Title:	Document Version:
Deliverable D3.4 **Guidelines of IPv6 QoS Measurement**	0.7

Project Number:	Project Acronym:	Project Title:
IST-2001-37611	6QM	IPv6 QoS Measurement

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
30/11/2004	05/12/2004	R – PU

* Type: P - Prototype, R - Report, D - Demonstrator, O - Other
** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Responsible and Editor/Author:	Organization:	Contributing WP:
David Diep	HIT	WP3

Authors (organizations):

Guido Pohl (FOKUS), Elisa Boschi (Hitachi Europe), Lidia Yamamoto (Hitachi Europe), Jordi Palet (Consulintel).

Abstract:

This deliverable describes some guidelines for applications and further research of the IPv6 QoS measurement.

Keywords:

Guidelines, further research, multi-homing, automated network, application monitoring.

Revision History

The following table describes the main changes done in the document since created.

Revision	Date	Description	Author (Organization)
v0.1	01/09/2004	Document creation	David Diep (HIT)
v0.2	15/10/2004	Input on network autonomics, extended architectures and inter-domain	Lidia Yamamoto (HEL)
v0.3	18/10/2004	Input on inter-domain	Elisa Boschi (HEL)
v0.4	26/10/2004	Input on hardware-based measurement probe	Guido Pohl (FOKUS)
v0.5	10/11/2004	Editorial changes and additional content	David Diep (HIT)
v0.6	22/11/2004	Minor changes	David Diep (HIT)
v0.7	05/12/2004	Final review	Jordi Palet (Consulintel)

Executive Summary

This deliverable is the closing deliverable of WP3. During the 6QM project many aspects of the IPv6 QoS measurement have been addressed. The purpose of this document is to identify the areas where further research could be performed in the future.

The document classifies the further research aspects into two categories:

- Guidelines for further system improvement.
- Guidelines for further application area.

Concerning the system improvement the document identifies the following area:

- Given the increase of traffic flowing in the network, the system should be able to deal with this increasing amount of data. This could be addressed by developing a hardware-based meter.
- The interdomain measurement remains a challenging issue and there is not yet some agreed standard to enable such a measurement. This topic still needs a great amount of work in order to deal with the existing heterogeneous systems and to create some technology that could be applicable by carriers at large scale.
- This current measurement system addresses IPv4 and IPv6 however it could be interested to look forward at the new emerging address families.
- The mobility was not addressed within the project and could be investigated in the future. The document identifies the related issues.
- The control of heterogeneous systems should also be investigated in the future.

Concerning the further application area the document identifies the following area:

- The usage of the QoS monitoring to support autonomic communication.
- The usage of the QoS monitoring to support the multi-homing in regard of the access selection.
- The usage of the QoS monitoring to assist automatic MPLS path configuration.
- The usage of the monitoring at application level would also bring value and this would need further investigation to target specific applications.

Many areas remains opened in the field of the QoS monitoring. However one very important aspect that is pointed out in this document is the possibility to integrate core measurement components into existing system such as control and configuration systems. This integration could really bring benefit to the community.

Table of Contents

Table of Figures

1. INTRODUCTION

The WP3 is composed of four deliverables:

- The deliverable D3.1 specifies the technologies to be used.
- The deliverable D3.2 documents the prototype measurement system.
- The deliverable D3.3 provides a revised specification of the measurement system.
- The deliverable D3.4 provides guidelines for applications and further research.

This deliverable is the closing deliverable of WP3. During the 6QM project many aspects of the IPv6 QoS measurement have been addressed. The purpose of this document is to identify the areas where further research could be performed in the future.

According to our opinion the further research should improve the QoS measurement system itself concerning the performance, the inter-domain, the support for new address families and mobility.

In addition, in this deliverable we also try to identify some areas where the QoS measurement could be applied to bring additional results or benefits to the overall service and user experience. The areas identified are the autonomic communication, the multi-homing, the MPLS configuration and the application monitoring.

2. GUIDELINES FOR FURTHER SYSTEM IMPROVEMENT

This section identifies some areas for improvement concerning the IPv6 QoS measurement system.

2.1 Performance

The broadband access is developing very quickly in some countries. For example Japan represents a very interesting case of success for broadband access. The situation of Japan presents several interesting characteristics. According to the statistics collected by the Japanese "Ministry of Public Management, Home affairs, Post and Telecommunications" (MPHPT), the majority of broadband users use DSL services. As shown in the figure below it is from far the most popular way to access broadband services.

Technology	Number of subscribers
DSL	11,819,177 (end of May, 2004)
Cable Internet	2,661,000 (end of May, 2004)
Optical Fiber	1,327,775 (end of May, 2004)
Wireless	29,000 (end of May, 2004)
Total	15,836,952

Figure 2-1: Subscribers per Broadband Technologies (source: [MPHPT])

According to the other statistics collected by the MPHPT, the number of DSL service subscribers has increased very quickly. In May 2000 the number of subscribers was very little with only 760 subscribers. However in five years the situation has totally changed according to recent statistics this number reached almost 12 millions at the end of May 2004. For reference the figure below presents the fast increase of DSL subscriber number since May 2000.

Date	DSL subscriber number
May 2000	760
May 2001	178,737
May 2002	3,028,556
May 2004	11,819,177

Figure 2-2: DSL Subscriber in Japan (source: [MPHPT])

In parallel, the DSL bandwidth capacity is increasing quite quickly too. According to [InfoCom] ADSL service offer reached 1.5Mbps in 2001, 12Mbps in 2002 and 40Mbps in 2003 (in downstream). Those figures should be taken with care as the bandwidth really available varies a lot depending on the distance of the user to the access point however it is a good indicator to understand the trend and the competition between ISP to provide more and more bandwidth. On its side the optical fiber access already offers service at 100Mbps to end-users. This means that

in a country such as Japan broadband users are already numerous and equipped with fast connection to the Internet.

