method, which helps to recall the already known but not present knowledge and to associate it with recently learned knowledge. Learners associate their knowledge by writing an essay about a self-chosen topic of the theory section. During the composition of such an essay in their own words, they pass the whole knowledge acquisition section again and can thereby discover unresolved problems as well as draw new conclusions.

Self-Test

The self-test's task is to provide learners with the possibility of a self-evaluation.

Self-tests help learners measuring their knowledge and discovering missing parts. Skilled learners can bypass theory by solving self-tests questions correctly. The self-test immediately provides results and in case of wrong results points to a resource where the missing information can be read. Providing a positive feedback even in case of a correct answer helps learners to return to a certain source text in case of doubts. Self-tests are not graded nor reviewed by a tutor; they are a pure self-evaluation tool.

Quizzes

The quizzes' task is to evaluate learners' work.

With quizzes, we analyze what learners really have understood of the lecture. A tutor grades quizzes. Quizzes consist of multiple choice and essay questions.

Discussion Board

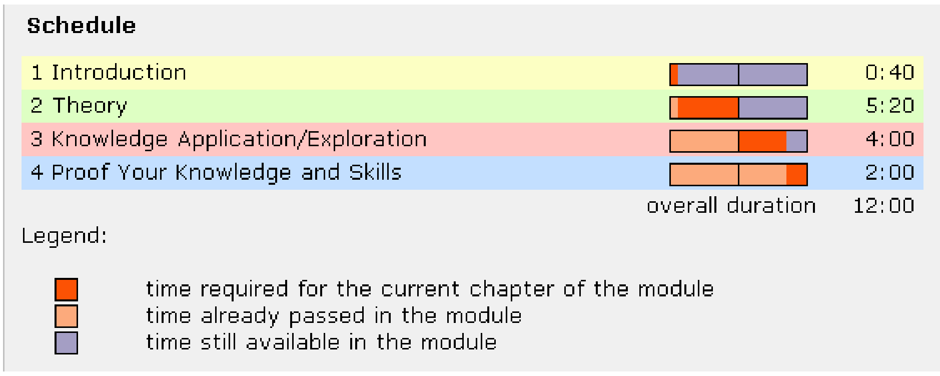
The discussion board's task is to provide a communication platform.

In the discussion board, learners communicate with learners or tutors. A tutor moderates the discussion board, solves open issues, and keeps discussions in the area of the module's topic. The board gives eager learners a chance to help others and they can thus deepen their own knowledge.

Schedule

The schedule's task is to provide fast information about the learning progress.

Figure 10 shows the developed schedule. The schedule replaces the missing orientation learners normally have when reading a book. It helps learners to see where they stay and how much time they still have to invest. The schedule is static and provides the expected duration in each of the module's sections. Learners that are more skilled progress faster, less skilled learners who read additional information slower. It helps learners also to remain on track and not to loose themselves in additional readings.



Schedule

1 Introduction	0:40
2 Theory	5:20
3 Knowledge Application/Exploration	4:00
4 Proof Your Knowledge and Skills	2:00
overall duration	12:00

Legend:

🟥	time required for the current chapter of the module
🟧	time already passed in the module
🟪	time still available in the module

Figure 10: Where to spend how much time.

Help System

The help systems task is to provide a solution to every problem.

We designed the help system to offer around the clock fast help in case of problems. The help system consists of several parts put together in a certain order. The first place to look for help is in frequently asked questions section. The second location to address to in case of problems is the discussion board. It is likely that learners find an answer to their question or get one within a short time. Browsing in already solved problems can give hints for the own problem. Tutors should extract important questions after each course cycle and summarize in the frequently asked questions section. If the discussion board does not cover the problem, learners can send an Email to the module tutor. As a last solution, learners can call a hotline number. Only by this filtering method, the hotline can be operated without having learners calling all the time. Our help system can be represented as a help pyramid, shown in Figure 11.

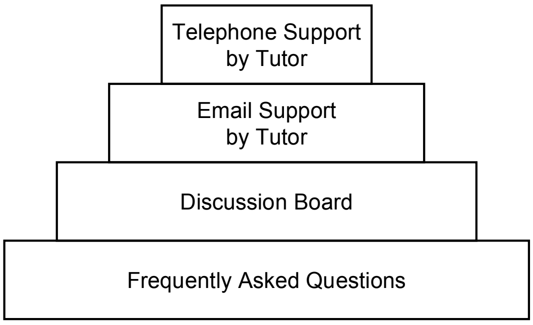


Figure 11: The help pyramid.

Interactive Animations

The interactive animation's task is to present theory in multiple dimensions.

Not all learners learn the same way. Some learners fully understand theory imparted as plain text, others need additional figures and some animations. Each supplementary dimension added to plain text activates a further brain region. Thus by adding interactive animations, multiple brain regions are activated to solve a problem.

Notes Tool

The notes tool's task is to enable learners to write directly into the text.

The notes tool should enable learner to write their text specific notes directly into the text. This is necessary to allow learners to use their traditional learning style.

The framework of the above-discussed methods contains text readings, references to recommended readings, self-test, self-evaluation, quiz, trial-and-error learning, and learning by doing, guided practical working, and discussions on discussion boards, reflections, mind map, logbook, video sequences, interactive animations, and schedule.

4.3 Course System Overall Architecture

Fig 1 shows the extended architecture with the components and their possible connections between each other. Connections between servers use Stunnel technology whereas connections between servers and end users TLS/SSL. We discuss the possible connections between the components in detail below.

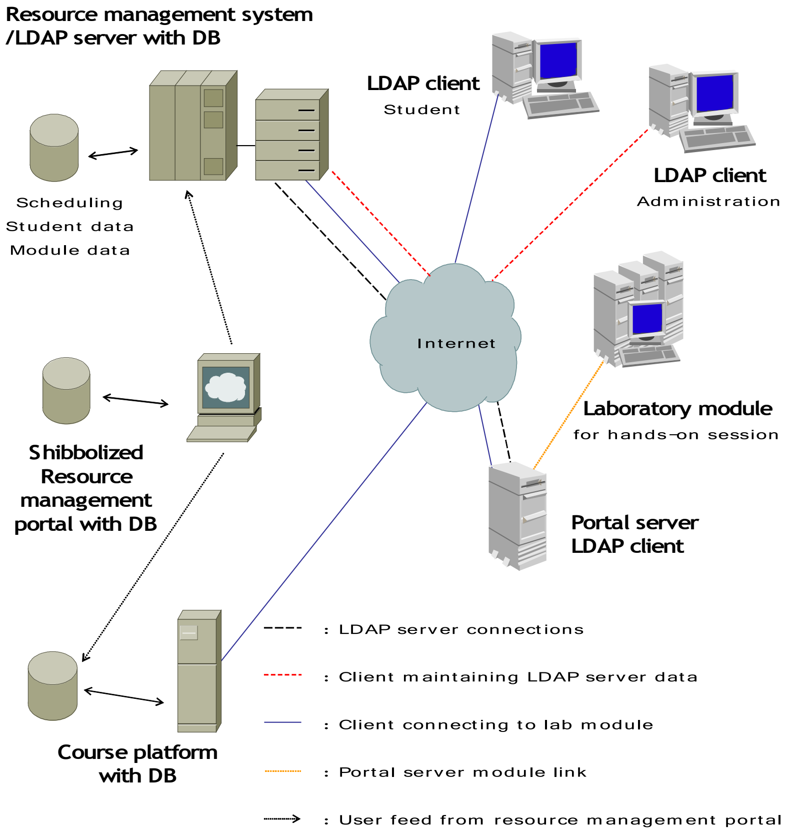

Resource management system /LDAP server with DB
Scheduling
Student data
Module data
LDAP client
Student
LDAP client
Administration
Internet
Laboratory module
for hands-on session
Shibbolized Resource management portal with DB
Portal server
LDAP client
Course platform with DB
: LDAP server connections
: Client maintaining LDAP server data
: Client connecting to lab module
: Portal server module link
: User feed from resource management portal

Figure 12: Multifunctional e-learning architecture

The components and their functionality:

- **Public key infrastructure**

  The higher-level certificate authority of the single or the sub certificate authority of the hierarchical public key infrastructure issues signed certificates, installed on the Shibboleth-enabled servers, such as the resource management portal, the LDAP server, and the portal servers. We recommend using the same public key infrastructure as the authentication and authorization infrastructure uses, also for server to server and server to client connections.

- **Higher-level user management system**

  The higher-level user management system writes user accounts into the LDAP directory of the resource management system. These updates occur automatically. This is a one-way connection from the higher-level user management system to the resource management system. The higher-level user management system in the extended architecture is the resource management portal. It is possible to use more than one higher-level user management system at once, i.e. more than one resource management portal.

- **Resource management portal**

  The resource management portal is the entry point for learners accessing the computer networks laboratory connected to the extended multifunctional e-learning architecture. All accesses to the course platform work only over the resource management portal, laboratory portals and the reservation system could theoretically be accessed directly if the URL are known.

  - **Client (Learner)**

- Learners connect to the resource management system if they want to book or change a booking of a laboratory training. Learners also connect to the laboratory portal servers and to the hands-on trainings behind the portals. The third server where learners connect is the course platform.

- **LDAP client (Administration)**

  An administrator connects to the resource system to administrate the user database or the module database. The administrator may connect to the central resource management systems' directory or to a referred directory if this exists.

- **Laboratory portal**

  The laboratory portal server connects to the LDAP server of the resource management system to authorize users by reading out the current user of the hosted laboratory. Only learners who have booked a timeslots for the respective laboratory module get the authorization to access the hands-on training.

- **LDAP server**

  The LDAP server of the resource management system now stores the users as unique AAI identity @ home organization in the database, used for the laboratory module reservations.

- **Course platform**

  If the course platform could access LDAP directories there would be an additional connection to the resource management system. The commercial course platform our institution operates was not able to use such a directory and works with a proprietary database. The resource management portal was connected to the course platform and automatically opens and maintains user accounts on the course platform.

4.4 Internet Remote Network Simulation Infrastructure (IRNSI)

The Internet Remote Network Simulation Infrastructure (IRNSI) provides a remotely accessible laboratory for network simulation. It offers an easy way to include practical exercises based on network simulations in e-learning courses.

The remote laboratory is fully accessible through the web by the means of a browser with support of Java applets.

Its integration in the authentication and authorization infrastructure AAI supports a single sign-on for your course including this laboratory.

General structure:

IRNSI consists of three parts: the reservation system, the laboratory portal and the labbed server.

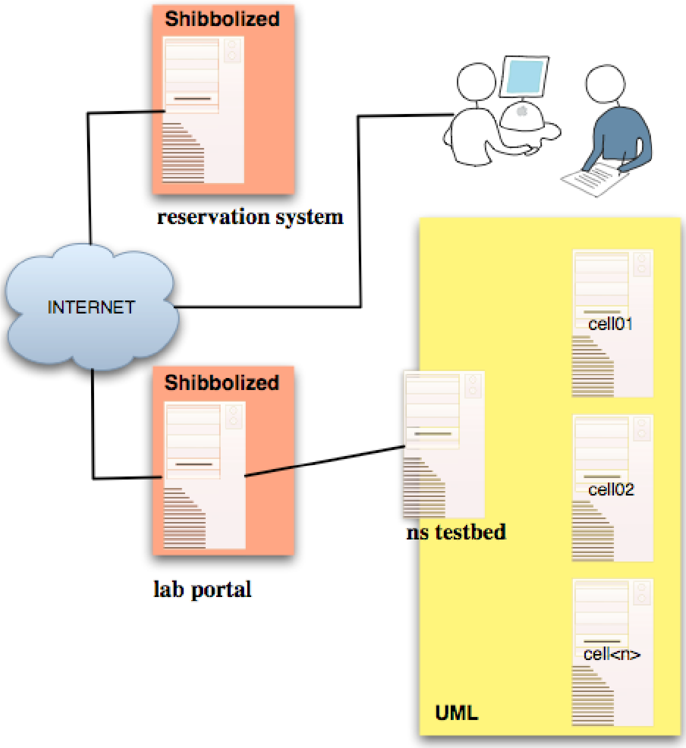


Figure 13: Lab architecture.

