IP-Availability and SLA

Jorma Kilpi
VTT, Technical Research Centre of Finland
P.O.Box 1000, FI-02044 VTT
Email: Jorma.Kilpi@vtt.fi

***Abstract*—We study possible Service Level Agreement (SLA) objectives corresponding network service availability in packet switched networks, focusing on IP networks. Service availability is looked from ISO-OSI reference model layers and cross-layer point of view. Both IETF and ITU-T metrics and definitions are discussed. We define IP network service availability, briefly IP-availability, as a set of metrics and consider the feasibility to measure these metrics. Regarding to a possible SLA, we also consider whether it is possible to affect or control a given single domain network in such a way that the performance regarding to an individual metric is improved.**

I. Introduction

Service Level Agreement (SLA) is a business contract between a network operator and a business customer. Network service availability means readiness for correct service provided by the network operator to the customer. In one form or another, service availability is always included in a SLA. The problem we are discussing in this paper is how should objectives corresponding network service availability be formulated in a SLA in order that they are *verifiable* both by the network operator and by the (business) customer? In addition to being verifiable the objectives *must correlate with the customer experience*. The operator itself needs to be certain that it can fulfill the service availability objectives. Further, the operator needs to ascertain its current and new business customers so that they can trust that the SLA objectives will be met, currently and in the future. In fact, the operator itself must have some trust that the true service availability is slightly better than what is sold out. There has to be some common understanding and agreement of what is the context of the service availability objectives in the SLA and how they are verified.

Increasing network size and complexity make network management more difficult and costly. Making the management, for example SLA compliance monitoring, more autonomous is a natural way to proceed. But monitoring is in vain unless some *actions* can be done to improve the service availability, sometimes even in real-time. These *Operation and Management (OAM)* actions must also be as autonomous as possible. Making complicated tasks autonomous requires both comphrehensive and systematic view of the whole system. Thus, systematic approaches to the definition of SLA objectives, SLA compliance monitoring, and to the set of possible actions are needed.

The scope of this paper is to try to clarify the context of possible SLA objectives corresponding network service availability in packet switched networks, focusing on IP networks.

II. Motivation and background

Availability, as an attribute to dependability, is defined in [1] as *readiness for correct service*. Readiness refers to time; at any time the correct service is available. From this we notice that the time resolution of the monitoring system/approach restricts possible service availability objectives. Moreover, for economical reasons the operator certainly wants to offer as good SLAs to its customers as ever can be verified. Hence, the monitoring capability of the operator actually defines quite exactly what kind of network service availability objectives the SLA may contain in order to be verifiable.

A graph based concept of *network availability* is defined in [2]. The difference is that we attempt to define service availability while [2] defines a network topology architecture concept. The authors of [2] define first path availability as a product of link and node availabilities and then define network availability as the minimum path availability over all shortest paths between two distinct node pairs.

There is also a closed form expression in [3] that aims to define service availability in IP networks. The problem of their formula is that it is not easy to see how it could be measured in practice. Otherwise, the discussion in [3] is very close to our apprach here. For example, the present author completely agrees with the opinion that IP service availability is essentially the ability of the IP network to carry customer traffic between any valid source and destination hosts. Service availability must be something that quantifies “the disruption in packet forwarding due to failures” [3].

In this study we are not searching for a closed form expression, instead we are looking at the operational procedures that are needed to achieve, measure and maintain an accepted level of availability. One of our key ideas is that whatever is written in the SLA must be something that the customer can verify at any time, while the main interest of the operator is to be able to detect and to locate faults or reasons of a possible violations of the SLA objective.

We are interested in the limits of monitoring methods and monitoring systems capabilities of current packet switched networks. Spatial coverage, monitoring overhead, cross-layer requirements and time resolution are important issues. Moreover, there has to be efficient methods to reduce the average duration of unavailable service time intervals, usually called Mean Time to Repair (MTTR) and increase the average duration of correct service periods which, in turn, is usually called Mean Time Between Failures (MTBF).

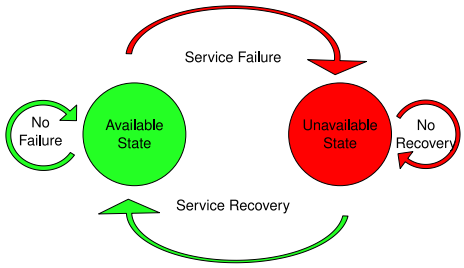

Fig. 1. Basic Availability Model.