To summarize the major points for the Japanese broadband are:

- The success of DSL access.
- The fast increase of subscriber number to broadband services.
- The high in bandwidth capacity.

This means that the traffic at the ISP access network is very likely to increase a lot to in the coming years with the deployment of new services exploiting such a bandwidth. The consequence on measurement equipment is that it will be required to create systems for gigabit capacity and beyond even near the access of the ISP network in near future implying enhanced capturing and filtering functions in the meters to enable higher capacity. It is also clear that in order to monitor the core network hardware based system is mandatory.

The increase of performance could be done by exploring the usage of:

- Kernel level meter.
- Network processor based meter.
- Hardware meter.

A hardware-based meter that integrates into the 6QM measurement system can be implemented in several ways. We pick here one possibility that proposes to use specialized peripheral cards that are hosted within a “standard” personal computer and that rely on peripheral bus connection via PCI or PCI-X to that computer.

A widely known series of dedicated network monitoring interface cards is the [Endace] DAG series. The series consists of cards each with support for one specific physical layer. The cards are suited to keep up with a line rate of OC-192 (or 10 Gigabit Ethernet).

The DAG cards realize monitoring functionality with time stamping of packets within Field Programmable Gate Arrays (FPGAs). Additionally, some of them have an onboard CPU that is user programmable and can be utilized to process captured packets on the fly. The DAG cards are designed to capture packets (or cells) completely or partly. Transmission of packets is not precluded but the functionality is currently not implemented.

Utilization of such cards for a meter could be beneficial, because of

- Precise time stamping due to hardware supported synchronization via GPS.
- Possibility to capture packets at line rate.

The latter property is mandatory for a system that is used for inter-domain measurements since internet service providers have higher line bit rates at their exchange points and their transit network then those that are usually used at network access.

Integration of measurement hardware into a hardware supported meter variant for the 6QM system can be realized as depicted in Figure 2-3. As can be seen in the architecture a DAG card is used to access the packets from the underlying network. The DAG card also attaches timestamps to captured packets. The control flow of the meter starts from the control interface and extends to the card driver software. The meter control must transpose commands that enter the control interface (OpenIMP control protocol) into control messages for the DAG card and the software components on top of the card. There is a helper library available for the filtering and classifying functionality, which is [CORAL]. Above the filtering and classifying, the packet is

processed by the packet processor component that calculates the packet identifiers. Finally, the packet is stored and scheduled for export via the export interface.

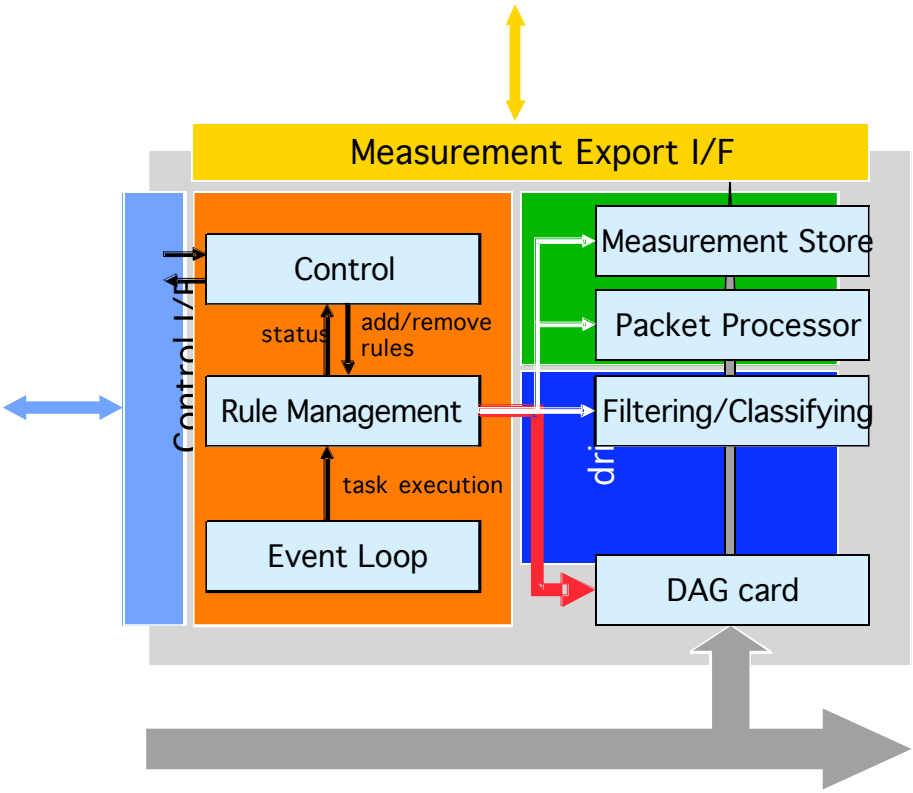

Figure 2-3: Hardware supported meter

The use of the DAG cards eases the burden for the CPU when capturing packets. Some functions need to be realized in software though, such as filtering and generation of packet identifiers.

