

# QoS Oriented Measurement in IP Networks

Vladimír Smotlacha

December 15, 2001

## Abstract

This report brings overview of QoS specification in IP networks. It focuses on the measurement of QoS related characteristics and introduces the method of multipoint passive measurement.

## Keywords

IP, QoS, active measurement, passive measurement, SLS, time synchronization

## 1 Introduction

Quality of Services (QoS) is one of the greatest challenges in IP networking and in Internet generally. The aim of QoS is to satisfy different service requirements by sharing the same infrastructure. QoS offers the ability to define qualitative (e.g. class of service) or quantitative (e.g. bandwidth) attributes of network service provided. Definitely, consistent and predictable behaviour of the communications channels is expected.

Network monitoring and measurement is increasingly regarded as an essential function for developing and supporting high-quality network services, building and improving innovative networking technologies, and analysing infrastructure trends and user behaviour. For supporting QoS-enabled services, traffic engineering and network operation, monitoring is needed to provide the feedback to operators or management systems in an efficient fashion. Monitoring is also crucial in the development, optimisation and testing of innovative networking technologies by providing the required knowledge on the infrastructure characteristics, traffic phenomena and system/network performance.

While effort in this area has resulted in a wide variety of hardware and software monitoring tools, demand for faster and more flexible monitoring and measuring technology is continuously growing far beyond what can be currently offered. The report is organized as follows. Section 2 introduces basic methods of QoS implementation. Section 3 describes Service Level Specification as an interface

between service user and service provider. Section 4 contains definition of QoS parameters according to the IETF and ITU-T. Current standardization and implementation activities of Classes of QoS are described in Section 5. Section 6 summarizes current methods of measurement in IP networks. Our method of QoS oriented measurement is described in Section 7.

## 2 QoS in IP Technology

In this section we shall discuss two approaches of QoS specification in IP technology: Intserv and Diffserv. Although QoS is not primary consideration of MPLS, we note here MPLS too because it introduces an effective and scalable identification of particular data flow which is basic condition for offering QoS.

### 2.1 Integrated Services

Intserv (Integrated Services) [RFC1633] extent the basic service model of IP and introduces new services to provide fine-grained assurances to individual flows:

- The **Controlled Load Service** [RFC2211] offers the same quality of service like the unloaded or lightly loaded network with the Best Effort service. Network resources are reserved for each particular data flow and therefore committed flows do not overload data network nodes. This service does not guarantee any quantitative parameter.
- The **Guaranteed Service** [RFC2212] offers quantitative upper limit on latency to flows conforming to a traffic specification. The principle is to reserve the bandwidth and the queue of known length for each data flow in each network node. This service is similar to a dedicated wire.

Intserv introduces the principle of connectivity to the connectionless IP technology. To establish a channel, signaling is essential. Usually, Intserv is associated with the RSVP signalling protocol [RFC2205]. As Intserv requires state information about any flow in each network router, scalability is a problem.

Intserv is not widely used and it seems not to be perspective framework for QoS in IP networks. For this reason it will not be further considered in this paper.

### 2.2 Differentiated Services

Diffserv (Differentiated Services) [RFC2475] is a layer 3 framework to provide control to aggregates of flows. As flows are recognized only at edge devices of domain (ingress and egress nodes), no state information per flow is required in other routers inside the Diffserv domain. Flows are classified at the edges, and then they are conditioned and aggregated. Each IP packet obtains a Diffserv Codepoint (DSCP), which identifies a per-hop behaviour (PHB). As the size of DSCP is 6 bits, at most 64 different PHB exist and 32 of them are subject of standardization. Three types of PHB are currently defined:

- The **class selector PHB** [RFC2474] subsumes the IP precedence model of the former ToS octet according [RFC791] and [RFC1122].

- The **Assured Forwarding** (AF) [RFC2597] offers different levels of forwarding for packets belonging to an aggregated flow. Network sources are allocated independently for each AF group. 4 AF classes are identified (Premium, Gold, Silver and Bronze), each with 3 levels of drop precedence. Not all of 12 AF classes have to be implemented.
- The **Expedited Forwarding** (EF) [RFC2598] guarantees tightly bounded delay, delay variation and loss ratio for conforming IP packets. The implementation requires that any router satisfies the condition, that the aggregate input flow does not exceed minimum output bandwidth. From an end-user viewpoint, EF emulates the virtual circuit.

### 2.2.1 DS Codepoint Field

DS Codepoint occupies the second octet of IP header, which was formerly called ToS (Type of Services). The history of this octet interpretation maps the evolution of different services offering in IP technology.

In early [RFC791] is introduced the structure of ToS with 3 bit of precedence level and others 3 bits (called DTR bits) for specifying normal or better value of delay, throughput and reliability. While [RFC1122] adopts the definition of 3 bits of precedence, [RFC1349] introduces 4 new types of services: minimize delay, maximize throughput, maximize reliability and minimize monetary cost. This concept is incompatible with Diffserv. Figure 1 and Figure 2 show difference between the original ToS octet and DS codefield.

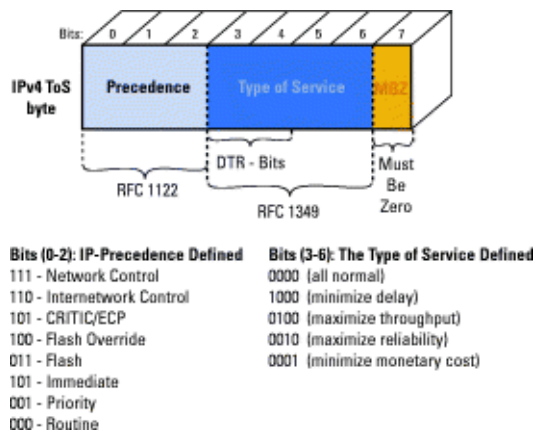


Figure 1: Original ToS Octet

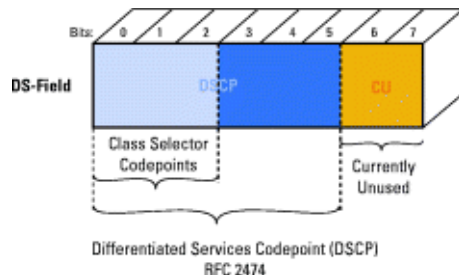


Figure 2: Diffserv Codepoint Field

## 2.3 Multiprotocol Label Switching

MPLS (Multiprotocol Label Switching) [RFC3031] is a technology which replaces packet routing by packet switching. It is based on the fact that packet routing consists of two phases: header analyzing and choosing the next hop. The first function partitions the entire set of possible packet headers into a set of FECs (Forwarding Equivalence Classes). The second one maps each FEC to a next hop. As far as the forwarding decision is concerned, different packets which get mapped into the same FEC are indistinguishable. All packets which belong to a particular FEC and which travel from a particular node will follow the same path.

The assignment of a particular packet to a particular FEC is done just once, as the packet enters the network. The FEC to which the packet is assigned is encoded as a short fixed length value known as a *label*. The label may optionally specify the Class of Services, too. When a packet is forwarded to its next hop, the label is sent along with it. At subsequent hops, there is no further analysis of the packet header. Rather, the label is used as an index into a table which specifies the next hop and a new label. The old label is replaced with the new label, and the packet is forwarded to its next hop.