The learners get exclusive access to one instance of a hands-on session, which requires a reservation mechanism. The learner makes a reservation for a specific module in a time-slot and after that can work during the slot on the reserved instance.

The laboratory portal manages the access to the labbed. It checks the user's authentication and authorization with the AAI and if the user has a reservation for the current time-slot. The laboratory portal web interface offers the user the possibility to reset his session. Additionally, the user can continue with the state of the system as he has left it in his last time-slot when he starts a new time-slot.

On the testbed server, we use virtualization (user mode Linux, UML) to provide multiple instances of the same module that are completely separated. For every instance the user gets a sand-boxed virtual server. The testbed sets up the virtual server according to a standard image at the beginning of each slot. This process assures that each learner gets a blank and clean module instance at the beginning of his hands-on session. Optionally, the changes of the user are stored and can be used to set up his next slot. Stored changes are wiped periodically (1 month).

Communication to the Test bed

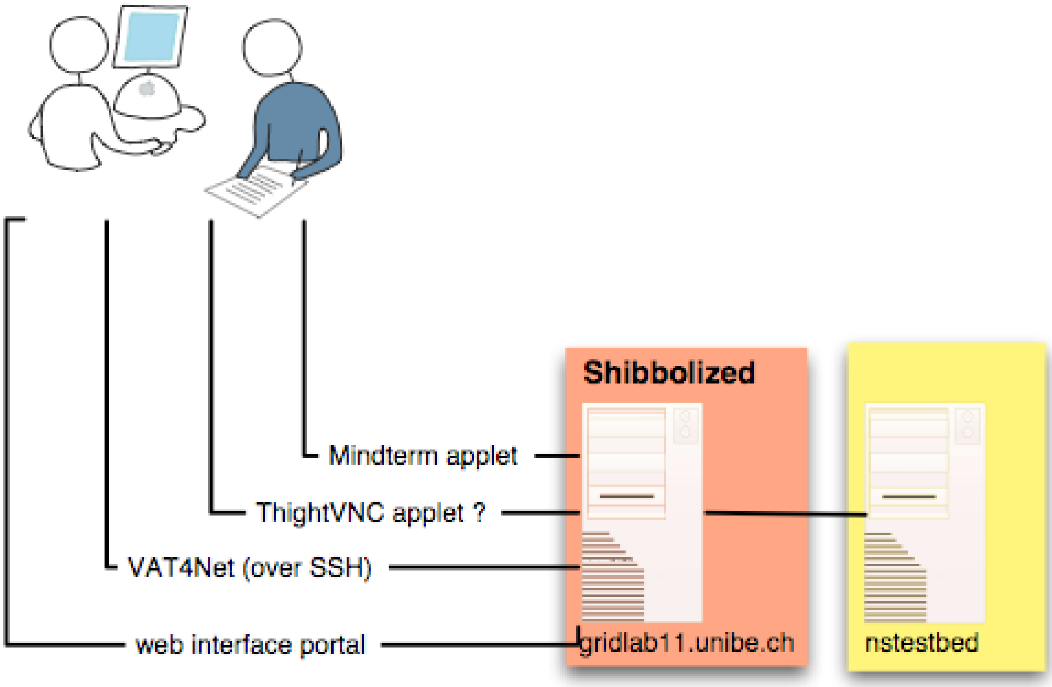


Figure 14: Lab bed connections

IRNSI offers the user different communication means. At the moment, the following communication options are available: terminal connection with java ssh applet (Mindterm), xserver connection with java applet (ThightVNC), visualization and animation of the results with VAT4Net, general options via web interface.

5 Traffic Engineering Module Description

5.1 Abstract

This module deals mainly with traffic engineering; i.e. the task of mapping traffic flow onto an existing physical topology following certain politics, different from ordinary shortest path first rule, so that the resulting traffic patterns achieve a balanced utilization of network resources.

MPLS and Constraint Based Routing can be used to achieve the benefits of traffic engineering. This because MPLS & CBR provide the ability to specify the explicit route that data packets should use to traverse the network, according to certain performance and administrative constraint. Moreover this solution overcome drawbacks of previous technology like “Overlay” solution.

Thus, in addition to the traffic engineering concepts, the module treats the description of the MPLS technology. After a brief introduction to show the problems that it addresses and compare it with other solution the architectural issues and the details of the MPLS protocols are described. The second part of the module theory explain the path calculation algorithm used by CBR and the resource reservation protocols used.

Finally, learners get the possibility to apply their knowledge in traffic engineering and MPLS in a hands-on session. In this way, the theory can be applied in real life scenarios.

5.2 Full Description

Goals:

Upon completing this course, the learner should be able to:

- Describe the need for TE
- Describe the drawbacks of the solutions to TE before MPLS
- Justify the reasons which led to the choice of the MPLS architecture to solve the TE problem
- Describe the procedure for packets forwarding in a MPLS domain
- Describe how MPLS protocol determine the path
- Understand and apply Aggregation and other optimization in certain scenario
- Understand and apply the CSPF algorithm to concrete network scenarios
- calculate LSP subject to constraints posed by TE
- decide where to apply fast rerouting in a concrete network configuration

5.3 Theory

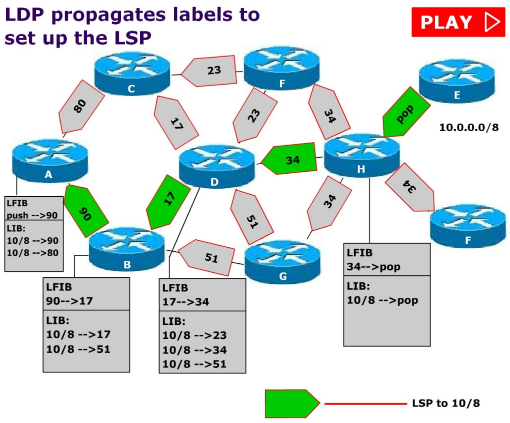
Chapter 1: Traffic Engineering.

This part is a brief introduction to the concept and history of traffic engineering and show some traffic-engineering application in the ISPs. The aim of these examples is to show that any solution to the traffic engineering problem has to establish routes that are not just optimal with respect to a certain scalar metric (e.g., administrative distance), but that also take into account the available bandwidth on individual links. Following this, we look at one specific solution to the traffic-engineering problem, called the “overlay” solution, according to which a service provider relies on the routing capabilities of a virtual-circuit-based network to construct routes that avoid the over utilization/underutilization problem. Problems related to this approach are highlighted. In an attempt to eliminate these problems, we try to solve the problem of traffic engineering by using the capabilities provided by plain IP routing. Again, we show that this solution is not viable since plain IP routing provides routes that do not take into consideration the available bandwidth on individual links.

Finally the current solution to the traffic-engineering problem based on MPLS and Constrained-Based Routing is introduced. Specifically, after a description of MPLS protocol, we show how the TE problem can be broken down into the following parts:

- Information distribution – How routers know what the network looks like and what resources are available.
- Path calculation and setup – How routers decide to build TE tunnels, and how these TE tunnels are actually built and maintained.

Resource reservation- How router reserve resources to meet the QoS requirements



LDP propagates labels to set up the LSP

LFIB
push -->90
LIB:
10/8 -->90
10/8 -->80

LFIB
90-->17
LIB:
10/8 -->17
10/8 -->51

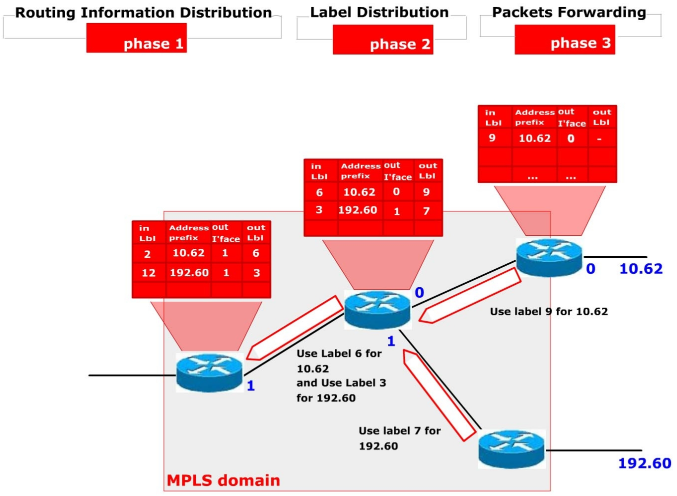
LFIB
17-->34
LIB:
10/8 -->23
10/8 -->34
10/8 -->51

LFIB
34-->pop
LIB:
10/8 -->pop

Figure 15: Label propagation examples

Chapter 2: MPLS.

This part deals with the fundamental concepts of label switching as implemented by the MPLS routing architecture. We begin with a description of the functional decomposition of network layer routing into control and forwarding components. In this manner, at first we examine label format and how packets are routed in a MPLS domain; then how labels are assigned, distributed and how path is set up. We present with some examples the type of data structures that are needed in a router to support label switching and finally two MPLS optimization are presented: Aggregation and Penultimate Hop Popping.



in Lbl	Address prefix	out I'face	out Lbl
2	10.62	1	6
12	192.60	1	3

in Lbl	Address prefix	out I'face	out Lbl
6	10.62	0	9
3	192.60	1	7

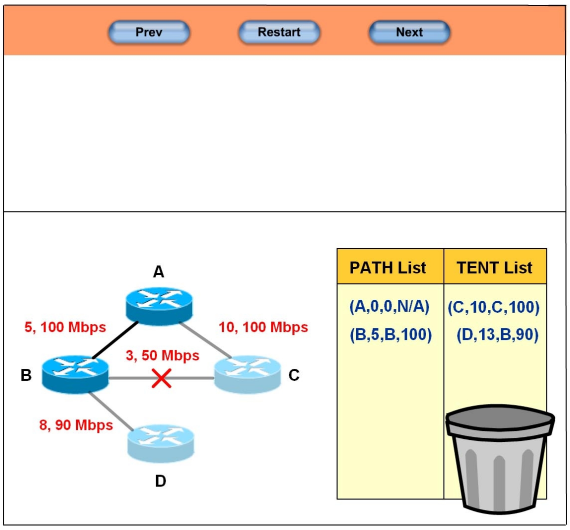
in Lbl	Address prefix	out I'face	out Lbl
9	10.62	0	-
	...	...	

Figure 16: Router Data Structure Update Example

Chapter 3: Path Calculation.

This part is devoted to the description of path calculation and setup. Specifically, the path calculation can be broken down into two pieces:

- the basic Shortest Path First (SPF) calculation that OSPF uses to build the routing table in an IP network;
    - the Constrained SPF (CSPF) used in a Traffic Engineering Tunnel and how it differs from the traditional SPF performed by IP routing protocols.



PATH List	TENT List
(A,0,0,N/A)	(C,10,C,100)
(B,5,B,100)	(D,13,B,90)

Figure 17: Path Calculation with CSPF Example

Chapter 4:Explicit Route.