A hardware-based network probe could also benefit from the use of so called "network processors" (NPUs). The definition of "network processor" is however somewhat loose and vague. Instances range from very specialized co-processors to more general-purpose processors with certain support for network packet processing. Standard task for packet processing is packet forwarding grounded on lookup of a packet's 5-tuple normally combined with a LPM (longest prefix match). Some of the NPUs (we arbitrarily selected [ClassiPI], [EZCHIP1]) can perform pattern matching at high rates within the whole packet content thus enabling layer 2 through layer 7 processing. A measurement probe could truly benefit from this capable processing power of such NPUs. Support for IPv6 packet processing must be investigated.

Moreover, at the opposite of the high performance hardware meter, one can also think about lightweight meter software using limited CPU and memory that could be installed on end user hosts, mobile devices or servers.

As a conclusion there are at least two ways to evolve for such a software one is to be able to increase the performance to process more packets and one is to be able to run with limited resource on lower performance plate-forms.

2.2 Inter-domain

Inter-domain performance measurement is a mandatory element to enable full end-to-end QoS support. However the great challenge is to make it really happen in practice and obtain its acceptance among competing network providers. The only chance to achieve this is to offer a technology with which providers can feel confident that they have control on the type and amount of information that is disclosed to other domains, and exactly to whom it is disclosed. Two main points deserve a particular attention when talking about inter-domain issues:

- Firstly, the heterogeneity of such an environment. Different ISPs already monitor their network but they often have very different tools and the configuration and data exchange systems need to be general enough to be deployable. It becomes evident the need for a standard format and protocol to perform inter-domain communication.
- Secondly, the issue of trust. In order to be willing to exchange their data and give information about their own network to third parties, ISPs need to join business coalitions, consortia, make cooperation agreements. Security aspects, and a mean to securely authenticate, authorize, exchange information is in this context strongly needed.

The current 6QM architecture for inter-domain measurements is a first step towards automation of inter-domain monitoring and measurement in a way that fully respects each provider's policies and constraints. The Specification of Measurement Service (SMS) Format allows measurements tasks to be requested, negotiated and established among different domains, while keeping domain-specific topology, access control, and other information private to each domain. It provides the general format to configure inter-domain measurements. It is general enough to be easily deployable in different domains and directly translatable in mostly meter configuration languages. The IDFIX data export format, strongly based on IPFIX (and therefore compliant to it) allows measurement results to be exported across domains. IDFIX is basically an adaptation of IPFIX to inter-domain, featuring a better performance, reducing the overhead without revealing each domain's private information.

However, much remains to be done in this area. For a fully flexible and resource-aware solution, the negotiation mechanism designed and proposed in [Yama2004] would have to be implemented and integrated into the platform.

Even the solutions addressed and suggested in the project would deserve to be deeper studied, implemented and tested. Configuring measurements and exporting data in such a heterogeneous environment needs standard formats and protocols. Standardizing the proposed solution would be a big step in the direction of a general format deployable in many different domains.

Security is another aspect extremely important that deserve particular attention. The appropriate solutions exist (e.g. a fully featured AAA system) and have been mentioned in the architecture design.

2.3 Support for New and Emerging Address Families

It is a fact that the current IPv4 model and addressing scheme is too limited to scale to a planet-wide Internet and to support the wide range of applications on today's and tomorrow's Internet. The proof of that is the large amount of middle boxes such as NATs, firewalls and proxies that are pervasive in the Internet nowadays. IPv6 was proposed about a decade ago as a solution to this problem. It brought back the hope of a single universal address space, large enough to hold all devices on the planet and beyond. It solved several other shortcomings of IPv4, and had a transition plan for the transition from IPv4 to IPv6.

However, the IPv6 design was not visionary enough. It did not bring enough concrete technical or business advantages to drive massive transition movements towards the new protocol. Its transition plan required both address families to be kept for a relatively long period, which would mean double work maintaining both protocol stacks, and did not really provide a solution for those starting with pure IPv6 to communicate with the legacy IPv4 Internet in a transparent way.

Today the major researchers and designers of the original Internet finally admit that a new architecture to satisfy all the diverse user, operator and business requirements must radically depart from the original model and must reach much farther into the future. The NewArch project [Newarch] is a testimony of this conclusion. It is developing new architectural solutions starting with a deep requirement analysis. As results, it has already produced concepts such as:

- FARA [Clark2003b], a new addressing architecture, which does not require a global address space.
- Role-based architecture [Braden2002], a new protocol and packet structure that departs from the traditional layered model towards functional composition of protocols, which is compatible with the middlebox model.

These concepts acknowledge the fact that a global address space is a myth, and that middleboxes represent a business requirement that must not be ignored. We do not know yet if these new concepts will actually become IETF standards or will be actually deployed. Much has to be researched before that happens, and many alternative proposals exist. However, in any case, there seems to be strong indication that, in the next generation Internet, IPv6 will be just another address family among others.

Therefore, in order to be suitable for the networks of the future, the 6QM platform will have to be enhanced to “MQM”, where “M” stands for “multiple address families”. This should not be a big problem in practice, since the 6QM platform is already a multi-address family system, supporting both IPv4 and IPv6. Adding other address families should be relatively straightforward.

2.4 Mobility

Mobile device supports more and more rich content and are expected to run IP multimedia application in the future. IPv6 and its dense number of addresses will especially enable this trend. As a result of those applications, the QoS will become an issue and will need to be controlled. However the QoS measurement in the context of the mobility presents many issues and challenges, the following of the section points out some of those issues.