## 3 Service Level Specification

Service Level Specification (SLS) concerns the problem of how to exactly specify the network service and the corresponding context. This specification should be a part of the Service Level Agreement (SLA) between the service provider and the service user. SLS has a negotiation phase with its own protocol, when the service is requested and acknowledged or rejected, and a provisioning phase, when the service is used in negotiated range.

SLS contains the following parts:

- scope of the provided service,
- data flow identification,
- conformance parameters and tests of conformity,
- excess traffic processing,
- guaranteed service class and QoS parameters, and
- service schedule.

### 3.1 Scope of provided services

The scope of SLS indicates where the service will be used. It includes ingress and egress nodes and the topology: pipe model (one-to-one), hose model (one-to-many or one-to-all) and funnel model (many-to-one or all-to-one).

### **3.2 Data flow identification**

The flow identification of a SLS indicates for which IP packets the service is enforced. The IP datagram stream is identified this way as one or combination of several of the following attributes:

- source - IP address, set of IP addresses,
- destination - IP address, set of IP addresses,
- application - protocol number, source port, destination port, and
- DSCP - differentiated services code point.

### **3.3 Conformance parameters, tests of conformity**

The conformance testing is the set of actions which uniquely identifies the *in-profile* and *out-of-profile* packets of the IP stream. It is usually done at an ingress node. The non-exhaustive list of the conformance parameters includes:

- peak rate,
- token bucket rate,
- token bucket depth,
- MTU (Maximum Transfer Unit), and
- minimum packet size.

Algorithms of the conformance tests include:

- peak rate measuring,
- token bucket algorithm,
- single rate three color marker [RFC2697], and
- two rate three color marker [RFC2698].

Prior to entering the conformance tests, some actions with data stream could be done according to SLS. The reason is to modify IP packets or the stream to pass strict conformity tests. This action includes e.g. assigning DSCP value which is done at the entry to diffserv domain, or even data stream shaping.

### **3.4 Excess traffic processing**

IP packets, which are *out-of-profile*, are treated according to the SLS. There are three usual methods:

- dropping - the packet is simply dropped,
- shaping - the packet is delayed until it is *in-profile*, and
- remarking - the packet is marked by a particular DSCP.

### 3.5 Guaranteed QoS parameters

The performance guarantees that the network offers for particular service are expressed by a set of QoS parameters and their values. Possible values can be quantitative, i.e. numeric, or qualitative, e.g. "low / medium / high".

To give an example, the project Tequila [TEQ] assumes a set of four parameters, which is now a subject of standardization [SLS]:

- delay - expressed either as the worst case bound (e.g. delay is less than 100 ms) or as the quantile (e.g. delay is less than 20 ms for 98 % of packets during 5 minutes),
- delay variation (jitter) - is expressed either as the bound or as the quantile,
- packet loss ratio, and
- throughput.

## 4 QoS Parameters

Two approaches of QoS parameters definition currently exist. ITU-T, be in general Recommendation I.350 [I350] or for IP in Recommendation I.380 [I380], adopts a statistical probabilistic definition for the QoS parameters. Contrary to this, IETF documents are based on deterministic philosophy. The principal document is *Framework for IP Performance Metrics* [RFC2330].

As the typical user is not concerned about how the service is provided, the QoS is expressed from his point of view by parameters which:

- focus on the user-perceived effects,
- definition is not dependent on the assumption about the network internal design,
- can be objectively measured at the service point, and
- are described in network independent terms.

### 4.1 QoS parameters in ITU-T

Document [I350] identifies three basic functions (phases) of the communication: access, user information transfer and release of connection. Performance criteria are also three: speed, accuracy and dependability:

- speed - describes the time interval that is used to perform the function or the rate at which the function is performed,
- accuracy - describes the degree of correctness with which the function is performed,
- dependability - describes the degree of certainty (or surety) with which the function is performed regardless of speed or accuracy, but within a given observation interval.

Matrix 3x3 identifies a total of 9 Parameters of Performance (PP) combining each function and each performance criteria. The PP may be primary, such as delay, or derived, such as availability of the system. The derived PPs are obtained via decision threshold of the relevant primary PP.

Performance Criteria	QoS Parameters
speed	delay throughput
accuracy	probability of error probability of mis-insertion
dependability	probability of loss

**Table 1:** Performance criteria and QoS parameters

Document [I380] identifies for IP the set of performance parameters similar way as in ATM. The differences are mainly due to the connectionless nature of IP and the possibility of packet fragmentation. The connectionless principle implies that fragments of the same packet may be routed differently. The first step is to define four types of IP packet transfer outcomes:

- successfully transferred  
The packet (all fragments of packet) is delivered to the destination within  $T_{max}$  with valid header and no error of content.
- errored packet outcome  
The packet (or any of its fragments) reaches the destination within  $T_{max}$  with either corrupted header or error in binary contents.
- lost  
The packet (or any of its fragments) is never delivered to the destination or is delivered after  $T_{max}$ .
- spurious  
The received packet was misinserted.

Using these types of outcomes, the following performance parameters are defined:

- IP packet transfer delay (IPTD)  
IP packet transfer delay is defined for all successful and errored packet outcomes. The value is  $(t_2 - t_1)$ , where  $t_2 > t_1$  and  $(t_2 - t_1) < T_{max}$ . If the packet is fragmented,  $t_2$  corresponds to the last fragment.
- mean IP packet transfer delay  
Mean IPTD is the arithmetic average of IPTD for a population of interest.

- IP packet delay variation (IPDV)

The 2-point packet delay variation is the difference between the absolute IP packet transfer delay and defined reference IPTD. An average packet transfer delay may be used as reference.

- IP packet error ratio (IPER)

IP packet error ratio is the ratio of total errored IP packet outcomes to the total of successful IP packet transfer outcomes plus errored IP packet outcomes in a population of interest.

- IP packet loss ratio (IPLR)

IP packet loss ratio is a ratio of total lost IP packet outcomes to total transmitted IP packet in population of interest.

- spurious IP packet rate

Spurious IP packet rate is the total number of spurious IP packet observed during a specified time interval divided by the time interval duration.

ITU-T currently defines no flow or throughput related parameters. However, two such parameters are proposed in the appendix of [I380]:

- IP packet throughput (IPPT)

IP packet throughput is the total number of successful IP packet transfer outcomes during a specified interval divided by the time interval duration.

- octet based IP time packet throughput (IPOT)

The same case as above but number of octets in packets is used instead of number of packets.

## 4.2 QoS parameters according to the IETF

In the IETF, the IP Performance Metric Working Group (IPPM WG) is organized, which represents the standardization initiative. The goal of the document *Framework for IP Performance Metrics* [RFC2330] is to introduce a set of standard metrics to provide quantitative characteristic of network and to let the Internet users and Internet providers understand the performance and reliability of both end-to-end paths and IP clouds.