After that path is computed with CSPF, we examine how to establish the forwarding state along the path, as well as how reserve resources along the path; two possible protocols (extended RSVP and CR-LDP) are illustrated and compared.

Chapter 5:OSPF Extension.

The OSPF flooding mechanisms could be used to distribute information to provide each node in a network with the link attributes.

Chapter 6:Fast Rerouting.

Finally, it is shown how the application of Fast Rerouting mitigates problems related to link failure in a MPLS domain.

Chapter 7:MPLS - Traffic Engineering Application.

The last chapter is devoted to showing examples of MPLS – Traffic Engineering Application.

5.4 Hands-On

In the hands-on session learners have access to a remote laboratory based on the NS2 simulation environment, test real-time experiments and have a graphical result of the trace file through the Internet Remote Network Simulation Infrastructure (IRNSI) described in the next paragraphs.

A simulated ISP network with border routers and internal routers is provided to users. Simulations can be ran with two scenarios: one without enabling MPLS and one with enabling MPLS.

Learners could configure the given scenario choosing certain parameters like the number of flows, the rate of each flow, flow destination, and, optionally, the explicit route, and then generate the simulation script through the GUI. Analyzing the results, users could compare performance in the two different scenarios.

The architecture and the operation of this laboratory architecture is detailed described in chapter 6.

6 Authentication Architecture

6.1 Shibboleth

The Shibboleth system offers a powerful, scalable, and easy-to-use solution when you want to share secured online services or access restricted digital content.

Shibboleth is standards-based, open source middle ware software which provides Web Single SignOn (SSO) across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner. The Shibboleth software implements the OASIS SAML v1.1 specification, providing a federated Single-SignOn and attribute exchange framework. Shibboleth also provides extended privacy functionality allowing the browser user and their home site to control the Attribute information being released to each Service Provider. Using Shibboleth-enabled access simplifies management of identity and access permissions for both Identity and Service Providers.

The Shibboleth system provides a standards-based link between existing authentication systems and resource providers of all kinds. For example, when a student requests access to a protected video clip, her home organization (origin site) requests her to authenticate (if she has not done so already) and then passes on the information that she is enrolled in Biology 562 to the site housing the video. The provider (target site) uses the fact that she is enrolled in this course to determine her eligibility to access the video.

Shibboleth is a system designed to exchange attributes across realms for the primary purpose of authorization. It provides a secure framework for one organization to transmit attributes about a web-browsing individual across security domains to another institution. In the primary usage case, when a user attempts to access a resource at a remote domain, the user's own home security domain can send certain information about that user to the SP site in a trusted exchange. These attributes can then be used by the resource to help determine whether to grant the user access to the resource. The user may have the ability to decide whether to release specific attributes to certain sites by specifying personal Attribute Release Policies (ARP's), effectively preserving privacy while still granting access based on trusted information.

When a user first tries to access a resource protected by Shibboleth, they are redirected to a service which asks the user to specify the organization from which they want to authenticate. If the user has not yet locally authenticated to a WebISO service, the user will then be redirected to their home institution's authentication system. After the user authenticates, the Shibboleth components at the local institution will generate a temporary reference to the user, known as a handle, for the individual and send this to the SP site. The SP site can then use the handle to ask for attributes about this individual. Based on these attributes, the SP can decide whether or not to grant access to the resource. The user may then be allowed to access the requested materials.

There are several controls on privacy in Shibboleth, and mechanisms are provided to allow users to determine exactly which information about them is released. A user's actual identity isn't necessary for many access control decisions, so privacy often is needlessly compromised. Instead, the resource often utilizes other attributes such as faculty member or member of a certain class. While these are commonly determined using the identity of the user, Shibboleth provides a way to mutually refer to the same principal without revealing that principal's identity. Because the user is initially known to the SP site only by a randomly generated temporary handle, if sufficient, the SP site might know no more about the user than that the user is a member of the IdP organization. This handle should never be used to decide whether or not to grant access, and is intended only as a temporary reference for requesting attributes.

6.1.1 Shibboleth Architecture

1.a. Identity Provider (IdP):

There are four primary components to the IdP component in Shibboleth: the Attribute Authority (AA), the Handle Service (HS), the directory service, and the local sign-on system (SSO). From the IdP site's point of view, the first contact will be the redirection of a user to the handle service, which will then consult the SSO system to determine whether the user has already been authenticated. If not, then the browser user will be asked to authenticate, and then sent back to the SP URL with a handle bundled in an attribute assertion. Next, a request from the Service Provider's Attribute Requester (AR) will arrive at the AA which will include the previously mentioned handle. The AA then consults the ARP's for the directory entry corresponding to the handle, queries the directory for these attributes, and releases to the AR all attributes the requesting application is entitled to know about that user.

1.b. Service Provider (SP):

There are three primary components to the SP component in Shibboleth: the Assertion Consumer Service (ACS), the Attribute Requester (AR), and the resource manager (RM).

From the SP's point of view, a browser will hit the RM with a request for a Shibboleth-protected resource. The RM then allows the ACS to step in, which will use the WAYF to acquire the name of a handle service to ask about the user. The handle service (HS) will then reply with a SAML authentication assertion containing a handle, which the ACS then hands off to the AR. The AR uses the handle and the supplied address of the corresponding attribute authority (AA) to request all attributes it is allowed to know about the handle. The AR performs some basic validation and analysis based on attribute acceptance policies (AAP's). These attributes are then handed off to the RM, which is responsible for using these attributes to decide whether to grant access.

1.c. Where are you from? (WAYF):

> It is responsible for allowing a user to associate them self with an institution of their specification, then redirecting the user to the known address for the handle service of that institution.

1.d. Federations:

When a number of organizations join together to use Shibboleth software to share access to resources in a common way, this is called a Federation. The Shibboleth system supports federations by providing scalable methods to manage and distribute configuration and security information among a large number of organizations, and a common vocabulary for user attributes.

Joining a federation is not explicitly necessary for operation of Shibboleth, but it dramatically expands the number of SPs and IdPs that can interact without defining bilateral agreements between all these parties.

A federation can be created in a variety of formats and trust models, but must provide a certain set of services to federation members. It needs to supply a registry to process applications to the federation and distribute membership information to the IdP and SP sites. This must include distribution of the PKI components necessary for trust between IdP's and SPs. There also needs to be a set of agreements and best practices defined by the federation governing the exchange, use, and population of attributes before and after transit. Also, there should be a way to find information on local authentication and authorization practices for federation members.

1.e. Relying Parties:

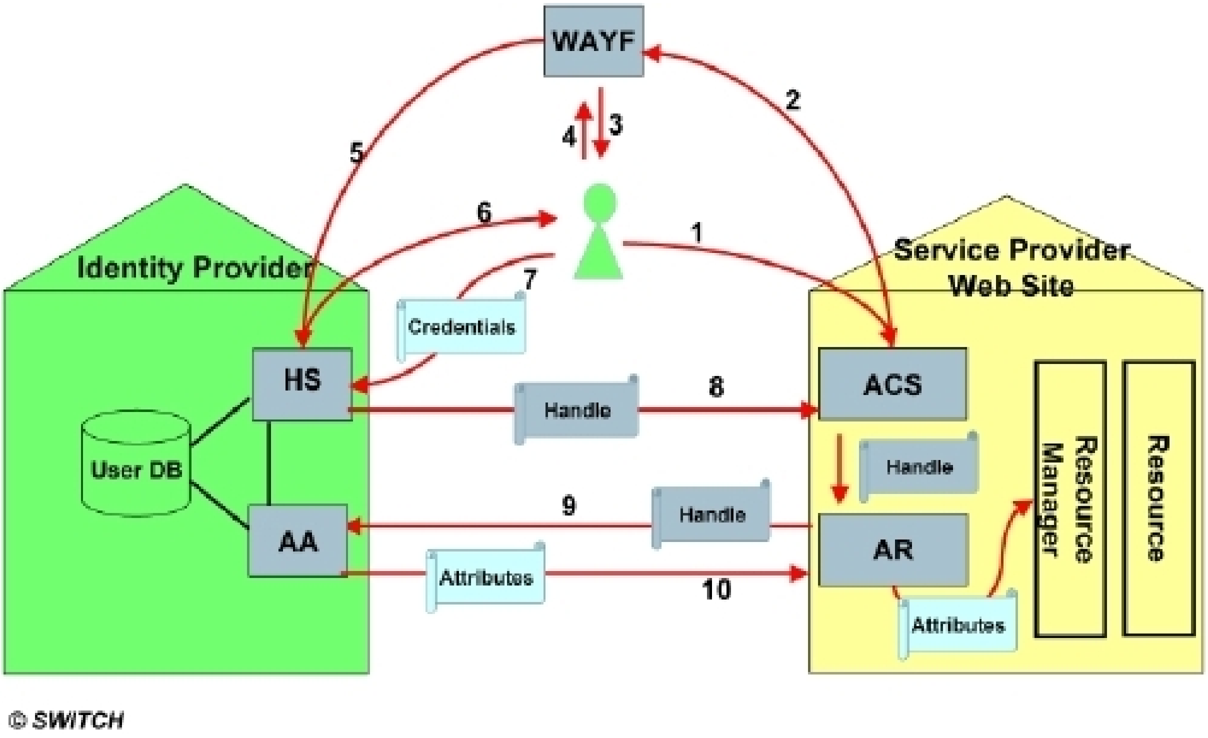
Certificates, policies, and other aspects of an interaction are specified on the basis of the relying party, and may or may not vary between relying parties depending on the deployment's needs. Each IdP and application at the SP site is assigned a URI, a unique identifier to enable control over configuration down to the level of an individual partner (a single relying party). By convention, this is termed a "providerId". More frequently, an entire federation will be viewed by an IdP or SP as a single relying party to simplify management. An individual IdP or SP with which this deployment exchanges information may sometimes be part of multiple relying parties if there are multiple trust agreements under which these transactions are performed. Care should be taken to avoid conflicting or inconsistent configuration in such cases.

1.f. Applications:

Applications as viewed by the SP implementation are not necessarily defined by the same metrics as in other contexts. An individual application represents a set of web resources that operates using the same attribute handling and trust configuration and shares a common session with the browser user.

1.g. Sessions

Much of the SP implementation is concerned with establishing, and subsequently maintaining, sessions with the browser user on behalf of the applications at the SP. A session consists of a cookie passed between the browser and web server, associated with a security context. The context contains the user's authentication information, and generally a set of attributes that make up the user's identity.



1. User attempts to access Shibboleth-protected resource on SP site application server.

2, 3, 4. User is redirected to a Where Are You From (WAYF) server, where the user indicates their home site (IdP).

5. User is redirected to the Handle Service at their IdP.

6, 7 User authenticates at their IdP, using local credentials.

8. Handle service generates unique ID (Handle) and redirects user to Service Provider site's Assertion Consumer Service (ACS). ACS validates the supplied assertion, creates a session, and transfers to Attribute Requester (AR).

9, 10. AR uses the Handle to request attributes from the IdP site's Attribute Authority. The attribute authority responds with an attribute assertion subject to attribute release policies; SP site uses attributes for access control and other application-level decisions.

6.1.2 Key Benefits Of Shibboleth

- Reduces time needed to manage access to protected resources. (Sharing class resources among several institutions and managing several hundred accounts...
- Increases security (Single SignOn - SSO - remembering multiple passwords, acquiring information about the users from reliable providers, etc.)
- Interoperates with similar standards-based solutions (it is based on SAML and thus interoperates with other software based on SAML...)