In the fixed IP network environment the assumption we made is that in order to measure end-to-to performance it is enough to place a measurement device on the same Local Area Network (LAN) as the host under observation because the LAN is not likely to create very different connection performance from one host to the other. So the measurement system will measure accurately the QoS experienced by the host under observation. In the mobile world the situation is different because of the radio access performance that is highly correlated with the location of the devices. One way to solve this problem is to have the metering system embedded in the mobile device itself for a proper estimation of the end-to-end QoS. However the mobile device can be very various for example laptop, PDA, or cell phone as a result the computing power, memory and power consumption are very various too among those devices. Therefore the software embedded in the device should be lightweight and tailored according to the hosting device characteristics.

The measurement of the QoS may require synchronization functionality for example the measurement of the one-way delay requires at least two points of measurement presenting a coherent synchronization in order to allow a proper output from time stamping functions. In order to achieve such synchronization the usage of the GPS is classical solution however in the context of an embedded device the synchronization scheme may become problematic and should be investigated. This may be solved by DCF77 or CDMA synchronization.

Mobile devices use the radio access, the classical constraint of the radio environment is the constraint in resource availability (limited bandwidth) or price (per-packet based billing). As a consequence the radio resource used for the monitoring should be minimized as much as possible as it is a strong issue. For example in the fixed network capturing every packet and exporting such an information from device is possible however to proceed in such a way on the mobile device is certainly unacceptable from a resource usage point of view. As a consequence optimized communications schemes are necessary.

Moreover if considering a protocol such as Mobile IPv6 [RFC3775] one should be careful. When the mobile host is out of its home network, it uses a Care-of-Address as a substitute for its home address. This Care-of-Address is changing typically when the mobile moves to another network. If the route optimization is used (implying that the feature is supported by the correspondent node) the traffic flow source or destination may vary over time as the optimized traffic is exchange directly between the mobile node and the correspondent node by using the mobile node Care-of-Address to exchange packets (illustrated on Figure 2-4).

For the delay passive measurement the user traffic is captured and filtered at several measurement points and then exported at a central point for correlation. The issue in the context of Mobile IPv6 is that the traffic flow identifier may change (in case of route optimization). It means that to measure a given user application flow, the filter that is used by the packet capture needs to be updated according to the change of the Care-of-Address.

This could be certainly be solved by monitoring the “binding update” message that serves to communicate the value of the Care-of-Address and then by reconfiguring the filtering used for the packet capture.

Moreover to one should be careful concerning the tunneling issue because the packets at the correspondent node are not tunneled while the ones at the mobile node may be tunneled as a consequence some additional operations may be required to match the packets at those points.

Delay passive measurement presents some issues to be solved; on the contrary the delay active measurement looks straightforward to apply in this environment if we consider the probing components embedded in the correspondent node and the mobile node.

Figure 2-4: Mobile IPv6

As a summary the monitoring for mobile would need to address at least:

- The software design adapted for light platforms.
- The problem of synchronization.
- The efficient radio resource usage.
- The potential adaptation for Mobile IPv6 environment.

2.5 Heterogeneous platform and Component Control

A complex system such as a communication network is composed of different elements that are also heterogeneous in terms of their capabilities and their control. Specifically for network elements that provide accounting or measurement functionality, working groups of IETF are working on standardization of protocols to unify the export of those data; among these working groups are IP Flow Export (IPFIX) or AAA; the latter promoting *Diameter*, which is also capable of transferring accounting data.

There is surprisingly little effort to unify or standardize a control protocol for accounting or measurement equipment with the exception of SNMP, RADIUS and DIAMETER. However, the mere existence of such a variety of control protocols shows that a measurement system might have to tackle with the problem of heterogeneity. Then also, the question arises whether these protocols are suitable for all cases of measurements.

Currently there is work in progress in an IETF working group called Next Steps in Signaling (NSIS). There are proposals for a common problem on how to control and configure network elements for accounting and measurement along a network path. Members of the NSIS WG propose a *path-coupled* signaling of configuration information because measurement components are usually configured for flows that follow a certain path based. For more information about the proposal, refer to [DrNSIS].

Also and in particular for the case of inter-domain measurements, the discussion about the NSIS proposal could be very beneficial to follow; since in case of inter-domain measurement configuration of network probes is a problem. The NSIS Working Group defines as one goal to develop a transport level protocol suitable for signaling and to investigate security consideration thereon.

In the future, the 6QM measurement system could integrate the result of such working group if possible in order to have a standard measurement setup.

3. GUIDELINES FOR FURTHER APPLICATION AREA

This section identifies some areas where the usage of the QoS measurement would bring interesting results and could lead to further research.

3.1 Network Monitoring for Autonomic Communication

The system designed and implemented in 6QM is very useful to measure network performance parameters such as delay, jitter, and packet loss. However, it is for the moment restricted to manual operation. The network manager specifies the required measurement parameters via a web-based user interface, and underlying scripts issue the required measurement commands to the meters, calculators and other elements involved in the measurement. This is very useful for tasks that require off-line, occasional monitoring of network operation. It is not suitable to provide immediate reaction to anomalous behaviors caused by faults, attacks, abnormal traffic, wrong configuration, and so on. The time scales for ideal reactions to such events and to take the necessary corrective actions are largely beyond what humans could handle, especially in large, complex and heterogeneous networks.

Such reactive network elements require adaptive traffic and resource controllers that react to changing network conditions in an automatic and timely manner. In order to achieve this, network monitoring and measurement should be incorporated as an integral part of any network system, not as an afterthought. This is among the conclusions of the joint EU-NSF NeXtworking 2003 Workshop [Nextw2003], which discussed the technical challenges of future network technologies.