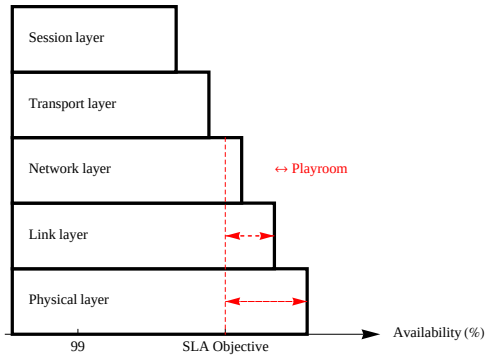

Fig. 2. Layered view of Availability leads to a staircase-like view.

It turns out that availability touches many network layers and services in a complicated way. In addition, every technological context requires different interpretation of the concept. Unavoidably the general treatment of the topic is many-sided, but we try to illustrate the general discussion by giving concrete examples of the treatment of availability.

Example 1: Several ITU-T Recommendations, for example G.827 and X.137, define a basic Availability model as a state diagram, like in Figure 1, where there are two states and some transition probability[1] between these states. For this simple model to be useful the definitions of the "Available" and "Unavailable" states and the conditions that cause transitions between these two states must be exact, correspond to reality, and be verifiable by measurements. Correspondance with reality means that both the operator and the users share the same opinion about the current state of Availability. For example, in X.137 eight performance parameters are used in computing the availability of a virtual connection in a X.25 type packet switched network, then five particular linear combinations of these parameters are called availability decision parameters. Finally, each decision parameter is associated with an outage threshold. Available state then requires that all decision parameters are within the acceptable side of the threshold values. It is not easy to judge whether this approach corresponds to the user experience or not. The fact that there is some freedom in setting the exact values of the thresholds does not make such a judgement easier.

III. Layer view of Service Availability

A layer view of service availability means that we consider each ISO-OSI reference model network layer separately. A lower layer provides service to the upper layer, an upper layer uses the service of the lower layer, and for a given layer we consider the availability of this service.

When focusing on the IP-networks we must take into account that the IP protocol stack architecture does not exactly map into OSI reference model [4].

[1]The phrase "transition probability" is dangerous since this easily comes along with some hidden assumptions about the nature of service availability. For example, mathematically it is tempting to assume that a failure rate does not depend on time which would mean that any OAM attempt to improve service level is in vain.

Upper layer service availability includes the lower layer service availability in the sense that if a upper layer service availability objective was satisfied, then all those lower layer service availability objectives that were needed to produce the upper layer service were essentially also satisfied. However, a link bit error rate (BER) can be worse than a SLA objective required, but the use of forward error correcting codes (FEC) may still have resulted in acceptable application layer service.

However, even if the lower layer(s) service availability objectives are satisfied it does not mean that the upper layer service availability objectives are satisfied. If all different layer specific service availabilities were well specified and were commonly measurable in time, then this would lead to a staircase-like view like shown in Figure 2 where the service availability in the lower layer must in practice be better than in the upper layer.

It is theoretically possible to set SLA objectives only to the layer of interest. It is then implicit that the lower layer(s) service availability must be high enough to provide the upper layer Availability and there is no need to set separate SLA objectives to these lower layer(s) (unless lower layer service is also sold).

Example 2: The ITU-T Recommendation Y.1540 defines an unidirectional concept of *IP service availability* along an end-to-end (E2E) path by setting a single outage criteria: the Packet Loss Ratio (PLR) satisfies the condition $\mathrm{PLR} > c_1$. Threshold values like $c_1 = 0.75$ and $0.03 \leq c_1 \leq 0.2$ are suggested, depending on the traffic class.

In IP-networks availability of one-hop paths reduces to a link layer service and availability of multi-hop paths is a network layer service. However, unavailability of one-hop paths need not necessarily imply unavailability of multi-hop paths, unless link layer failures separate the two end points of the path, that is, make the network disconnected and re-routing impossible.

Like the BER & FEC case above, this shows an important aspect of our layered view of services: locally in time and in space it can be that the lower layer service availability is worse than the upper layer service availability. In such a case the upper layer service is robust.

Like noticed in [2] and in [3] taking use of this local

robustness of IP-networks requires that the alternate paths have enough resources available to handle the traffic of the failed path(s). This is possible if the total network load is low or if there is sufficient transfer capacity left on purpose for back-up path(s).