Shibboleth offers a compelling alternative for providers of services and content to higher ed, by eliminating the need to build extensive custom front-ends and interfaces to deal with the variety of systems customer sites use for controlling access to resources and services

Issue	**Without Shibboleth**	**With Shibboleth**
End User Authentication	Most content and service providers, if they want to offer services to end users on campuses, generally have had only two options: 1. provide and manage individual accounts for each user, with the high level of support and insecurity this entails. 2. integrate with each	Unified authentication mechanism from the vendor perspective, much more scalable, and much less integration work required to bring a new customer online.

	customer campus SSO.	
Access Control	Fine-grained access control impractical, usually defaults to access decisions based on IP address (or range of addresses), possibly combined with time of day.	Ability to implement fine-grained access control (e.g. access by role), allowing customer sites to effectively control access by attributes and thus control usage costs, by not granting access unnecessarily – compelling marketing message for vendor.
Competitive Advantage: Leading Edge		Ability to market yourself as being at the forefront of compelling new technology adoption. E.g., as Shibboleth enables role based access control (RBAC); vendors are able to offer new service offerings.
ROI - Vendor	Variable and potentially significant costs associated with bringing new customer sites online.	Once the initial Shibboleth integration work has been completed on the vendor’s systems, the incremental cost of adding new customers is relatively minimal, in contrast.
ROI - Customer		Many campuses are already implementing Shibboleth as core infrastructure, to

		support inter-institutional applications, thus they would be leveraging something already in place. If your customers have Shibboleth implemented, it is a matter of managing attributes. For those who have not yet implemented Shibboleth, the installation is relatively easy.
Competitive Advantage: Joint Procurement (e.g. statewide university systems)	Less feasible to offer joint procurement service opportunities in some cases.	Opportunity to offer joint procurement services through federation membership, providing economies of scale for both vendor and customer.

6.2 AAI – SWITCH

6.2.1 Overview

To manage the users access and authentication to the resources, the EuQoS e-learning course adopted the Shibboleth architecture and is part of the SWITCH federation (The Swiss Education & Research Network).
Based on the Shibboleth system, SWITCH has developed the Authentication and Authorization Infrastructure (AAI).
The objective of the AAI is, in a nutshell, to simplify inter-organizational authentication, authorization, and access to web resources and with a single login a student can access e-learning systems at multiple universities. The AAI makes use of a concept called Federated Identity Management.

Without an AAI, a user registers with each Resource he/she would like to access and usually will receive a new username and password pair for each Resource, so-called credentials. The problems are obvious:

- Users have to deal with too many username and passwords, typically one pair for each Resource.
- Each Resource administrator has to register the users on his/her own.

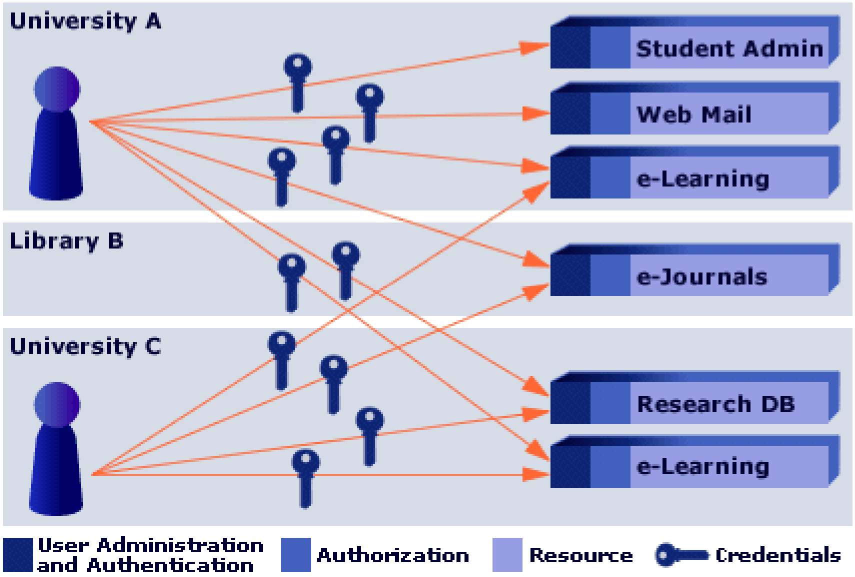


Figure 18: Authentication Without AAI

The AAI simplifies the processes for all parties involved using the concept of federated identity management:

- A user registers only once - namely with his/her so-called home organization to which the user is affiliated.

  This Home Organization is responsible for maintaining the user related information and provides the user with the credentials. Home Organizations can be institutions like universities, libraries, and university hospitals etc.
- **Authentication** is always carried out by the user's Home Organization, which can also provide additional information about the user to the Resource upon Resource's request and user's consent.

  Like this, all AAI-enabled Resources are available to a user with a single set of credentials. At the same time, there is no need for Resource operators to register new users, because they get the required information directly from the user's

Home Organization.

- An access control decision is made by the Resource based on the retrieved information about the user.

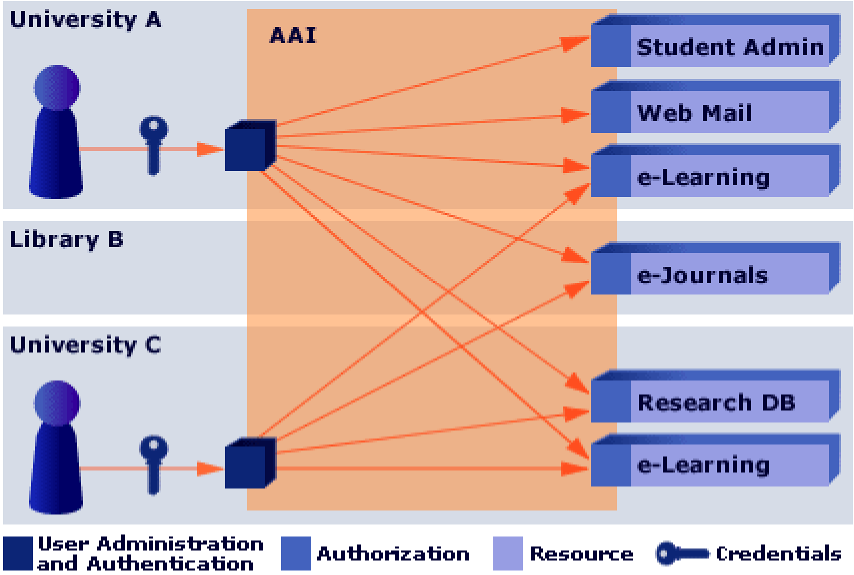


Figure 19: Authentication With AAI

Thus federated identity management is based on the concept that Resources rely on user authentication at the user's Home Organization and they obtain from there some information about the user for its authorization decisions.

SWITCHaai uses this federated approach to guarantee that each party remains in control of the steps relevant to it:

- Home Organizations register and authenticate their members
- Resource administrators define their access rules

SWITCH, on the other hand, operates the central AAI components and supports both Home Organizations and Resources.

6.2.2 AAI Model

The core functionality of an AAI is to tightly couple together the three basic interactions between a user, his or her home organization and a resource during the authentication and authorization process. These three basic interactions are:

- 1. user authentication, which is always carried out by the user's Home Organization;
- 2. access request; and
- 3. delivery of authorization attributes from the Home Organization to the resource. The set of authorization attributes which is transmitted to an access control manager has to be configurable and extendible, depending on the needs of the Resource Owner and respecting the restrictions from the data protection law.

In order to describe the functionality of the AAI, the following generic model has been developed:

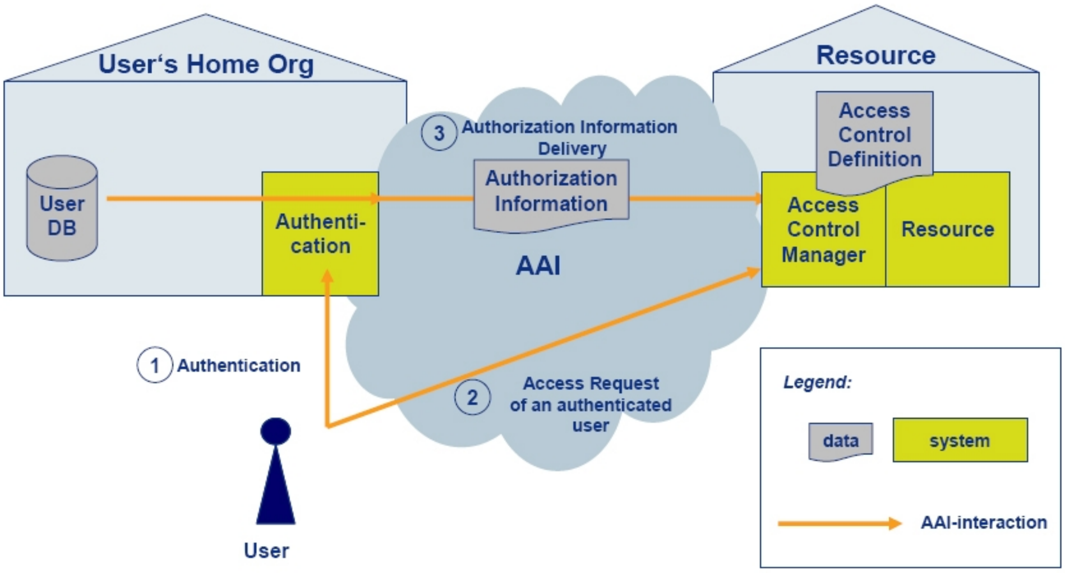


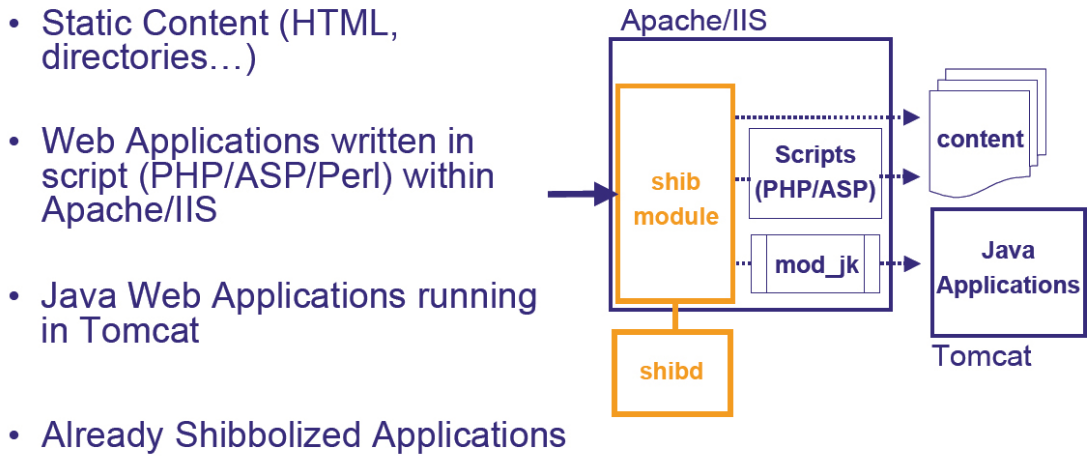
Figure 1: Generic functional model of an AAI

Figure 20: AAI Model

After having received the authentication acknowledgement and the authorization attributes from the user's Home Organization, the access control manager, on behalf of the Resource Owner, can decide whether to grant or deny access to the resource.

6.2.3 AAI Operation in EuQoS

In the EuQoS system the resources are represented by the theory course modules or by the Hands-on laboratories. Everyone of these resources is "protected" by the shibboleth software and in this way is completely integrated in the AAI architecture.