Going even beyond this, the Autonomic Communication Coordination Action [ACCA] is a recent EU-funded initiative to investigate and promote a new communication paradigm based on autonomic elements that self-organize into a coherent network structure following human input, but without requiring manual configuration and management. It fills in the gap between the Autonomic Computing initiative by IBM (which focuses on general computational and software engineering aspects) and D. Clark's high-level "Knowledge Plane" vision [Clark2003].

An Autonomic Communication Network (I) is made up of multiple autonomic elements, each of them containing controllers that make autonomous decisions based on high-level policies and sensed network conditions.

What would be necessary in order to make the 6QM system suitable to be incorporated as a sensor in IACN? First of all, the user interface would have to be eliminated, and replaced by a sensor configuration language that would enable sensors to be deployed and activated upon demand. The actual user interface would be situated at a much higher level iIhe ACN system, in which the user would specify the desired goals to be achieved and the rules It the ACN system should respect when implementing these goals.

The second issue to tackle is the export interface, where significant changes can be expected. The current export interface is based on massive data transfer to a database, where the data is typically analyzed by a human network manIr. In an ACN, sensor data is used as feedback information for autonomous controllers. In this context, it is neither practical nor efficient to export large amounts of data to be analyzed at a central place. A decentralized solution seems much more appropriate, in which sensor output is processed and filtered locally depending on the

goals provided by the requesting entities, and then possibly aggregated with the output from other sensors, in order to obtain the desired information that can be used in a control decision process. The exact way is which this can be achieved promises to be a rich subject of rIarch within ACN systems.

3.2 Multi-Homing

Multi-homing refers to a configuration of having connection through several service providers. The purpose of this practice is usually to offer better resiliency to failure or to allow some load balancing among several services. The Internet Draft [Multi6] presents an interesting list of scenarios for multi-homing in IPv6.

In the context of the QoS, failure can be interpreted as the non-compliance of the existing service to the SLA that is required by the customer or user application, which may result in the degradation of the application performance.

IPv6 QoS monitoring could certainly be used in the context of multi-homing to assist the service provider selection. In the context of those companies having connections to several ISP, the QoS monitoring could be used to monitor the service offered by the different ISP. The QoS monitoring system could also be bound to the network configuration (Figure 3-1).

For example the monitoring system would monitor each of the services and send this information to a system in charge of selecting the most appropriate service. In addition the QoS parameters, the selection algorithm could take as input other factors such as service price or service preference for example. Then in case the service in use needs to be reconfigured, a network configuration module would be called to realize the configuration changes.

As a consequence it could be possible to build an automated system to benchmark ISP and automatically reconfigure the network to use the best service according to criteria such as QoS, price etc.

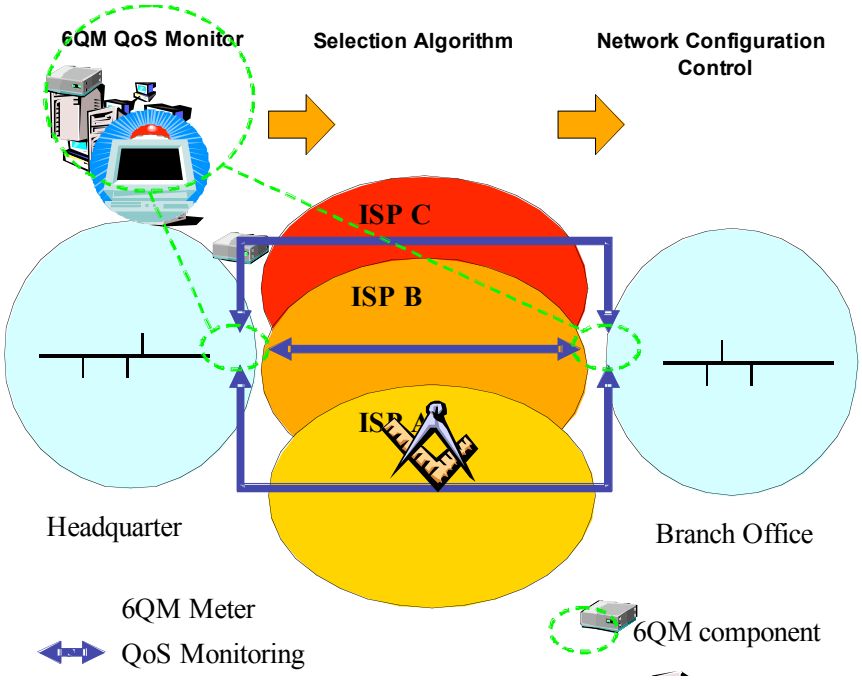

Figure 3-1: ISP Benchmark

A similar multi-homing scenario could be applied to the mobile environment a mobile device having the possibility to use GPRS/3G infrastructure and a WiFi access could use the QoS monitoring to determine which service provides the best connection for its application and then reconfigure its network connection to benefit from the best QoS (Figure 3-2).

Once again in this scenario other parameters are expected to be taken into account. This is especially true concerning the price which may really influence the behavior of the end user who may accept a lower QoS if the service is cheaper for him.