### 4.2.1 Definition of metrics

The term metric is not used here in the strict mathematical meaning, it is understood as a carefully specified quantity related to the performance and the reliability of operational Internet. Metric has to be defined in terms of standard units of measurement (e.g. meters, seconds or bits). In definition of metric, stochastic terms (probabilities) should be avoided. E.g. instead of metric "packet loss probability between A and B" should be used "packet loss rate between A and B" (the result may be "0.03" for the first definition, "3 packets from 100" for the second one). The reason to distinguish between these two

definitions is, that a hidden assumption about a stochastic model of the behavior being measured is often included in probabilities. The fundamental goal is to avoid definition biasing by these hidden assumptions. An example of such hidden assumption might state that packet loss in a network component due to queuing overflow can be described as something that happens to any given packet with a particular probability. Such model can obscure crucial correlation between queuing drops among a set of packets.

The distinction between stochastic and deterministic approaches concerns only the definitions of metrics. It is not applied to techniques used to analyze the results of measurements.

Metric definition has to contain exact specification of packets used to make the measurement. [RFC2330] suggests that metric's name should include a type of packet whenever metric's value depends on it. Unless otherwise stated, the packet is *standard formed*, which means that it satisfies the following criteria:

- the packet is not a fragment,
- the length given in the IP header corresponds to the size of IP header plus the size of the payload,
- it includes valid IP header,
- the TTL is 255, and
- it does not contain any IP options.

A special type of the *standard formed packet* is the *minimal IP packet* whose payload is 0 bytes.

A fundamental property of many Internet metrics is that the value of the metric depends on the type of IP packet used to make the measurement. Because of this distinction, generic notion of a *packet of type P* is introduced, where in some contexts P will be explicitly or partially defined or left generic.

Internet measurement is often complicated by the use of Internet hosts themselves to perform the measurement. These hosts can introduce delays, which have nothing to do with the network behavior we would like to measure.

This problem is particularly acute when timestamping of network events occurs at the application level. Time which is got this way we call *host time*. In order to provide a general way of eliminating the host influence, two notions of *wire time* are introduced. These notions are only defined in terms of an Internet host H observing an Internet link L at a particular location:

- For a given packet P, the *wire arrival time* of P at H on L is the first time T at which any bit of P has appeared at H's observational position on L.
- For a given packet P, the *wire exit time* of P at H on L is the first time T at which all the bits of P have appeared at H's observational position on L.

#### **4.2.2 Metric specification**

- analytical metric specification

The Internet community has developed a common analytical framework (called *A-Frame*). The major objective is to get network characterization consistent in both analytical and practical settings so that a non-empirical study could be correlated with real network behaviour. A - Frame concept is intended to abstract from real Internet components so that:

- essential function of components is retained,
- properties relevant to particular metric are retained, and
- non relevant properties are dropped.

Examples of analytically defined metrics:

- propagation time of a link,
- bandwidth of a link for packet of size  $k$ ,
- hop count of a route.

- empirical metric specification

Some metrics do not fit into A-Frame terms because the A-Term lacks the detail or power of the real system. The metric can be still well specified by describing a reference methodology to measure it.

Empirical metrics have the following properties:

- there has to be a clear definition in terms of Internet components,
- there has to be an effective means to measure them, and
- there should be (maybe incomplete) understanding of the metric in A-Frame terms.

### **4.2.3 Composition of metrics**

Composition is some form of extrapolations of metric. The effectiveness of composition depends on analyzes of relationships between relevant A-Frame components and on correspondence with measurement methodology. Two distinct types of composition are recognized:

- spatial composition

Spatial composition is a characteristic of the metric which can be applied to paths and subpaths and for which A-Frame concept suggests useful relationship between the metric applied to subpaths (including a complete path). An example is the assumption that delay of a path is close to sum of delays of all appropriate links and routers.

- temporal composition

Temporal composition is a characteristic of the metric for which A-Frame concept suggests useful relationship between metric applied at time T and at set of earlier times. A simple example is flow capacity during a 5 minute period.

#### 4.2.4 Notions of metrics

Metrics can be classified according to the way of measurement repeating:

- singleton metric

The metric is a single (atomic) instance of measurement.

- sample metric

A number of distinct instances of singleton metric is performed. The reason is to see the variations and the consistency in the metric.

- statistical metric

The metric is derived from sample metric by computing the statistics of the obtained values of singleton metric. An example is a mean value.

The way of collecting samples is a part of metric specification. We describe three common methods here:

- periodic sampling

Sampling is repeated at fixed time intervals. There are several disadvantages of this method: sampling is easily anticipated, only a part of periodic behavior can be observed and even the network might be moved into a synchronization state when the measurement affects it.

- random additive sampling

Samples are separated by independent, randomly generated interval with statistical distribution  $G(t)$ . This approach avoids synchronization but complicates frequency-domain analysis. Unless  $G(t)$  is an exponential distribution, sampling remains predictable. Therefore, *Poisson sampling* with distribution function  $G(t) = 1 - e^{-\lambda t}$  of probable interval length, plays a special role. As exponential distribution is unbounded, it is desired to limit the longest interval by some reasonable maximum value.

- geometric sampling

External events are measured with a fixed probability  $p$ . Geometric sampling is unbiased and not predictable. An example would be capturing all packets over a link, while only these are recorded if a randomly generated number uniformly distributed between 0 and 1 is less than given  $p$ .

#### 4.2.5 Clock issues

Measurement of time is a base of many metrics. It is necessary to study errors introduced by an imperfect clock.

The *Network Time Protocol Specification* [RFC1305] includes a nomenclature for clock characteristics. Let the clock report time  $T_c$  while true time (UTC) is  $T_t$ . We can define absolute issues (with respect to UTC):

- offset

offset is the difference between local and true time:  $offset = T_c - T_t$ ,

- skew  
skew is the change of offset in time, i.e. the first derivative of offset,
- drift  
drift is the variation of skew in time, i.e. the second derivative of offset,
- accuracy  
the clock is accurate at particular moment if the offset is zero, i.e. accuracy says how close the offset is to zero,
- precision  
precision is the smallest unit in which clock reports time,
- resolution  
the smallest unit by which the clock is updated, and
- synchronization  
two clocks are synchronized if they are accurate with respect to one another.

Relative offset, relative skew and relative accuracy are defined as related to another clock instead of true time. As number of metrics involves comparing of time reported by two different clocks, the process of computing the difference removes any error due to clock inaccuracies with respect to true time. Therefore these relative characteristics are important for description of both clocks.

The requirement of measurement methodology often starts with assurance that clocks are synchronized and have minimal relative skew and drift. The clock can derive their time using network time synchronization protocol such as NTP [RFC1305, Mil97].

NTP is based on a request/response principle when timestamps exist for both sending and receiving.

Let we call client station A and server B, than  $t_0$  - time of sending request (relative to clock A)  $t_1$  - time of receiving request (relative to B)  $t_2$  - time of sending response (relative to clock B)  $t_3$  - time of receiving response (relative to A)

Assuming symmetrical behaviour of network, e.g. the same one-way delay in both directions, the offset between clocks A and B is

$$offset = ((t_0 + t_3) - (t_1 + t_2)) / 2$$

and round-trip delay (from which maximal error can be derived)

$$delay = (t_3 - t_0) - (t_2 - t_1)$$

System NTP uses delay and offset (computed from formulas given above) for synchronizing client's clock to that of a server.