- Static Content (HTML, directories…)
- Web Applications written in script (PHP/ASP/Perl) within Apache/IIS
- Java Web Applications running in Tomcat
- Already Shibbolized Applications

Figure 21: General Resource's outline

(1-2) When a user tries to access the resource, the shibboleth module verifies his credentials and if he is not still authenticated, redirects the browser to the WAYF server.

(3-4-5) The User would then select his Home Organization and the WAYF service would redirect the browser to the User's Home Organization.

(6-7-8) The User then would complete the authentication by the AAI account and then he is redirected to the Resource carrying on the handle session.

(9-10) By the handle session the resource server could receive the user's credential and grant the access.

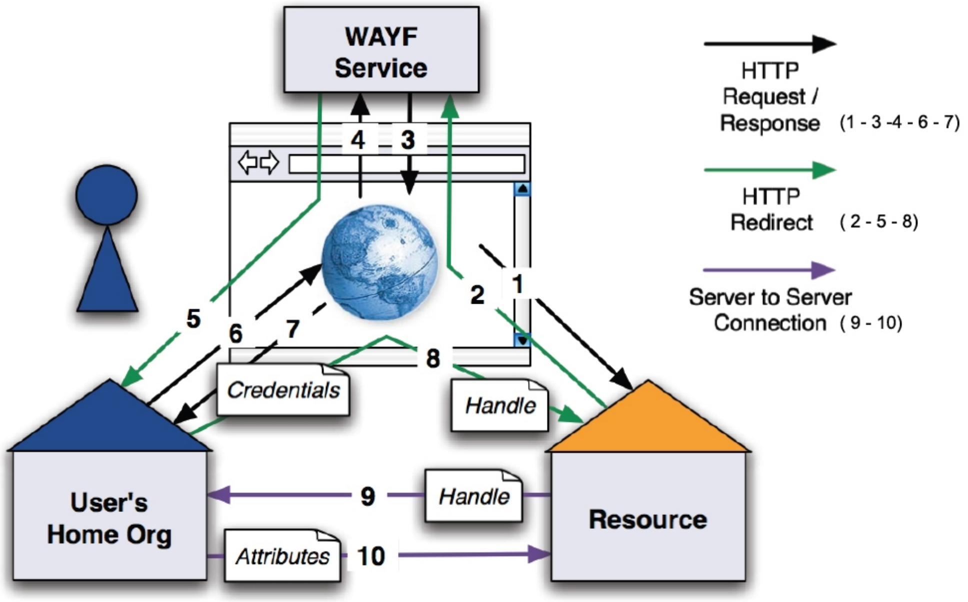

WAYF Service
4
3
1
2
5
6
7
8
Credentials
Handle
User's Home Org
Resource
9
Handle
Attributes
10
HTTP Request / Response (1 - 3 -4 - 6 - 7)
HTTP Redirect (2 - 5 - 8)
Server to Server Connection (9 - 10)

Figure 22: Resource Access Steps

This architecture provides the following benefits:

- Thanks to the 'virtualized' ID, resources can save the effort of registering and administering users based on paperwork.
- Because of standardized interfaces, resources can integrate users of other organizations without much effort.
- Due to a standardized authentication mechanism, users are granted access to various resources of a number of organizations with a single password, irrespective of location.
- All parties profit from a standards-based AAI

7 Hands-On: NS Laboratory

7.1 Overview

Traffic Engineering is one of the seven e-learning module developed in the work package 6 of first EuQoS phase.

In contrast to traditional laboratories, the audience of the EuQoS e-learning computer networks laboratories is global as learners can theoretically attend the laboratory wherever Internet access is possible and perform simulation without any further work in environment configuration.

The laboratory portal web interface offers the user the possibility to reset his session, and he can continue with the state of the system as he has left it in his last time-slot when he starts a new time-slot.

The interaction between the learner and the emulation platform can be achieved by the way of a classical Web Browser, allowing the learner to control the experimentation and to analyze and visualize results; the java web interface and the adaptation to the scenarios is included to the planned future activities.

Thanks to its integration in the authentication and authorization infrastructure (AAI), a single sign-on allows access to any resource, of course including this laboratory.

The result may be exploited as an extension to traditional teaching activities in universities and industrial further education. Actually the University of Pisa is one of the partners involved in the exploitation of the module. EUQOS course modules should help learners to go beyond traditional expository teaching.

7.2 Internet Remote Network Simulation Infrastructure

In this chapter we will describe the global architecture and the working details about the NS2 laboratory used in the hands-on session.

This Laboratory, installed and configured at the I.E.T. Department of the Pisa's University, is completely integrated in the EuQoS e-learning federation (SWITCH).

The Traffic Engineering Hands-on laboratory is based on the Internet Remote Network Simulation Infrastructure (IRNSI) which offers an easy way to include practical exercises based on network simulations.

IRNSI is fully accessible through the web by means of a web browser with support for Java applets. IRNSI is integrated in the course system by the lab portal and therefore supports the single sign-on of the EuQoS course.

The picture 23 shows the main parts that compose the NS2 laboratory and the connection between the servers involved in this architecture. These resources, as all the other ones in the EuQoS e-learning, are protected by the shibboleth authentication system, but this first access step, already described in chapter n°5, is not highlighted in the picture.

The NS2 lab is composed by 2 servers:

- Lab Portal Server (2) which manage the access from the internet to the NS-2 Testbed.
- NS2 test bed (3) where simulation effectively runs.

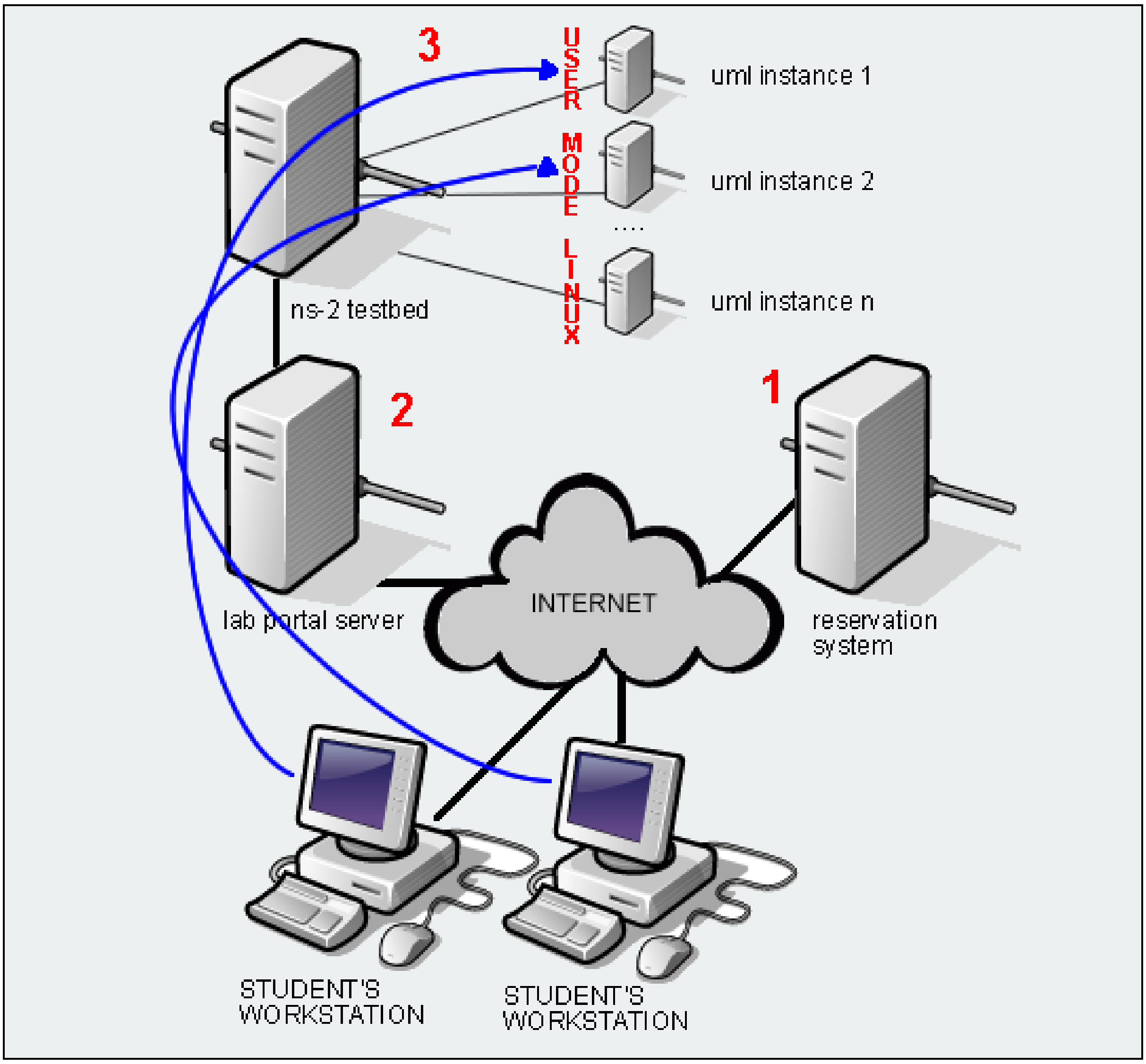


Figure 23: Laboratory Architecture

Moreover, the Traffic Engineering lab takes advantage of a further server, called Reservation System (1), commonly used by all the module of the e-learning system to manage the user access. In Fact, some modules needs to reserve time slots for the hands-on sessions in the laboratories, because the expensive laboratory devices are available only in limited numbers. The laboratory reservation system does not affect anything else than the admission to the laboratory devices of the respective modules. Everything else of these modules is accessible all the time.

Access Steps:

- Student try to access the NS2 laboratory and reach the Lab Portal Server which is the only machine directly connected to the internet.
- Lab Portal verifies the user's resources reservation, and, if it is not valid, redirects the user to the reservation system.
- The user makes a reservation, when available, for the resources he is interested in
- After that, the reservation procedure is completed, the lab portal is accessible during the time slot reserved.
- From the Lab Portal, the user can work on simulation running a virtual machine in the NS-testbed.
- As depicted in the picture other users can connect to the laboratory at the same time running a further virtual machine.

7.3 Portal Server

As already pointed out, the portal server is the main door to access the NS laboratory. This machine is the only one directly connected to the Internet with a static public IP address and two servers (Apache and Tomcat) are installed in it.

The lab portal provides an easy way to include laboratories in the course system. It provides an AAI protected container to access them. The portal checks if the authenticated user is a valid course participant and in case of a time-shared resource, if a slot is booked. This is accomplished by using web-services of the resource management server.