A. Examples of Cross-Layer and Multi-Layer Requirements to Network Service Availability

Example 3: Leased Transport Service. Consider a mobile operator who wants to connect base station (BTS) sites to radio network controller (RNC) site using a Transport Operator's Metro Ethernet network as depitched in Figure 3. This means essentially pre-fixed minimum capacity bit pipes between pre-defined locations.

The transport service availability looks like almost completely a L2 concept for the mobile operator. Indeed, the Transport Operator's network looks like a multi-port Ethernet switch for the Mobile Operator.[2] However, the Transport Operators Ethernet edge (or demarcation) switches may need to be able to check the *Differentiated Services Code Point (DSCP)*[3] field of the payload IP-packets in order to be able to separate various traffic classes of the mobile customer from each other. Thus, the requirement to correctly classify traffic according to DSCP field of the IP packet header, a cross-layer feature, is likely to be included in the SLA between Mobile and Transport operator. For example, a miss-classification ratio could be required to be smaller than some specified bound.

The mobile operator should not see effects of other traffic than its own unless the bought minimum transmission capacity is exceeded[4]. Customer IP-packets are transmitted as a payload and, for example, the *Time-to-Live (TTL_{IP})* field of the IP-packet header is not changed.

The service Availability objectives that the Mobile Operator would like to have in the SLA are for multi-layer services: transparent Ethernet-looking interface (L2), separation of customers traffic classes according to DSCP field (L3), guaranteed minimum transfer capacity (L3) and, for example, out-of-order delivery not allowed (L4). All other possible Layer 3 service Availability issues are hidden inside of the Transport Operator's cloud which can be made of any technology. Since RNC and BTSs have IP-addresses for remote control purposes anyhow, it means that the Layer 3 of the Transport Operator and the Layer 3 of the mobile operator are completely separated. This natural choice separates most of the OAM functionalities of different operators and makes the SLA more simple in this sense. However, in order not to mix L2 control traffic of the two operators, it is expected that the Transport Operator will simply drop Mobile Operators L2 control frames. This means that the Mobile Operator has to use L3 level path monitoring between BTSs and RNC sites.

[2]For more information about packet switched mobile backhaul see Metro Ethernet Forum (MEF) homepage http://metroethernetforum.org/ and Next Generation Mobile Networks (NGMN) alliance home page http://www.ngmn.org/.

[3]Without DiffServ known as Type of Service (TOS) field.

[4]The Metro Ethernet is not build only for mobile backhaul since it is not economical. There can be all kinds of other traffic.

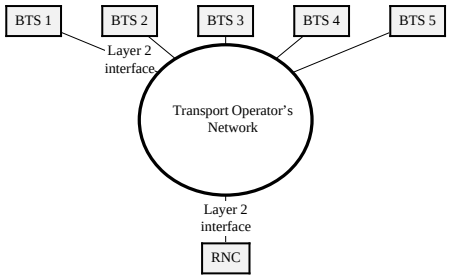

Fig. 3. Leased packet switched mobile backhaul.

This raises the question of how much the Mobile Operator must do own monitoring and how much it can trust to the SLA.

Example 4: Enterprise IP network. Consider the case where a company, an enterprise or an organization buys network services from an operator. In this case Availability contains also IP-layer concepts for the customer: Connectivity within the company and to the Internet, DHCP performance, DNS performance and routing performance. Which of these could/should be included in the SLA depends on the situation. For example, it may be that even the company end users' equiments (PCs, laptops, phones) also belong to the network service operator. Or, it can be the case that the company owns the infrastructure and, essentially, only OAM is bought, say when the formerly company owned network service is outsourced. In this case closely related to Availability are security issues, they can also be expected to be included in the SLA.

Example 5: Internet Service Provider (ISP). Consider a large ISP which has a countrywide backbone IP network and which provides IP transport service and Internet access to several smaller operators or companies. Different customers have different requirements, hence the number of SLAs that the ISP is involved may be large. While a tailored SLA is a well selling product, it would certainly be helpful if the main guidelines and common requirements of various SLAs were commonly measurable. In the end the total network capasity is finite, it is a shared resource for every customer, and the ISP must guarantee fairness between customers.