## 4.3 Metrics for IPPM

### 4.3.1 IPPM Metric for Measuring connectivity

Connectivity is the basic assumption of any Internet service. In [RFC2678], several one-way and two-way connectivity metrics are defined. The unit of any connectivity metric is a Boolean value. The simplest instantaneous one-way connectivity metric is defined as an event 'packet transmitted at time  $T$  from source reaches its destination'. The interval connectivity metric is derived from existence of instantaneous connectivity in at least one time during the interval. Finally, the interval temporal connectivity metric defines what we naturally understand as a useful two-way connectivity: Times  $T_1$  and  $T_2$  and intervals  $dT_1, dT_2$  exist, such that  $T_1 + dT_1 < T_2$ , at  $T_1$  has Src instantaneous connectivity to Dst, at  $T_2$  has Dst instantaneous connectivity to Src and packet, which was sent at  $T_1$  (resp.  $T_2$ ) arrived at  $T_1 + dT_1$  (resp.  $T_2 + dT_2$ ).

### 4.3.2 One-way Delay Metric for IPPM

The one-way delay metric, as defined in [RFC2679], is one of the basic quantitative characteristics of the network propagation delay. It is preferred to round-trip delay as there may be a significant asymmetry in paths to the destination and back to the source and even if the two paths are symmetric, they may have different performances due to queuing. The metric is defined as the difference between wire-time of first bit of the *Type-P* packet at the transmitter and wire-time of the last bit at the receiver. The metric involves an upper bound of delay and says that packet is considered lost and the value of metric is undefined if the last bit does not arrive within that predefined period of time. If the packet is fragmented and if, for whatever reason, reassembly does not occur, the packet will be deemed lost. Note that measuring one-way delay requires clock synchronization between the sender and receiver. Given the derived sample metric, several statistics of sample may be defined: minimum, medial, percentile and inverse percentile.

### 4.3.3 Round-trip Delay Metric for IPPM

Type-P Round-trip Delay metric is defined in [RFC2681] the following way: at wire-time  $T$ , the first bit of the Type-P packet from Src to Dst is sent, after receiving the packet at Dst, a Type-P packet back to Src is sent immediately. The last bit of packet is received at wire-time  $T+dT$ .  $dT$  is value of round-trip delay. Again, an upper bound of delay is given. If the packet does not arrive inside this interval, it is considered lost and the value of metric is undefined. As time is measured only at one site, round-trip delay is not an issue of the clock synchronization between Src and Dst.

### 4.3.4 Packet Loss Metric for IPPM

Type-P One-way Packet Loss metric is defined in [RFC2680]. The packet is considered lost if fails to arrive to destination in reasonable period of time. This time threshold is parameter of metric. Corrupted packets are counted as lost. The measurement methodology relies on the one-way delay.

### 4.3.5 IP Packet Delay Variation Metric for IPPM

The definition of IP packet delay variation metric (ipdv) is still a work in progress. In Internet-Draft [IPDV1], the ipdv is based on one-way delay metric and is defined as the difference in delay between two consecutive packets. If any of one-way delays is not defined, the value of ipdv is undefined, too. Based on ipdv samples (Poisson stream), some statistics are suggested: distribution of values, percentile, inverse percentile, jitter and peak-to-peak ipdv.

## 4.4 ipdv and IPDV comparison

Packet delay variation is defined differently in IETF and ITU-T. The relationship between ipdv and IPDV (i.e. 2-point delay variation as defined by ITU-T) is studied in [IPDV0] (former version of [IPDV1]):

- from ipdv to IPDV

Suppose that an arbitrarily chosen packet  $P_0$  is start packet of the ipdv measurement sequence. Given ipdv measurements for a series of packets, the IPDV is

$$IPDV(k) = IPDV(0) + \sum_{i=1}^k ipdv(i)$$

- from IPDV to ipdv

Given a sequence of IPDV measurements, the ipdv value for a pair of packets  $P_{k-1}$  and  $P_k$  is

$$ipdv(k) = IPDV(k) - IPDV(k - 1)$$

## 5 Classes of QoS

Classes of QoS services are a qualitative description of network services. Classes unify two approaches: application viewpoint where some general requirements on service type are identified, and the ability of network technology to provide and guarantee that service. QoS classes in IP are not standardized yet.

### 5.1 Service Classes according to the ITU-T

Although adopting of the model of ATM QoS services is impossible in IP, ITU-T has a proposal, which is inspired by ATM [Y1541]. It identifies 4 classes: real-time, interactive, non-interactive with guaranteed parameters and unspecified class. Table 2 contains typical values of performance parameters for particular classes.

### 5.2 Service classes in the IETF

In IETF no official definition of QoS classes exists. However, there is an initiative to bind the values of QoS parameters to several groups according to range of these values. One such proposal is given in [SEQ] and [GEA] (the origin is probably in [Camp]) which is based on following the consideration:

	Nature of the network performance objective	Default objectives	<b>Class 0</b> (real-time)	<b>Class 1</b> (interactive)	<b>Class 2</b> (non-interactive)	<b>Class 3</b> (U class)
<b>IPTD</b>	Upper bound on the mean IPTD	No default	150 ms	400 ms	1 s	unspec.
<b>IPDV</b>	Upper bound on the $1 - 10^{-4}$ quantile of IPTD minus the min. IPTD	No default	50 ms	50 ms	1 s	unspec.
<b>IPLR</b>	Upper bound on the packet loss probability	No default	$1 * 10^{-3}$	$1 * 10^{-3}$	$1 * 10^{-3}$	unspec.
<b>IPER</b>	Upper bound	$1 * 10^{-4}$	default	default	default	unspec.
<b>SPR</b>	Upper bound	not yet defined	default	default	default	unspec.

**Table 2:** ITU-T IP QoS classes

- *best effort* service, as is usually considered, does not correspond to a set of unbounded values of all QoS parameters. In general, for a usable service, at least delay, bandwidth and packet loss should have a defined value,
- for each parameter the values, when bounded, are restricted in just one direction,
- the parameter variation values can be divided into four ranges: single value, short, medium and wide range, in decreasing order of QoS provisioning. *Single value* (SV) represents the minimal lower bound for the parameter.

	<b>Single value (SV)</b>	<b>Short Range</b>	<b>Medium Range</b>	<b>Wide Range</b>
<b>One-way delay</b>	Measured value at empty network	less then SV + 50 ms	less then SV + 250 ms	less then SV + 10 s
<b>ipdv</b>	Between 0 and time full size packet transmit at line speed	25 ms	50 ms	none
<b>Packet loss</b>	0	$< 10^{-4}$	$< 10^{-3}$	$< 0.1$
<b>Bandwidth</b>	Fixed value; allow for a burst of one MTU size packet	n.a.	n.a.	at least one full size packet per second

**Table 3:** Proposal of IETF QoS parameters values range

Using this proposal (Table 3), a useful exercise is to map some common QoS services to given ranges of values. The mapping, as was evaluated in [SEQ], is given in Table 4. Services Prioritized Bandwidth and Guaranteed Bandwidth are in the project SEQUIN merged for simplicity into new class IP+. Definition of IP Premium and IP+ classes according project Sequin is given later in this text.