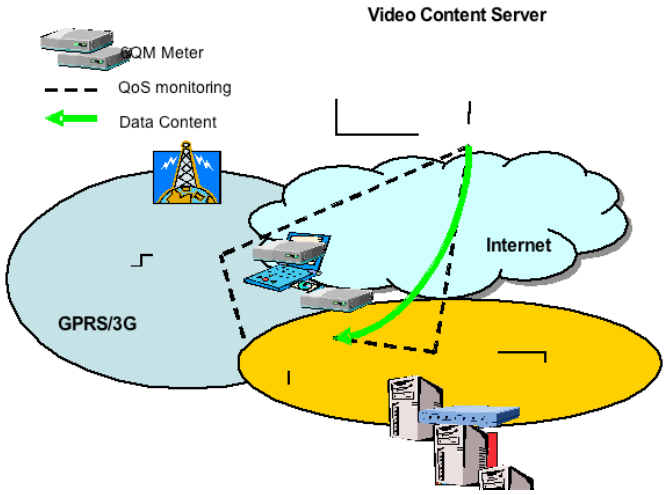

Figure 3-2: Monitoring and Mobile Multi-Homing

While thinking about such a usage of QoS monitoring in multi-homing context with automated configuration. Some issues would need to be investigated for the selection algorithm such as:

- The definition of parameters to be used in the selection algorithm
- The avoidance of instability in the system
- The limitation of system configuration latency

3.3 MPLS based Automated Network

Multi-protocol label switching (MPLS) is a framework defined by the Internet Engineering Task Force (IETF). MPLS architecture is defined by [RFC3031]. MPLS provides mechanisms independent from link layer and network layer technologies to enhance network performance. Basically MPLS is based on a label that is inserted between the link layer header and the network layer header of the packet. A MPLS router receiving such a packet examines the packet label content to determine the next hop. Once a packet has been labeled, its path through the backbone is determined by the label switching. Among other benefits, MPLS label allows the simplification of the packet forwarding through routers and also the definition of explicit path setup enabling traffic engineering.

In the context of MPLS usage there could be some interesting combination between QoS monitoring and MPLS configuration. Indeed to maintain the SLA required by a running application it would be interesting to investigate the possibility of QoS monitoring as an input for MPLS path control and reconfiguration.

The Figure 3-3 illustrates this idea:

- There is a video traffic between the server and the client through R1, R2, R3

- Then some failure in the measured QoS is detected by the monitoring system ("QoS Monitor")
- The system identifies the segment having some bad performance.
- The monitoring information is then submitted to an engine ("MPLS Configuration Algorithm") in charge of finding the appropriate new path configuration satisfying the QoS requirement.
- Once a new configuration is computed the configuration is performed by the "MPLS Path Control" module.
- Hopefully at the end of this process the new path satisfies the QoS requirement of the application.

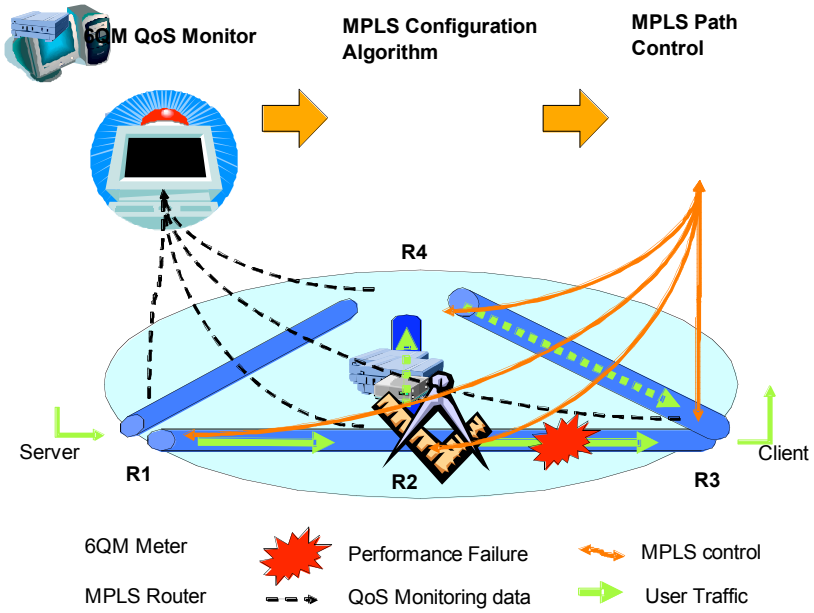

Figure 3-3: Monitoring and MPLS

A dynamic auto-configurable system would be very interesting however such a system would present many challenges and issues to be solved. The following of this section points out some issues.

Once the path is detected as not conforming to the QoS requirements how to determine a new path satisfying those requirements? This would certainly require monitoring the other existing path and sub-path to check their availability and the QoS they can offer for some extra traffic.

The configuration of the path certainly needs to be global. Indeed the change of one path may affect other traffic in a negative way that does create QoS failure on other paths. As a consequence a reconfiguration should globally satisfy the maximum of existing flows. This would require some prediction model on the expected QoS for the new configuration.

Then the question of the scalability is raised, because a solution that provides good results on a simple topology may be inappropriate for a larger topology. This is especially an issue here as the new configuration needs to be globally satisfying for the maximum number of existing flows. So there is a need to build an algorithm that is scalable for large networks.

In this scenario there is also a constraint about the metering system scalability concerning packet-processing capability as the meters may have to deal with high packet rates.

Moreover one can think about other relevant issues such as system instability, or the limitation of configuration latency.

A combination of MPLS and QoS monitoring for auto-configured network would be very challenging and raises many interesting issues.

3.4 Application Monitoring

The research realized by the consortium was focused on IPv6 measurement. IPv6 thanks to its large number of addresses is expected to ease the development of end-to-end services such as voice over IP (VoIP) or videoconference systems. The work performed was focused on network layer QoS however it would be also interesting to go above network layer in order to measure the behavior of the application itself in other words the QoS parameters specific to the considered applications. The following of the section illustrates this idea with VoIP services using H.323.