IV. Components of IP-Availability and Single Domain SLAs

Having the same overall idea than in Example 1 the ultimate idea of Figure 4 below, when reading from left to right, is to define a set of metrics that together aim to define *IP network service availability*, which we briefly call *IP-availability.* We emphasize that this is a set of metrics for discussion, the aim of this study is not to end up with a closed formula or with a composite metric.

Reading from right to left Figure 4 below splits the IP network service availability into three components, routing, Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP) whose performance together forms the IP-Availability. Although DNS and DHCP performance may

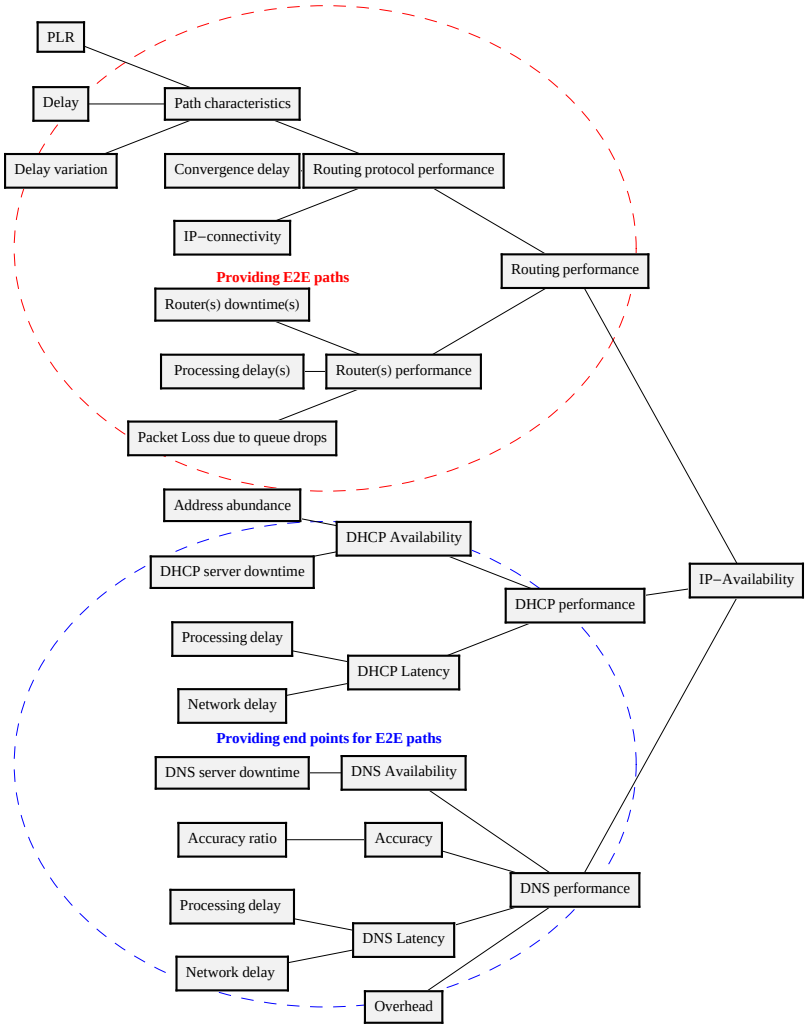

Fig. 4. Components of IP-Availability.

not typically be included in the current SLAs, we consider here the possibility and meaningfulness of including them also in a SLA. The main motivation for including DNS and DHCP in IP-Availability is that if they are not working properly the customer may not be able to verify that the network is able to carry traffic from valid sources to correct destinations. That is, to maintain the correlation with the customer experience seem to require to include DNS and DHCP performance in the concept of IP-Availability. The "routing performance" in Figure 4 is roughly the same as the concept of "path availability" in [3].

Furthermore, Figure 4 divides these components into smaller attributes and, finally, into metrics like downtimes, delays, losses and so on. Focusing on a single domain and a SLA that will contain network service availability objective, we ask which of these metrics can be effectively measured/monitored and what network configurations can be affected/controlled in order that the objective is satisfied?

A. *DNS Performance*

DNS is needed when the other end point of the connection is outside of the operators domain. We assume now that the network operator maintains at least one DNS proxy server inside the domain. As a protocol, DNS is an application layer protocol [4], but the service that it provides is needed at the network service level.

DNS performance has been recently studied in [5] where metrics to quantify the quality of DNS are defined. These metrics are based on accuracy, availability, latency and overhead of DNS service. "Accuracy and availability refer to the ability to supply up-to-date and correct DNS records to the client so

that it can connect to and only to[5] the desired site",[5].