	Best Effort	Less than Best Effort	IP Premium	Prioritized Bandwidth	Guaranteed Bandwidth
<b>One-way delay</b>	wide	wide	medium	medium	medium
<b>ipdv</b>	wide	none	short	medium	medium
<b>Packet loss</b>	medium	wide / none	short	medium	short
<b>Bandwidth</b>	wide	wide / none	according to SLS	according to SLS	single value

**Table 4:** Proposal of QoS services

### 5.3 Projects oriented to QoS providing

In this section, the most active initiatives concerning SLS architecture are described.

#### 5.3.1 Aquila

An IST project Aquila (Adaptive Resource Control for QoS Using an IP-based Layered Architecture) attempts to design predefined SLS types. This task is inspired by the fact that the mapping between SLS parameters and Diffserv classes is very complex. Predefined SLS types support a range of applications that have similar communicative behaviour and similar QoS requirements. From the operator view it simplifies the network management and allows more efficient flow aggregation. Aquila defines following SLS types [AQU]:

- PCBR - Premium CBR,
- PVBR - Premium VBR,
- PMM - Premium Multi Media and
- PMC - Premium Mission Critical

#### 5.3.2 Cadenus

The IST project Cadenus (Creation and Deployment of End-User Services in Premium IP Networks) aims at providing service creation and configuration in a dynamic way [CAD]. It assumes two different types of dynamic behaviour: time varying user requirements and time varying network conditions.

#### 5.3.3 Tequila

Tequila (Traffic Engineering for Quality of Service in the Internet, at Large Scale) is a project from the IST family. The project involves formalism of specifying SLS. It makes a distinction between qualitative and quantitative SLS [TEQ].

#### 5.3.4 Sequin

Sequin (Service Quality across Independently Managed Networks) is an IST project. The objective of Sequin is to define and implement an end-to-end approach to Quality of Service that will operate across multiple management domains and will exploit a combination of IP and ATM technology. As the project started at the end of 2000, it is now in an early phase. In addition to Best Effort, two QoS services are defined in [SEQ]:

- IP Premium For selected flows the network capacity is conserved and therefore the packet is never lost due to congestion. The delay and delay variation is independent of the load. It offers a service equivalent to virtual leased line. This service is associated to Expedited Forwarding PHB.
- IP+ IP+ service provides a minimum guaranteed bandwidth between each two network nodes. If capacity is available, the traffic is allowed to use more than the minimum guaranteed. This service is associated to Assured Forwarding PHB.

Indicative value range of QoS parameters for all three service classes is given in Table 5.

Future multi domain extension of these services requires that all domains have to implement Diffserv and agree on interface specification with mapping between DSCP.

	<b>Best Effort</b>	<b>IP Premium</b>	<b>IP+</b>
<b>One-way delay</b>	Unspecified	Distance delay + 50 ms	Distance delay + 100 ms
<b>ipdv</b>	Unspecified	< 25 ms	< 25 – 50 ms
<b>Packet loss</b>	< 5%	Negligible	< 2%
<b>Bandwidth</b>	Unspecified	According to SLS	According to SLS

**Table 5:** SEQUIN QoS services

### 5.3.5 GEANT

A project set up by a consortium of European national research and education networks (NRENs) has the goal to improve current pan-European research network, TEN-155, by creating a backbone at Gigabit speeds. GEANT serves the European research community by supplying it with a number of services, including a testbed and guaranteed QoS features. The network will be moved to full operation in November 2001.

Apart from Best Effort, the GEANT network will support the IP Premium service as introduced by the Sequin project. Implementation of other QoS services, e.g. IP+, is currently being discussed. QoS framework of GEANT is given in [GEA].

### 5.3.6 Qbone

The QoS working group of Internet2 introduces Qbone Premium Service, which utilises the Expedited Forwarding PHB [Qbone]. QPS assures low loss, low latency and low jitter and is designed for 'CBR like' traffic. QPS uses a Bandwidth Broker concept, which is an abstraction that automates the admission control and configuration functionality.

## 6 QoS Parameter Measuring and SLS auditing

Although QoS parameter could be defined by many ways, any correct definition of QoS parameters provides a method how to measure particular parameter. To give clear interpretation to each agreed parameter value in SLS is also important, especially by describing the measurement methodology. It is desired that in

principle each user should be able to check and measure the most important parameters himself.

To ensure that the requested service can be provided, it is necessary to monitor both the client behaviour (whether the traffic actually submitted by the user complies to the SLS parameters) and the network behaviour (whether the network actually provides the requested QoS). Such a tool can provide information on the acceptability of the client and network behaviour and on the utilization of network resources. It can also provide guidance on more appropriate data description and QoS parameters than those requested in SLS.

Measurements performed in the Internet are focusing on the areas of topology, workloads, performance, and routing. Topological data describes the network link infrastructure on different protocol layers. Workload measurements are those related to the resource usage of routers or switches and the utilisation of links. Performance measurements focus on the analysis of end-to-end behaviour and on the diagnosis of network problems. Routing measurements provide insight into the dynamics of routing protocols such as routing table updates.

Passive and active measurement are the two fundamental approaches used in communication networks. By passive measurement we mean the standard approach of tracking the performance and behaviour of packet streams simply by monitoring the traffic passing by the measurement point. By active measurement we mean the injection of artificial probe traffic into the network, and the measurement of its characteristics at different points, typically back at the origin (round-trip end-to-end measurement), or at some terminating destination (one-way end-to-end).

Passive measurements are usually used to measure metrics pertaining to a certain network element, that is at-a-point metrics such as link throughput and packet size statistics. However from the application point of view, particularly real-time applications, end-to-end quality of service metrics are more important, and for these the passive approach is inappropriate as the presence of traffic between the end points is not guaranteed. Thus active measurement methods are typically used to obtain end-to-end statistics such as delay, loss and route availability.

While workload and routing measurements typically utilise passive measurements, performance and topology measurements rely on active measurement methods to a large extent. In spite of this general classification, the choice of the most appropriate measurement technique to measure a certain metric will depend on the actual circumstances and requirements, and in most cases both passive and active measurement techniques can be applied.

Currently many projects oriented towards definition and implementation of various types of network services exist which deal with QoS parameters as well (e.g. Sequin, GEANT, Qbone), while there are other projects whose goal is QoS parameters measurement and SLS auditing (e.g. RIPE TTM, Surveyor, Caida, Scampi). Besides complex project, there are lots of more or less general tools for parameter measurement.

## 6.1 Passive measurement

Passive measurement allows getting only limited set of performance parameters. Some of them, like amount of transferred data or line capacity are important to describe particular data flows or observed line but in principle they are not QoS parameters and therefore are outside our interest. Only bandwidth can be estimated among QoS parameters and for particular protocol (e.g. TCP, RTP), where counter is a part of packet header, we can monitor packet loss, too. Delay and delay variation at some path could be assessed only in case of simultaneous monitoring at both ends of this path.