H.323 standard provides a foundation for audio, video, and data communications across IP-based networks. H.323 is a recommendation from the International Telecommunications Union (ITU) that sets standards for multimedia communications. It is a family of specifications including– parts of H.225.0 - RAS, Q.931, H.245 RTP/RTCP and audio/video codecs, such as the audio codecs (G.711, G.723.1, G.728, etc.) that compress and decompress media streams. H.323 defines important building blocks for the creation of multimedia communications. The figure below presents an exemplary message exchange for a successful direct end point call assisted by Gatekeeper.

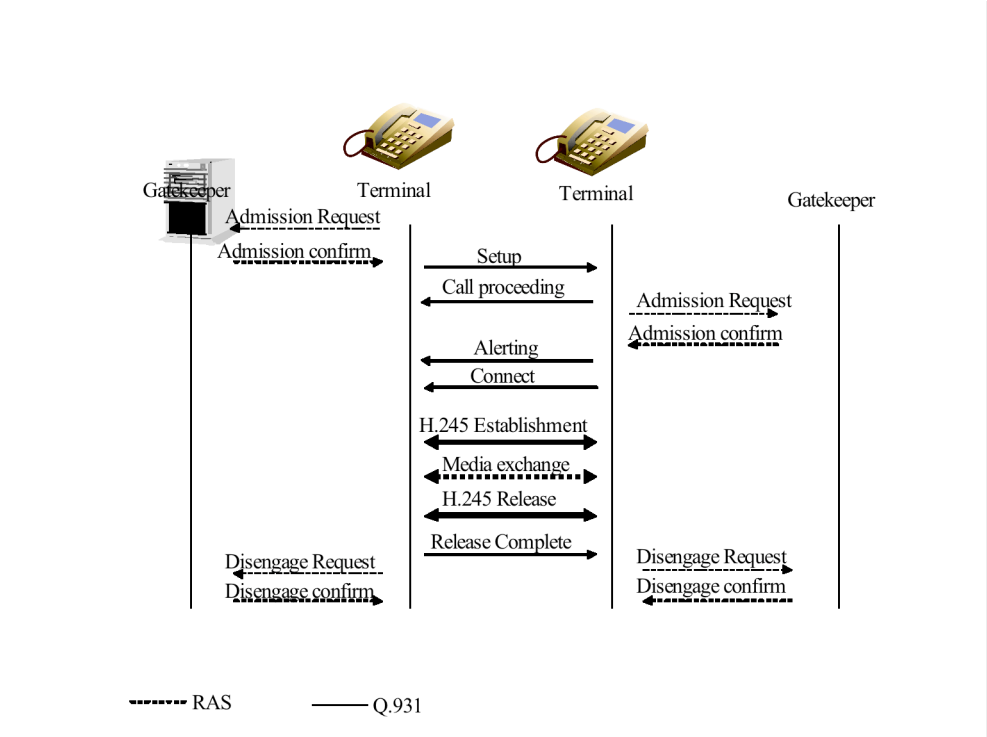

Figure 3-4: Direct End Point Call Establishment using H.323 and Gatekeeper

In the case of the VoIP one interesting point would be the binding between the call manager and the QoS system in order to setup the appropriate measurement environment when a call is setup.

Moreover, a network level QoS monitor would investigate the performance of the voice service between the two terminals by monitoring the IPv6 packet delay, jitter or loss however the voice application presents its own QoS characteristics of interest such as:

- The blocking probability of a call.
- The delay between "setup" command transfer and "connect" command reception.
- The overall setup delay between the admission request and voice channel establishment.

Such information is very important to characterize the application behavior. In order to evaluate those values, the meter would need to analyze the packets that are captured and interpret the content of the message as a consequence this would require:

- The support of additional protocols above network layer.
- The creation of some state in the meter.

Another specific aspect of application monitoring and examination of application behavior is the measurement of service availability. For applications that are based on a server-client model, it is vitally important that a necessary service is a reachable and working. A Service Level Agreement might contain guaranties concerning access to a set of working services.

Such agreements could range from a guaranteed available access to the Internet or any other resource offered by an external service provider. If for instance a groupware solution is outsourced to an external party then a service user will certainly be interested to verify that the contractor maintains the bought service available as agreed in the contract.

Availability is normally quantified as a quotient ranging from zero to one or as a percentage and is determined as follows: $Availability = \frac{MTBF}{MTBF + MTTR}$ where MTBF is the mean time between failure and MTTR is the mean time to repair.

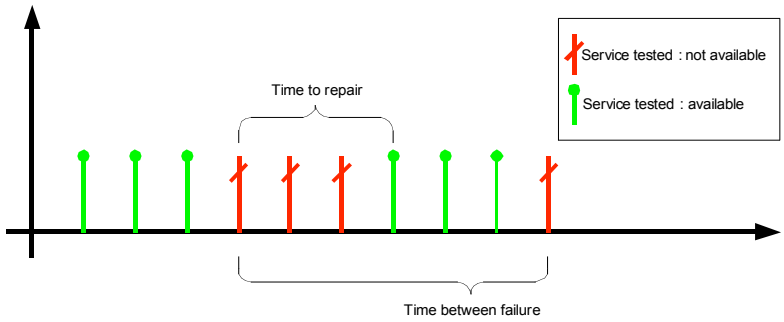

Figure 3-5: Availability terms

In a basic scenario probes periodically or randomly test certain aspects of the availability of services that are important for business processes of a fictive enterprise. Among those tests, probes examine and log availability of Web servers, Email and Fax servers et cetera as depicted in Figure 3-6. An interesting aspect thereof is to expose actual causes for unavailability by breaking down network path at "hot spots". Referring to Figure 3-6 the cause for unavailability of the services that is experienced by a user could be in fact a router problem.