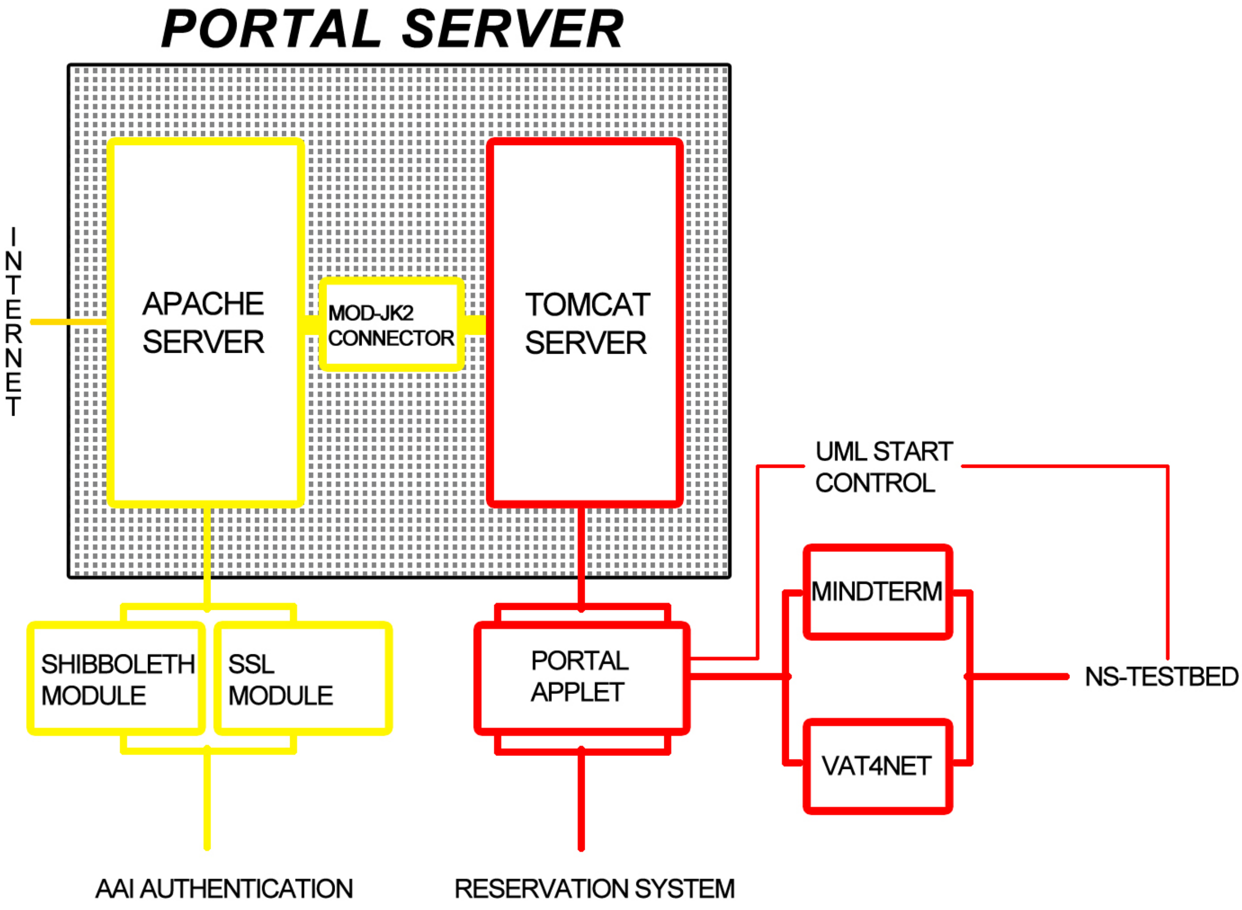


Figure 24: Portal Server Architecture

When a web client accesses this machine, the apache server installed answers the request. The main function of the Apache is to manage the AAI authentication process, and for this purpose it is configured to operate with 2 further modules: Shibboleth module and SSL module.

The SSL module is used to manage the certificate released by the “Thawte” Certification Authority and together with the shibboleth software accomplishes the AAI authentication process, as already described in paragraph number 5.

As soon as this step is satisfied, the apache ends its function and forwards all the incoming connections to the tomcat server, where the “Portal Applet” is deployed.

This application completely controls the laboratory and offers to the client the necessary front-end interface to take advantage of the lab potentiality.

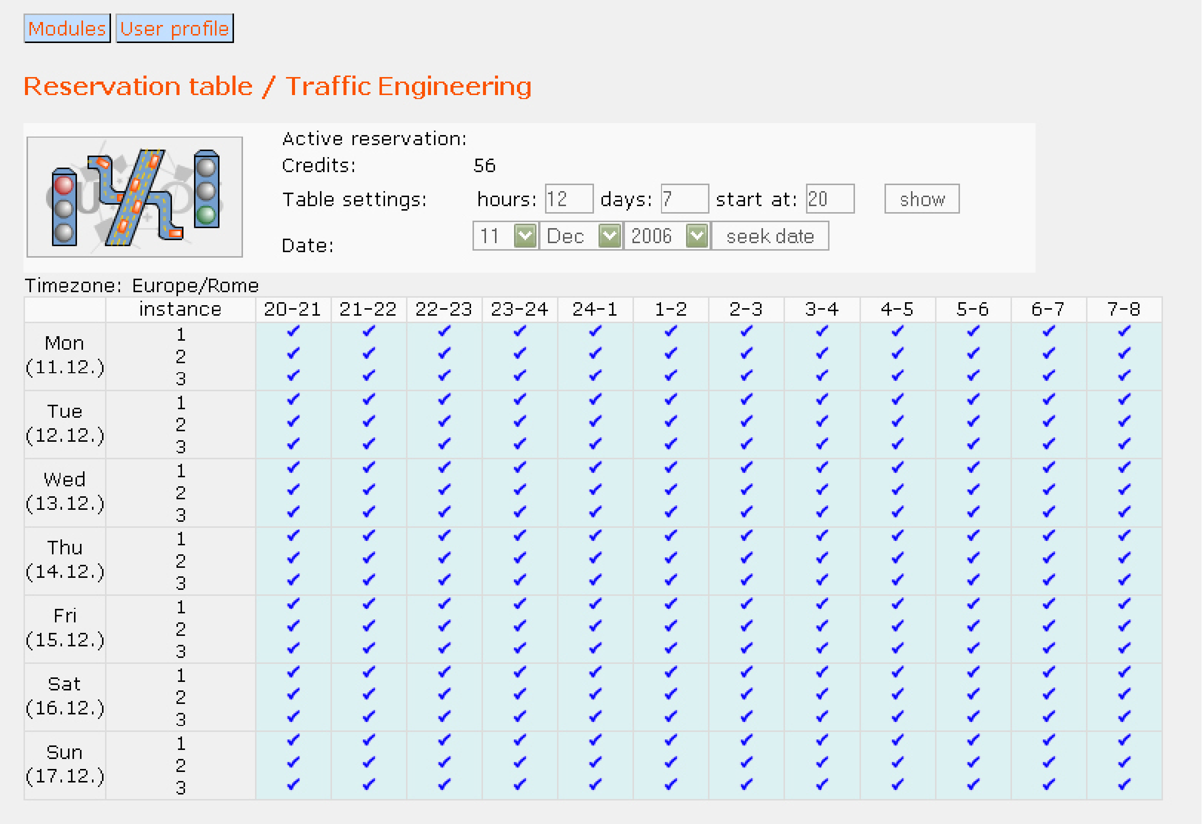
As soon as a new connection is established, the Portal Applet verifies the user credential to use the laboratory in the current time slot and if this is not satisfied forwards the connection to the central reservation system server. If available, the user can reserve the resource in the current time slot by the intuitive reservation interface and then he will be redirected back to the portal server where he is connected; if the resource is not currently available, the user can book an other time slot in the next few days.

This reservation procedure is very simple and quick from the student point of view thanks to the AAI federation architecture.

In fact, the portal applet (i.e. Tomcat server) is placed behind the Shibboleth software (i.e. Apache server) and when the user is redirected to the “Reservation System” he is already authenticated to the AAI federation and he has all the necessary credential to access the Reservation Server without a further log-in. The same happens when the user is redirected back to the Portal server from the reservation system.

In fact, the portal applet (i.e. Tomcat server) is placed behind the Shibboleth software (i.e. Apache server) and when the user is redirected to the “Reservation System” he is already authenticated to the AAI federation and he has all the necessary credential to access the

Reservation Server without a further log-in. The same happens when the user is redirected back to the Portal server from the reservation system.



Reservation table / Traffic Engineering

Active reservation:
Credits: 56
Table settings: hours: 12 days: 7 start at: 20 show
Date: 11 Dec 2006 seek date

Timezone: Europe/Rome

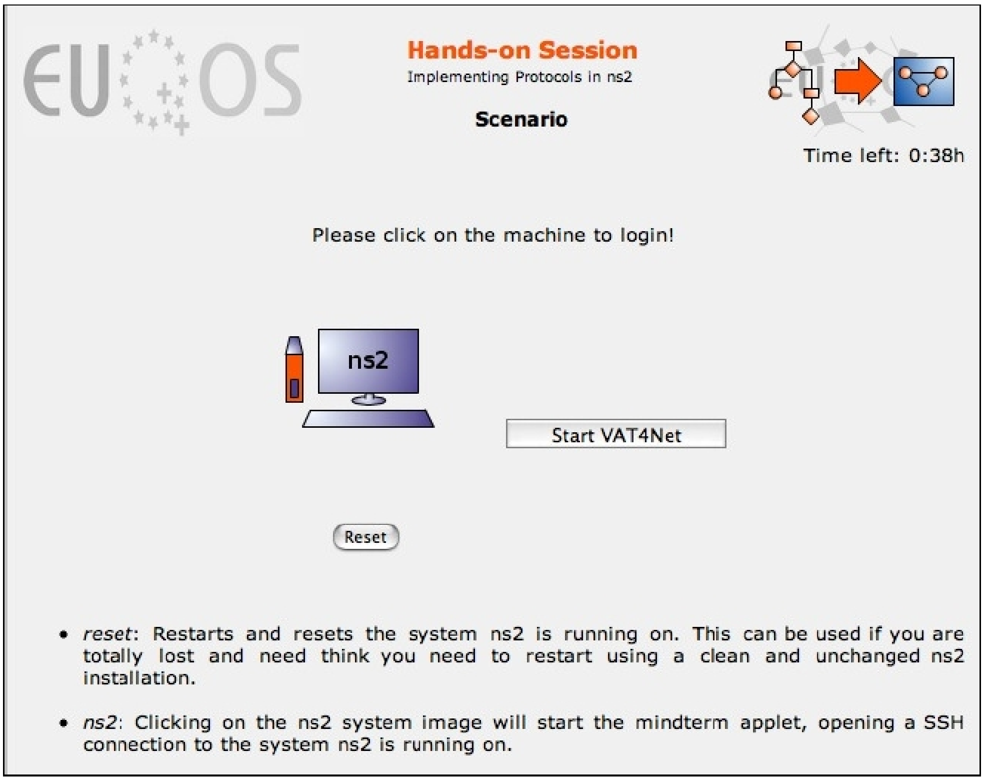
	instance	20-21	21-22	22-23	23-24	24-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8
Mon (11.12.)	1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tue (12.12.)	1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Wed (13.12.)	1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Thu (14.12.)	1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fri (15.12.)	1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sat (16.12.)	1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sun (17.12.)	1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 25: Reservation System

In fact, the portal applet (i.e. Tomcat server) is placed behind the Shibboleth software (i.e. Apache server) and when the user is redirected to the “Reservation System” he is already authenticated to the AAI federation and he has all the necessary credential to access the Reservation Server without a further log-in. The same happens when the user is redirected back to the Portal server from the reservation system.

After that the AAI authentication and the resource reservation have been accomplished, the user can access the laboratory web interface which is based on 2 other java applet. Both of them are project developed and released by Sourceforge project:

- MINDTERM used to work on the ns-test bed virtual machine
- VAT4NET used to analyse the simulation results



Hands-on Session
Implementing Protocols in ns2

Scenario

Time left: 0:38h

Please click on the machine to login!

- *reset*: Restarts and resets the system ns2 is running on. This can be used if you are totally lost and need think you need to restart using a clean and unchanged ns2 installation.
- *ns2*: Clicking on the ns2 system image will start the mindterm applet, opening a SSH connection to the system ns2 is running on.

Figure 26: Portal Web Page

Figure 4 shows the lab portal of an IRNSI (Internet Remote Network Simulation Infrastructure) module. As these modules are time-shared resources, the lab portal shows on the top right the remaining time for the current user. The user will be warned if his slot time is almost over.