Some, mostly aggregated, data can be collected at network and submitted via SNMP protocol. Alternatively, proprietary solutions, like CISCO Netflow, were deployed for this purpose. Large set of tools for analyzing Netflow output exists, e.g. CAIDA Cflowd [CFL] or system developed and used in CESNET [Kosnar].

Second method is to monitor data at a particular line. Data capture and analysis are two independent operations and therefore it is desired to store data traces (packet headers plus timestamps) in common format. In project Passive Measurement and Analysis, three such formats are used: fr, srl and tsh. All preserve IP and TCP header, format srl is oriented at ATM technology and preserves ATM cell header and LLC as well [PMA].

Capturing data at a line brings new challenge at broadband lines like OC-48 (2.5 Gbit/s) or OC-192 (10 Gbit/s), which exceeds capacity of the 64-bit PCI bus. To avoid the bus limitation, intelligent data filtering, aggregation and compression should be integrated directly into the specialized adapter. Design principles of these adapters is given in [Clea]. Example of such solution is the project DAG [DAG] which develops hardware and software analysis tools capable of providing real-time monitoring of high performance optical networks.

Another method of passive measurement is computer input traffic analysis done directly in workstation. These tools allows examining data from a live network, providing analyses and statistics, and considering secure issues as attack detection. However they do not deal with QoS parameters. NTOP [NTOP] or Ethereal [ETHR] should be noted as complex tools of such type.

### 6.1.1 Advanced project of passive measurement

The goal of the new IST project SCAMPI [SCA] is to develop a scalable monitoring platform for the Internet which will be used for traffic engineering, analysis of traffic flow characteristics and network debugging.

SCAMPI has the following main objectives:

- to develop a network adapter initially at 10 Gbit/s tailored to the needs of monitoring tools,
- to develop an open and extensible monitoring architecture, to support a secure, programmable, multi-domain and shared monitoring infrastructure,
- to develop novel monitoring tools based on the SCAMPI platform and
- to identify the technical challenges and produce recommendations on future monitoring systems of 100 Gbit/s and beyond.

## 6.2 Active measurement

There are many widely used tools for active measurement of performance parameters. Probably the most common tool is *ping*, which measures reachability, round-trip delay, packet loss ratio and some statistics: maximal, minimal and average round-trip delay. All this measurement can be done for arbitrary packet size. Another useful tool is *netperf*, which measures path throughput for both UDP and TCP and packet loss ratio for UDP. Third common tool that should be noted is *RUDE/CRUDE* [RUDE], a pair of programs for one-way delay, one-way delay variation and packet loss measuring. It uses the UDP protocol.

The main problem of each active measurement method is its invasive character. It affects the network and therefore design and operation of such tool and even interpretation of results should be done carefully in order to avoid obtaining incorrect data.

### 6.2.1 Advanced project of active measurement

Several projects dealing with active measurement are currently under way. The primary metric is always one-way delay measurement. A standardization effort exists [OWDP, OWDPR] in order to unify the used methods.

- AMP - Active Measurement Project

AMP [AMP] is project of NLANR (National Laboratory for Applied Network Research). There are currently around 130 AMP monitors collecting data. Three types of measurement are currently available: round-trip times (RTT), loss and topology.

These tests are continuously run on all the AMP monitors to all the others. They are also done to a number of other sites where the site managers have agreed to accept this traffic. The data from these monitors is available through several interfaces: web interface, animations viewable by web browser and raw data.

- RIPE TTM

The Test Traffic project [TTM] is one of the activities proposed by RIPE - (Réseaux IP Européens). The goal of the project is to independently measure the connectivity parameters, such as delays, losses and routing vectors, in the Internet. The project implements the metrics designed by the IPPM WG.

In order to measure the delays and determine the routing, measurement boxes are installed at each participating provider. These boxes measure and collect the data. Data are then transferred to a central machine at the RIPE, where they are processed and made available to participants of the project. As the measurement of one-way delay requires clock accuracy of 1 ms or better, each box has its own GPS receiver disciplining local clock.

- Surveyor

Project Surveyor [SURV] aims to measure the performance paths among participating organizations. It is based on IETF standards of IPPM WG. The infrastructure consists of measurement machines and a central database

machine to which the results of the measurements are reported. Measurement machines running BSD are deployed at various locations around the world. Precise global time synchronization among the machines is achieved by using the GPS. While this accuracy is important in the current wide area of network measurements, it becomes all the more important when measuring performance between nodes in a high-speed network.

## **7 Multipoint passive measurement**

Several ways of QoS parameters measuring are described in the previous chapter. The appropriate method depends on particular condition and reason for measurement. Still many open problems could be identified. An interesting topic, which is not widely published, is a multipoint passive measurement of QoS parameters. This method, where data flows are monitored in more points of network at the same time, is a transient phase between active measurement and simple passive measurement in the sense that it combines some advantages of both:

- the measurement does not affect observed subject - the network,
- the measurement is based on real data flows, and
- it is possible to measure parameters which are not visible in case of simple (one point) passive measurement - for instance one-way delay or ipdv.

### **7.1 Components of multipoint passive measurement**

Passive Measurement System (PMS) has following units:

- measurements site

Measurement site is a workstation collecting data from observed line. It is equipped by measurement adapter, Internet connectivity and source of accurate time.

- measurement server

Measurement server is a workstation which controls the whole measurement process including the measurement sites configuration.

- central database

In central database are stored selected raw data for further analysis and processed data for trends evaluation.

- analysis server

This site is designed for data analysis and visualization.

The crucial part of PMS is the measurement adapter, which can be:

- standard Ethernet NIC (10/100 Mb/s),

- standard ATM card (up to OC12), or
- specially designed intelligent cards (e.g. projects DAG or SCAMPI), which can be used up to OC192 (10 Gb/s).

We assume that practical realization of PMS will be used standard Ethernet NIC and SCAMPI adapter which will be developed by partners of project SCAMPI. The adapters will have substantial advantages:

- high throughput,
- data preprocessing (filtering, compression), and
- assigning accurate timestamp (i.e. wire-time).

## **7.2 Principle of multipoint passive measurement**

The method of multipoint passive measurement consists of the following steps:

- in measurement points, the IP packets are captured, including the timestamps,
- IP header (optionally header of higher protocol - TCP, UDP, RTP, ...) is analyzed,
- a decision algorithm is applied in order to decide whether to save the packet or to drop it,
- packet is converted to the format suitable for saving,
- packet is transferred to the central database and stored there, and
- desired parameters can be calculated after pairing saved packets.

Having a set of captured packet from several sites of measurement, we can evaluate desired parameters:

- one-way delay  
One-way delay we obtain directly by subtracting timestamps value of the same packet.
- one-way delay variation  
One-way delay variation is derived from the sequence of one-way delay of the same packet type.
- packet loss ratio  
Lost packet is identified by not detecting the packet at the destination. In order we are able to evaluate packet loss ratio, there is a strict requirement that capturing adapter is not allowed to lose packets.