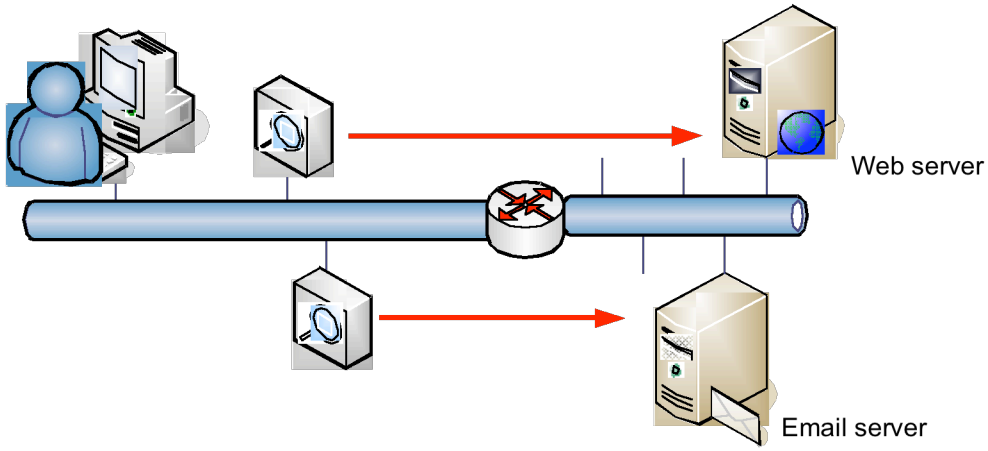

Figure 3-6: Probes testing services

Those additions would increase the complexity of the meter however the gain would be to have in a single system analyzing both the network QoS and the application QoS. This would help to understand easily why an application is not working by distinguishing network problems from application problems. These additional functions would be customized according to the target application.

4. SUMMARY AND CONCLUSIONS

This deliverable is the closing deliverable of WP3. During the 6QM project many aspects of the IPv6 QoS measurement have been addressed. This document identified areas where further research could be performed in the future.

According to our opinion the further research should improve the QoS measurement system itself. In addition, in this deliverable we also identified some areas where the QoS measurement could be applied to bring additional results or benefits to the overall service and user experience.

Many areas remains opened in the field of the QoS monitoring. However one very important aspect that is pointed out in this document is the possibility to integrate core measurement components into existing system such as control and configuration systems. This integration could really bring benefit to the community. This could really promote the usage of the measurement in various environments.

5. REFERENCES

[ACCA] Autonomic Communication, http://www.autonomic-communication.org/

[Braden2002] Braden, R., Faber,"T., Handley, M., "From Protocol Stack–o Protocol Heap -- Role-"ased Architecture". HotNets-I, Princeton, NJ, October 2002.

[Clark2003] David D. Clark, Craig Partridge, J. Christopher Ramming, John T. Wroclawski, "A Knowledge Plane for the Internet", Proc. of ACM SIGCOMM 2003, Karlsruhe, Germany, August 2003.

[Clark2003b] Clark, D., Braden, R., Falk, A.,"and Pingali, V., "FARA: Reorganizing the Addre"sing Architecture". Proc. ACM SIGCOMM 2003 FDNA Workshop, Karlsruhe, Germany, August 2003.

[ClassiPI] PMC-Sierra, Inc. http://www.pmc-sierra.com/products/details/pm2329/

[diameter] Diameter home page: http://www.diameter.org

[DrNSIS] draft-dressler-nsis-metering-nslp-00.txt

[Endace] Endace Measurement Systems; http://www.endace.com/default.htm

[EZCHIP1] 7-Layer Packet Processing: A Performance Analysis (White Paper); http://www.ezchip.com/images/pdfs/ezchip_7layers.pdf

[EZCHIP2] IPv4 to IPv6 is Not Merely 50% More (White Paper); http://www.ezchip.com/images/pdfs/EZchip%20IPv6%20white%20paper%20v1.01.pdf

[infoCom] Information and Communications in Japan 2003

[CORAL] libcoral - a C API for CoralReef; http://www.caida.org/tools/measurement/coralreef/doc/doc/libcoral-c.html

[Newarch] NewArch Project: Future-Generation Internet Architecture, http://www.isi.edu/newarch/

[Nextw2003] Ioannis Stavrakakis, Ibrahim Matta, Michael Smirnov (editors), "Report on the COST (EU) - NSF (USA) Workshop on Exchanges & Trends in Networking (NeXtworking'03)", http://cgi.di.uoa.gr/~nextwork/nextworking2003/, July 2004.

[MPHPT] http://www.soumu.go.jp/joho_tsusin/eng/

[Multi6] J. Palet et Al, "Analysis of IPv6 Multihoming Scenarios", IETF internet draft, draft-palet-multi6-scenarios-00.txt, expiration Date: January 10, 2005

[RFC3031] E. Rosen et Al., «Multiprotocol Label Switching Architecture", RFC3031, January 2001

[RFC3775] D. Johnson et Al., « Mobility Support in IPv6 », RFC3775, June 2004

[Yama2004] Lidia Yamamoto, « Automated Negotiation for On-Demand Inter-Domain Performance Monitoring », In Proceedings of 2nd International Workshop on Inter-Domain Performance and Simulation (IPS 2004), Budapest, Hungary, March 2004.