7.3.1 Vat4Net

The Visualization and Animation Tool for Network Simulations (VAT4Net) is part of IRNSI and has been developed during phase 1 of EuQoS. VAT4Net is a tool to visualize and analyze network simulations.

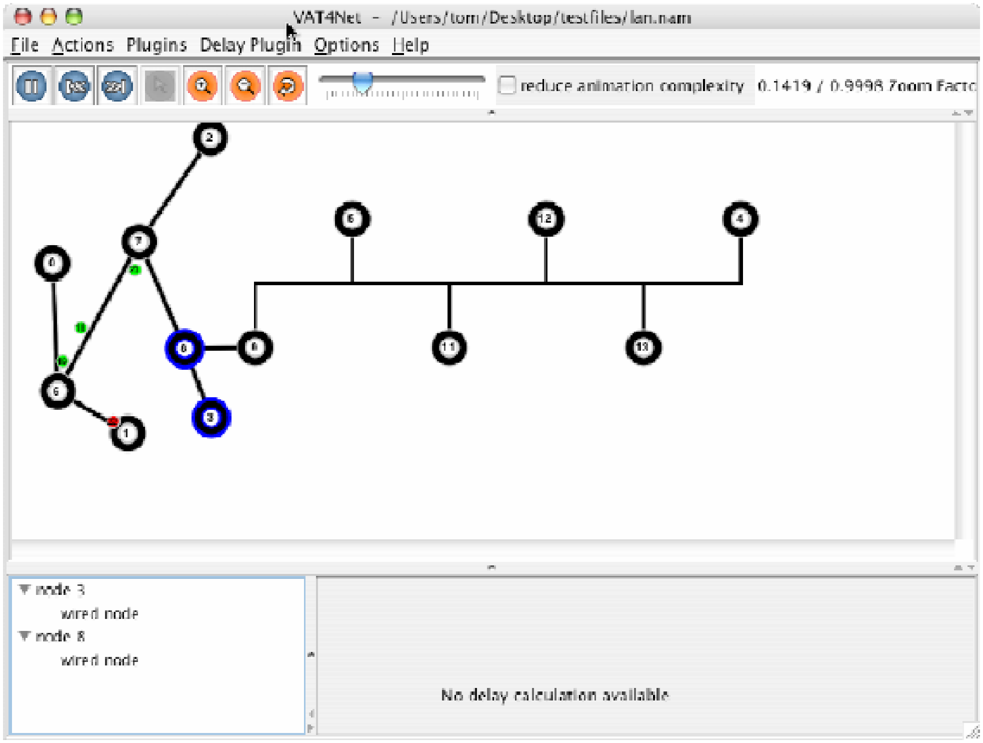
The animated representation of the network should help on analysing the running simulation. Having a graphical view on the scenario could help to discover several problematic areas in the network. The animation should give a good overview. On the other hand the visualisation possibilities prepare a more closer look on the simulation. Different statistical plug-in for main network-specific measurement are (and planned to be) available.

Visualization includes an animation mode, which makes it possible to visualise the dynamics of network situations during a running simulation. The part that enables static analysis is plug-in based, which facilitates enhancements and adaptation to one's needs.

VAT4Net has been developed to run as an applet or a stand-alone application as well, to handle local simulation trace files or remotely produced ones. For the remote case, it implements a remote parser and server component. At the moment, the client and the server part communicate through unsecured channels.

Future releases will integrate SSH secured connections and will add support for various trace file formats.

VAT4Net has been published on Sourceforge web site as open source software (licensed under GPL), enabling future users to have a look at the current status and give them the possibility to give feedback, evaluate their own requirements, and participate to the development.


VAT4Net - /Users/tom/Desktop/testfiles/lan.nam
File
Actions
Plugins
Delay Plugin
Options
Help
□ reduce animation complexity
0.1419 / 0.9998 Zoom Facto
2
7
0
6
1
8
3
6
12
4
11
13

▼ node 3
wired node
▼ node 8
wired node

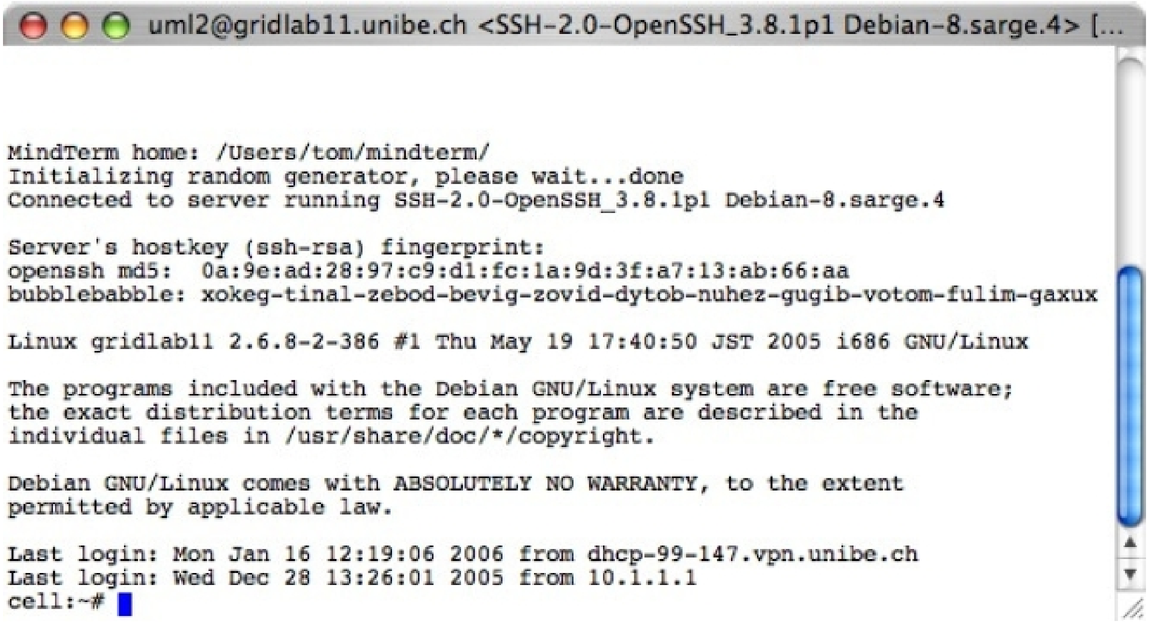
No delay calculation available

Figure 27: Vat4Net Interface

7.3.2 MindTerm

MindTerm is a complete ssh-client , and it is today probably the most widely spread client that implements the SSH1 and SSH2 protocols written in pure Java.

One of the key practices of developing security software it is proper implementation of the underlying algorithms and protocols it uses. It is a self-contained archive that only needs to be unzipped into a chosen directory and it is ready to be used. It can be used as a standalone program or as a web page applet or both. The MindTerm application will open a port on the client's machine (local machine) and any connection to that local port is forwarded to the remote host, and its listening port over an encrypted ssh session. When user runs MindTerm from the Portal Server, an instance of the test bed virtual machine is remotely started at first; after that, this applet automatically sets up an SSH tunnel to the new cell (UML instance). The User is now logged into the root folder of the remote NS-testbed virtual machine, where NS2 is already installed and configured for the required work.


uml2@gridlab11.unibe.ch <SSH-2.0-OpenSSH_3.8.1p1 Debian-8.sarge.4> [...

```
MindTerm home: /Users/tom/mindterm/
Initializing random generator, please wait...done
Connected to server running SSH-2.0-OpenSSH_3.8.1p1 Debian-8.sarge.4

Server's hostkey (ssh-rsa) fingerprint:
openssh md5:  0a:9e:ad:28:97:c9:d1:fc:1a:9d:3f:a7:13:ab:66:aa
bubblebabble: xokeg-tinal-zebod-bevig-zovid-dytob-nuhez-gugib-votom-fulim-gaxux

Linux gridlab11 2.6.8-2-386 #1 Thu May 19 17:40:50 JST 2005 i686 GNU/Linux

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Mon Jan 16 12:19:06 2006 from dhcp-99-147.vpn.unibe.ch
Last login: Wed Dec 28 13:26:01 2005 from 10.1.1.1
cell:~#
```

Figure 28: MindTerm Applet

7.4 NS Testbed

7.4.1 User Mode Linux UML

User-Mode Linux is an Open Source solution that creates a virtual Machine and allows you to run multiple instances of Linux on the same system at the same time. As each guest (virtual linux systems) is just a normal application running as a process in user space, this approach provides the user with a way of running multiple virtual Linux machines on a single piece of hardware, offering excellent security and safety without affecting the host environment's configuration or stability.

UML does not require any additional virtualization software. Instead, you patch the source of the Linux kernel you want to run as your Guest OS (Virtual Operating System). This UML patch converts the kernel into an executable binary called 'linux', which allows the Guest kernel to run on the main system as a separate operating system. Running this UML patched kernel, all is needed to do is to give it a filesystem to use, and the user has an independent Linux system running on his computer. This new kernel is a user space application running on the real kernel (Host OS). The UML kernel receives system calls from its applications and sends/requests them to the Host kernel.

It runs its own scheduler and virtual memory (VM) system, relying on the host kernel for hardware support. It includes virtual block, network, and serial devices to provide an environment that is almost as full-featured as a hardware-based machine. UML cannot destroy the host machine. Furthermore, the UML block devices, also called disks, can be file on the native Linux file system, so that user cannot affect the native block devices. Each UML instance is a complete virtual machine that's all but indistinguishable from a real computer. All of them run as a normal user on the host. They give root-level access,

the ability to start daemons, the ability to run text and graphical applications, full networking, and almost all of the other capabilities of a Linux system. The only exception is that user cannot directly address hardware inside UML, so the UML environment provides virtual network adapters, virtual X Window displays, and virtual drives.
The virtual machine can be configured through the command line, which allows memory and devices to be configured. The kernel, and hence any programs running under UML, runs as a software process of the real/host Linux system rather than directly under the hardware. UML can give complete root access, and can run the same programs, that would normally be ran on a Linux server.

7.4.2 UML in NS-Testbed

On the testbed server, virtualization is used (user mode Linux, UML) to provide multiple instances of the same module that are completely separated. For every instance the user gets a sand-boxed virtual server. The test-bed sets up the virtual server according to a standard image at the beginning of each slot. This process assures that each student gets a blank and clean module instance at the beginning of his hands-on session.

The user's changes to the file system of the UML instance are stored in a Copy-On-Write (COW) file. The standard image is write protected and may not be modified by the user itself. With the COW file and the standard image, it is possible to restore the last state of a user's session (see Figure 29). This offers the student to continue his work in a later time-slot. By default IRNSI loads the latest state at the beginning of the user’s next time slot. Optionally, the user can reset the state of the virtual machine by the web interface. The reset invokes the restart of the virtual server instance, but only loads the standard image and generates a new clean COW file.

As already introduced, NS2 is installed in the UML file system image and it is used by all the virtual machines (UML instance). This installation is already patched for the Traffic Engineering, it supports the MPLS protocol and it is already configured for the required hands-on sessions of the e-learning module.