- bandwidth

The calculation of bandwidth from one-way delay samples is an important and difficult task, which is intensively studied. One of the most advanced method is given in [Lai].

- fragmentation ratio

The problem of this parameter evaluation is the correct pairing of original packet and its fragments.

## 8 Conclusions and open problems

In the multipoint passive measurement method described above, several open problems could be found. In this report we focus on three of them, which will be elaborated in the dissertation thesis:

- formats of stored packet traces,
- evaluation of qualitative parameters, and
- time synchronization in all points of measurement.

### 8.1 Format for packet storing

Packets have to be converted to some suitable format in order to be stored for further processing. The result of conversion is called *packet trace*; identification of two traces of the same packet (from different points of measurement) is called *pairing*. The following fields should be included in stored unit which describes one IP packet:

- timestamp with resolution up to microseconds,
- whole IP header,
- header of higher level protocols (TCP, UDP or RTP), and
- a hash value of selected fields for easier identification of packet trace pairs.

In the project PMA (Passive Measurement and Analysis), set of similar formats (FR, FR+, TSH, CORAL) is designed ([PMAF]). While the simplest format FR contains only the timestamp and part of IP header, formats FR+ and TSH contain TCP header as well. The CORAL format is specially designed for ATM networks. None of these formats deals with UDP or RTP and therefore can not be accepted for our purpose.

The main goal of new format, which has to be developed, is:

- effective storage of large amount of packet traces in database,
- simple and quick identification of packet trace pairs regardless of fragmentation, and
- completeness in order not to lose any important information.

## 8.2 Evaluation of qualitative parameters

The set of predefined SLS often includes qualitative performance parameters in addition to quantitative (numeric) parameters. An example of a qualitative parameter is the delay differentiated as small, moderate or any. The qualitative substance of these parameters is mainly derived from definition of QoS services at the lowest level, for instance AF PHB class of Diffserv; therefore, these parameters can not be observed like quantitative parameters with not good known values. It implies that classical deterministic approach according to IPPM WG can not be applied. The only way how to evaluate qualitative parameters and validate them is deployment of a new methodology which should be derived from the definition of qualitative parameters. We can identify two primary features:

- evaluation has to be done on the statistical bases because parameters are defined on probability of particular phenomenon, and
- evaluation and validation have to be made in context of measurement the same parameter of others data flows because parameters values are always relative to each other.

## 8.3 Time synchronization

Good time synchronization is the essential challenge for all measurement where data are collected or generated at more places. Substantial increase of line speed requires better time accuracy and better precision. While in the 10 Mbit/s Ethernet a packet 1500 bytes long is read within  $1.2ms$ , in case of gigabit Ethernet it takes only  $12\mu s$ . It is clear, that for the measurement in LANs, clock should be synchronized up to the order of microseconds and for WANs, where the delay of current networks used to be several milliseconds, the offset between clocks exceeding  $1ms$  is not acceptable.

Avoiding specialized measurement devices, where hardware circuit synchronizes clock to external source (for instance GPS), the problem is how to discipline clock via software. The reachable accuracy strongly depends on the stability of the clock oscillator, which is in current workstation based on uncompensated quartz. Temperature, power supply and component variations affect this quartz. The most significant affect is frequency temperature dependency, which is typically in the order of one ppm (Part Per Million, e.g.  $10^{-6}$ ) per degree Celsius.

Existing NTP implementation ([Mil97, Mil98]) solves two cases: synchronization to NTP server via network and synchronization to the external source - generally pulses (PPS - Pulse Per Second). For the practical realization, where the best clock stability and accuracy is necessity, two methods can be used:

- external source of high precision clock

The combination of NTP v.4 [Mil98] together with PPS API [RFC2783] and nanokernel [Mil00] implementation (Solaris, Linux, FreeBSD) is an excellent solution for synchronizing clock to external clock. It is the standard way how primary NTP servers are realized.

This approach we deployed in our original system for QoS measurement which is used in CESNET laboratory ([QMT]), and

- high quality clock oscillator and network synchronization

When we replace the standard quartz by temperature compensated oscillator or oven-controlled oscillator, the parameters of clock improve radically: frequency temperature dependency in the whole operational range 0 - 50 degree Celsius is in order of 0.01 ppm and frequency drift is in the order of 0.001 ppm.

The second method differs from the standard model of workstation clock [Mil98] which assumes standard quartz oscillator. The proposed system of high quality local clock oscillator, synchronized via network, is characterized by extreme low ratio local clock drift to external clock drift (external clock drift includes packet delay variation). Adaptation of NTP algorithm to this system is important topic to be studied.

Another potential weakness of current NTP v.4 is the calculation of the local clock offset from mean one-way delay (as the half of round-trip delay). This model includes the hidden assumption, that one-way delay has symmetrical distribution. In real networks, one-way delay distribution function is highly asymmetrical, as there is evidently a physically given minimum of delay. Therefore other distributions, for instance exponential could be used as more realistic model of one-way packet delay distribution. In [Shal], a very stimulating idea is given to base the offset calculation on the minimum delay of the set of samples instead on the mean.

The previous two paragraphs can be summarized that the following interesting issues of NTP are to be studied in depth:

- samples filtering algorithm,
- constants of control loopback, and
- model of network clock.

## References

- [AQU] S. Salsano, F. Ricciato, M. Winter, G. Eichler, A. Thomas, F. Fuenfstueck, T. Ziegler, C. Brandauer. Definition and usage of SLSs in the AQUILA consortium. draft-salsano-aquila-sls-00.txt, Internet Draft, November 2000.
- [CAD] S. P. Romano, M. Esposito, G. Ventre, G. Cortese. Service Level Agreements for Premium IP Networks. draft-cadenus-sla-00.txt, Internet Draft, November 2000.
- [Camp] M. Campanella. IP QoS Parameters. TF-NGN, January 2001.
- [Chah] T. Chahed. IP QoS Parameters. TF-NGN, November 2000.

- [Clea] J. Cleary, S. Donnelly, I. Graham, A. McGregor, M. Pearson. Design principles for accurate passive measurement. in PAM 2000, Passive and Active Measurement Workshop, Hamilton, New Zealand, April 2000.
- [Curtis] J. Curtis, T. McGregor. Review of Bandwidth Estimation Techniques. New Zealand Computer Science Research Students Conference, Canterbury, New Zealand, April 2001.
- [GEA] M. Campanela, T. Ferrari, S. Leinen, R. Sabatino, V. Reijs. D9.1 Specification and Implementation Plan for a Premium IP Service. GEANT project (IST-2000-26417), April 2001.
- [IPDV0] C. Demichelis, P. Chimento. IP Packet Delay Variation Metric for IPPM. draft-ietf-ippm-ipdv-05.txt, Internet Draft, July 2000.
- [IPDV1] C. Demichelis, P. Chimento. IP Packet Delay Variation Metric for IPPM. draft-ietf-ippm-ipdv-07.txt, Internet Draft, February 2001.
- [Kosnar] T. Košnar. Traffic Analysis and Infrastructure Monitoring in CESNET2 Network. in PAM 2001, Passive and Active Measurement Workshop, Amsterdam, April 2001.
- [Lai] K. Lai, M. Baker. Measuring Link Bandwidths Using a Deterministic Model of Packet Delay. in Proceedings ACM SIGCOMM, September 2000.
- [Mil97] D. L. Mills. Clock Discipline Algorithm for the Network Time Protocol Version 4. Electrical Engineering Department Report 97-3-3, University of Delaware, March 1997.
- [Mil98] D. L. Mills. Adaptive Hybrid Clock Discipline Algorithm for the Network Time Protocol. IEEE/ACM Trans. Networking 5, 6 (October 1998).
- [Mil00] D. L. Mills, P.-H. Kamp. The nanokernel. Proceedings, Precision Time and Time Interval (PTTI) Applications and Planning Meeting (Reston VA, November 2000).
- [OWDP] S. Shalunov, B. Teitelbaum, M. Zekauskas. A One-way Delay Measurement Protocol. draft-ietf-ippm-owdp-02.txt, Internet Draft, February 2001.
- [OWDPR] S. Shalunov, B. Teitelbaum. A One-way Delay Measurement Protocol Requirements. draft-ietf-ippm-owdp-reqs-00.txt, Internet Draft, July 2001.
- [SCA] Annex 1 - Description of Work. Project SCAMPI (IST-2001-32404), Scampi consortium, August 2001 (non-public document).
- [SEQ] M. Campanela, P. Chivalier, A. Sevasti, N. Simar. D2.1 Quality of Service Definition. SEQUIN project (IST-1999-20841), March 2001.
- [Shal] S. Shalunov. NTP Implementation and Assumption about the Network. draft, June 2000.
- [SLS] D. Goderis, et al. Service Level Specification Semantics and Parameters. draft-tequila-sls-00.txt, Internet Draft, November 2000.

[TEQ] D. Goderis, at al. D1.1: Functional Architecture Definition and Top Level Design. TEQUILA project (IST-1999-11253), September 2000.

[QMT] S. Ubik, V. Smotlacha, S. Saaristo, J. Laine. Low-cost Precise QoS Measurement Tool. <http://www.cesnet.cz/doc/techzpravy/2001/07/qosplot.ps.gz>, June 2001.

## **Standards**

[RFC791] J. Postel. Internet Protocol. RFC-791, DARPA, September 1981.

[RFC1122] R. Braden. Requirements for Internet Hosts – Communication Layers. RFC-1122, IETF, October 1989.

[RFC1305] D. L. Mills. Network Time Protocol Specification. RFC-1305, IETF, March 1992.

[RFC1349] P. Almquist. Type of Service in the Internet Protocol Suite. RFC-1349, IETF, July 1992.

[RFC1633] R. Braden, D. Clark, S. Shenker. Integrated Services in the Internet Architecture: an Overview. RFC-1633, IETF, June 1994.

[RFC2205] R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin. Resource ReSer-  
vation Protocol (RSVP) – Version 1 Functional Specification. RFC-2205,  
IETF, September 1997.

[RFC2211] J. Wroclawski. Specification of the Controlled-Load Network Element  
Service. RFC-2211, IETF, September 1997.

[RFC2212] S. Shenker, C. Partridge, R. Guerin. Specification of Guaranteed  
Quality of Service. RFC-2212, IETF, September 1997.

[RFC2330] V. Paxson, G. Almes, J. Mahdavi, M. Mathis. Framework for IP Per-  
formance Metrics. RFC-2330, IETF, May 1998.

[RFC2474] K. Nichols, S. Blake, F. Baker, D. Black. Definition of the Differentiated  
Services Field (DS Field) in the Ipv4 and Ipv6 Headers. RFC-2474, IETF,  
December 1998.

[RFC2475] K. Nichols, S. Blake, F. Baker, D. Black, M. Carlson, E. Davies, Z. Wang,  
W. Weiss. An Architecture for Differentiated Services. RFC-2475, IETF,  
December 1998.

[RFC2597] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski. Assured Forwarding  
PHB Group. RFC-2597, IETF, June 1999.

[RFC2598] V. Jacobson, K. Nichols, K. Poduri. An Expedited Forwarding PHB  
Group. RFC-2598, IETF, June 1999.

[RFC2678] J. Mahdavi, V. Paxson. IPPM Metrics for Measuring Connectivity.  
RFC-2678, IETF, September 1999.

- [RFC2679] G. Almes, S. Kalidindi, M. Zekauskas. A One-way Delay Metric for IPPM. RFC-2679, IETF, September 1999.
- [RFC2680] G. Almes, S. Kalidindi, M. Zekauskas. A One-way Packet Loss Metric for IPPM. RFC-2680, IETF, September 1999.
- [RFC2681] G. Almes, S. Kalidindi, M. Zekauskas. A Round-trip Delay Metric for IPPM. RFC-2681, IETF, September 1999.
- [RFC2697] J. Heinanen, R. Guerin. A Single Rate Three Color Marker. RFC-2697, IETF, September 1999.
- [RFC2698] J. Heinanen, R. Guerin. A Two Rate Three Color Marker. RFC-2698, IETF, September 1999.
- [RFC2783] J. Mogul, D. L. Mills, J. Brittonson, J. Stone and U. Windl. Pulse-per-second API for Unix-like operating systems, version 1. RFC-2783, Internet Engineering Task Force, March 2000.
- [RFC3031] E. Rosen, A. Viswanathan, R. Callon. Multiprotocol Label Switching Architecture. RFC-3031, IETF, January 2001.
- [I350] ITU-T Recommendation I.350. General Aspects of Quality of Service and Network Performance in Digital Networks, including ISDN. March 1993.
- [I380] ITU-T Recommendation I.380. Internet Protocol Data Communication Service - IP Packet Transfer and Availability Performance Parameters. February 1999.
- [Y1541] ITU-T Draft Recommendation Y.1541. Internet Protocol Communication Service - IP Performance and Availability Objectives and Allocations. November 2000.

## **WWW References**

- [AMP] Project AMP (Active Measurement Project).  
*<http://moat.nlanr.net/AMP>*.
- [CFL] Cflowd (Traffic Flow Analysis Tool).  
*<http://www.caida.org/tools/measurement/cflowd>*.
- [DAG] Project DAG.  
*<http://dag.cs.waikato.ac.nz>*.
- [ETHR] Ethereal - Network Protocol Analyzer.  
*<http://www.ethereal.com>*.
- [NTOP] Project NTOP.  
*<http://www.ntop.org>*.
- [PMA] Project PMA (Passive Measurement and Analysis).  
*<http://moat.nlanr.net/PMA>*.

[PMAF] Project PMA - data formats.  
*<http://moat.nlanr.net/Traces>.*

[Qbone] Project Qbone.  
*<http://qbone.internet2.edu/arch>.*

[RUDE] RUDE & CRUDE (Real-time UDP Data Emitter).  
*<http://www.atm.tut.fi/rude>.*

[SURV] Project Surveyor.  
*<http://www.advanced.org/surveyor>.*

[TTM] RIPE TTM project.  
*<http://www.ripe.net/test-traffic>.*