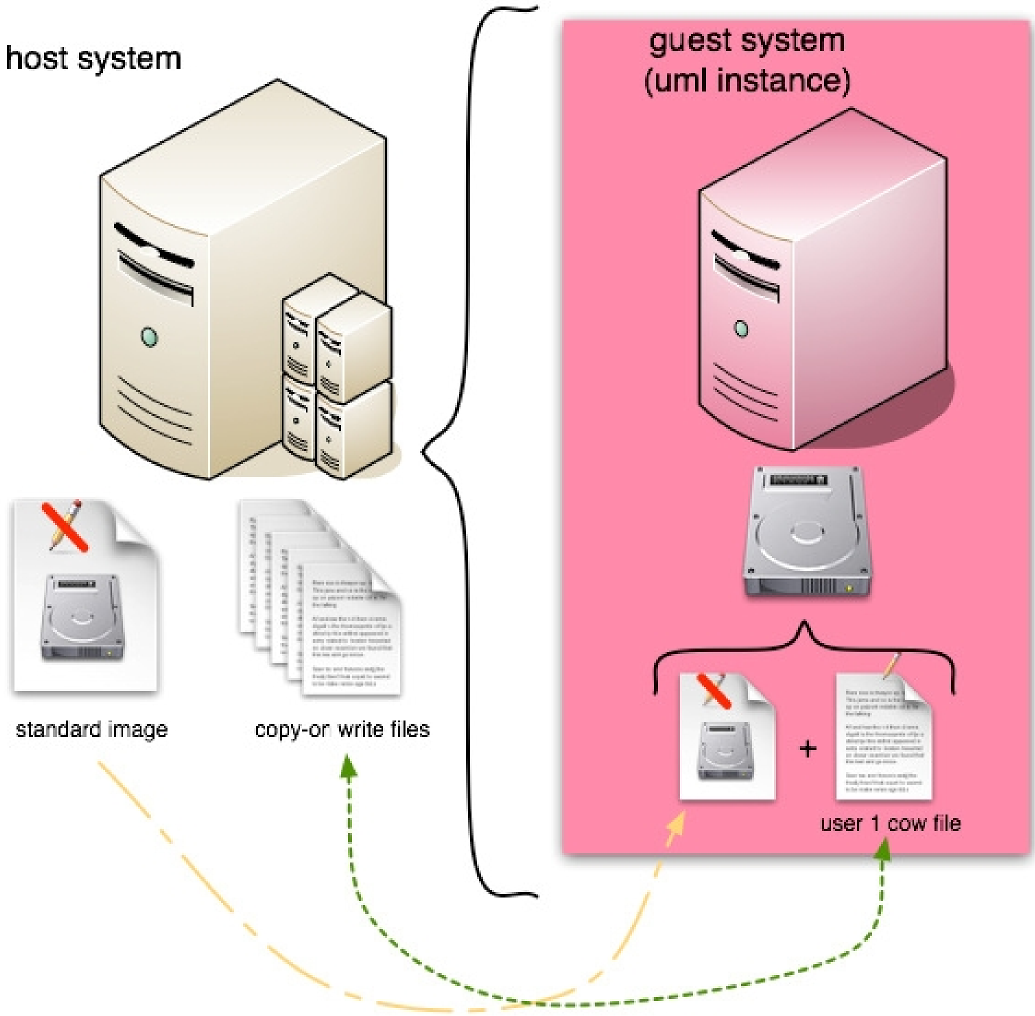


Figure 29: Virtual disks consist of standard image (write protected) and a user specific copy-on-write file

7.5 NS Scenes

Throughout the described architecture, learners are able to use the NS2 software installed in the testbed machine.

The native NS2 software don't support the MPLS protocol and so that, this installation has been appropriately patched to allow the traffic engineering of the flow in the users simulations.

The work to patch NS2 with MPLS protocol is based on two available patch developed by the Department of Computer Engineering of the Chungnam National University (Korea) and by the Siemens research center.

Further more, two different simulative scenario have been implemented and are provided in the NS2 folder of the testbed system:

- The first scenario includes an MPLS autonomus system domain
- The second scenario includes only plain IP router

The MPLS scenario is depicted in the figure below.

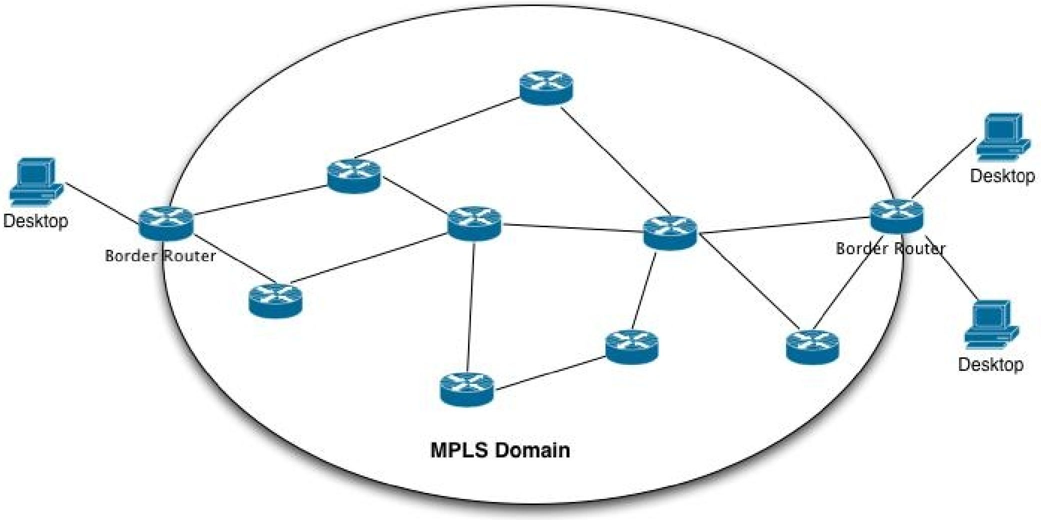


Figure 30: Network Scenario Topology

This scenario, used for the traffic engineering simulations is composed by ten routers which formed the MPLS domain. Two router (Border Routers)delimits the AS and connect the domain to the sources and destinations of the traffic flows. The plain IP routing scenario is based on the same network topology.

Lab learners could use both the scenario to run simulations, evaluate the performance rate (packets loss, packets delay, link utilization) and compare the obtained informations. Finally an appropriate traffic engineering have to be projected according to the analysis result.

8 Conclusions and Future Developments

The EuQoS project has been created essentially to improve the QoS in the telecommunication field. That is to really let networks and applications be interoperable and then to let the new services distribution be faster and usable.

Especially, in the next future EuQoS is projecting a software platform which is able to realize an uniform use of the different applications on heterogeneous access network. In this way, the applications which requires a special QoS to be correctly distribute on commercial networks will receive a sensible improvement and the qualified traffic on the Internet could be enlarged.

This improvement of the internet features will allow the quickly development of several kind of applications like the VoIP application, video conference, video streaming, education, tele-engineering and medical applications which have got numerous potentiality and will have a great evolution in the next future.

Anyway, one of the application that is going to definitely get a wide diffusion using the new networks capability is the e-learning.

In fact, allowing a good reception of multimedia, realtime and interactive services, the e-learning activities are going to be an important help to improve the classic way of teaching, and it will frequently be integrated in the academic courses, in the company training and in the public administration formation project. This trend is following what is already happened in the USA some years ago.

EuQoS too is going to project a powerful e-learning system and in this context this thesis work has been developed. The study and the implementation of a solution to provide the Traffic Engineering e-learning module has been my contribute to the the EuQoS e-learning project.

Within the framework of this thesis, the goals to reach were to project a theory section for the related knowledge, to implement a network simulation laboratory where learner could focuses only on the traffic engineering study and finally to manage the integration of this module in the EuQoS e-learning system.

The objectives of the work have been reached and the Traffic Engineering module, implemented by me, has been integrated in the EuQoS e-learning architecture and used in the course “Advanced Networking Architectures and Wireless Systems” held by Prof. Luciano Lenzini at the University of Pisa, and in the course “Multimedia Communications" held by Prof. Torsten Braun at the University of Bern.

This work has been developed within phase 1 of the EuQoS project, when the first seven e-learning module have been realized. During the second phase of the project, already started, seven more modules will be implemented and the whole system will be integrated in several more academic courses.

9 Abbreviations and Acronyms

AA	Attribute Authority
AAI	Authentication and Authorization Infrastructure
ACS	Assertion Consumer Service
AR	Attributes Requester
ARP	Attribute Release Policies
AS	Autonomous System
BGP	Border Gateway Protocol
CBR	Constraint-Based Routing
COS	Class of Service
COW	Copy-On-Write
CR-LDP	Constraint Based Label Distribution Protocol
CSPF	Constraint Shortest Path First
EuQoS	Europeen Quality of Service
FAQ	Frequently Asked Questions
GPL	General Public License
GUI	Graphic User Interface
HS	Handle Service
ICT	Information Communication Technology
IDC	International Data Corporation
IdP	Identity Provider
IET	Institution of Engineering and Technology
IETF	Internet Engineering Task Force
IRNSI	Internet Remote Network Simulation Infrastructure
ITU	International Telecommunication Union

LMS	Learning Management System
LSP	Label Switched Path
MM	Multimedia
MPLS	Multiprotocol Label Switching
NRT	Non Real Time
NS2	Network Simulator 2
OS	Operating System
OSPF	Open Shortest Path First
P-SLS	Peering Service Level Specification
PKI	Public Key Infrastructure
QoS	Quality of Service
RA	Resource Administrator
RM	Resource Manager
RSVP	Resource ReserVation Protocol
RT	Real Time
SLA	Service Level Agreement
SLS	Service Level Specification
SP	Service Provider
SPF	Shortest Path First
SSH	Secure SHell
SSL	Secure Sockets Layer
SSO	Single SignOn
SWITCH	Swiss Information TeCHnology Services
TE	Traffic Engineering
U	Unbounded
UML	User Mode Linux
VAT4Net	Visualization and Animation Tool for Network Simulations
VM	Virtual Memory
WAYF	Where Are You From
WP6	Work Package 6

10 References

[1] "EuQoS" project, http://www.euqos.org.

[2] Deliverable D1.1.1: "Definition of Business, Communication and QoS models – Intermediate". EuQoS project, March 2005.

[3] Tracie E. Monk, "Inter-domain Traffic Engineering: Principles and Case Examples", INET2002, June 2002.

[4] Deliverable D1.1.3_v2: "Business models and system design specification", EuQoS project, September 2005

[5] Christoph Graf, Ueli Kienholz, Thomas Lenggenhager, Marc-Alain Steinemann, André Redart, "AAI – Authentication and Authorization Infrastructure", SWITCH, December 2003.

[6] Deliverable D6.1.3: "Description of complete pilot course implementation and course teaching / learning platform including evaluation report from pilot course delivery", EuQoS project, January 2006

[7] X.Masip-Bruin, M.Yannuzzi, R.Serral-Gràcia, J.Domingo-Pascual, J.Enríquez-Gabeiras, M.Callejo, M.Diaz, F.Racaru, G.Stea, E.Mingozzi, A.Beben, W.Burakowski, E.Monteiro, L.Cordeiro: "The EuQoS System: A Solution for QoS Routing in Heterogeneous Networks"

[8] Deliverable D6.1.1: "Specification of contents and didactical concept of the course to be offered", EuQoS project, March 2005

[9] Joe Pulichino, "Future Directions in e-Learning Research Report 2006", The Elearning Guild Research, April 2006

[10] Lucio Magliozzi, “Datamat” Press Release, http://www.datamat.it .

[11] The User-mode Linux Kernel Home Page, “http://user-mode-linux.sourceforge.net”

[12] Jeff Dike, “A user-mode port of the Linux kernel”.

[13] “Learning with User-Mode Linux”, Honeynet project

[14] Stephen Downes, “e-Learning 2.0”, National Research Council of Canada.

[15] Shibboleth project, “http://shibboleth.internet2.edu”

[16] Nikolaos Vasiliou, “Overview of Internet QoS and Web Server QoS”, Department of Computer Science, University of Western Ontario, April 2000.