In Table I we consider, for each DNS metric of [5], whether the metric is really measurable or not, is it possible to affect or control the network configuration in such a way that the performance regarding to the metric is improved. Finally, we consider what would be a possible OAM action that would improve the performance.

The authors in [5] discuss the impact of *Time-to-Live (*TTL_{DNS}*)* value of DNS resource records (RRs). According to their empirical study, domain administrators do not typically attempt to optimize (TTL_{DNS}) values. However, according to the modelling scenario in [5], it seems that optimization is worthfile.

The conclusion about DNS proxy server(s) is that, depending on the context, DNS performance could be part of SLA if the boundary conditions can be specified. The responsibility of the network operator ends at the gateway.

B. DHCP Performance

In order to start to communicate on the Internet a host must have three key pieces of information provided by DHCP: its IP-address, the subnet mask and the default gateway, [4].

DHCP performance is studied at least in [6] and in [7]. Both studies point out that choosing the size of the dynamic address pool and length of the lease period affect to the performance of the DHCP server. The metric *address abundance* in Table II is the number of free IP addresses in the dynamic address pool. Monitoring this value is non-specified since the DHCP specification RFC 2131 deliberately describes only client-server interactions and specific DHCP server implementations may incorporate any controls or policies desired by the network administrator.

Example 6: The DHCP service that the customer end-user will see may not be included in the SLA. For example, a box which integrates WLAN base station and a cable or ADSL modem may have a built-in Firewall, Network Address Translation (NAT) and a DHCP server which is enabled by default [6]. While the box itself gets IP-address from the network operator's DHCP server, its own DHCP server provides IP-addresses to the laptops that are attached to the WLAN. This box can be a customer's or a provider's device. Moreover, if some misconfiguration is possible, by mistake or by a malicious user, then this box DHCP server may become an unauthorized DHCP server for the whole network [6].

The conclusion about DHCP performance is that, depending on the context, it could be part of a SLA.

C. Intra-Domain Routing Performance

The considerations about DNS and DHCP above are the same for Best-Effort (BE), Integrated Services (IntServ) and Differentiated Services (DiffServ) service architectures. However, to evaluate routing performance the service architecture must be taken into account.

If only BE service is sold, there may be multiple paths between a source and a destination. Connectivity, in the sense of RFC 2678, is the main metric. There are some implicit transfer capasity assumptions. The main routing performance issue is the re-routing possibility and the role of the network availability concept of, for example, [2] is more significant. Topological redundancy with some free capacity guarantees also service availability to some extent. For example, in [3] it is mentioned that the Sprint IP core network is designed to absorb the effect of failures without overloading links unless several links fail simultaneously. With only BE service a transparency of the network, in the sense that any destination inside the domain and any gateway is equally reachable, could be demanded in a SLA.

If path changes are frequent, they affect to the end-user experience, since then it is not possible to avoid or bound rapid changes in delay(s). Most real-time applications cannot tolerate them. Such changes are typically larger in magnitude and more rapid than queueing delays alone in a fixed path. Thus, with DiffServ and IntServ service context we assume that path changes are infrequent and we can speak about 'the' path and its characteristics. From a DiffServ or IntServ service user point of view the available bandwidth on the path must be sufficient for the application or for the traffic class and, in the DiffServ case, also traffic classification according to the DSCP field must work properly. Now the connectivity is implicit but the path capacity is explicit.

Example 7: (Continuation of Example 2.) The minimal test of IP service availability of Y.1540 is as follows. For active probing Y.1540 suggests $M = 1000$ packets during an interval of $T = 300$ seconds (5 min). Then the probing intensity is $M/T = 3.3$ packets per second (PPS). With a packet size of 1500B this means a 40 kb/s flow rate. If $\mathrm{PLR} = 0.75 = c_1$, then 10 kb/s is the minimal acceptable available bandwidth. Thus, defining a minimal test of availability, even in a BE service, induces a minimal acceptable bandwidth.

The above Example 7 indicates that a path is not a valid path unless it has some minimal transfer capacity always available. For BE service a 40 kb/s E2E service with 75% PLR could be offered, but for IntServ and DiffServ service it is better not to offer a path with such characteristics at all.

The two issues discussed above, the path change frequency and the available bandwidth in the path, are not yet included in Figure 4. Clearly the path change frequency should be so low that a streaming data flow (VoIP, IPTV) typically does not experience a path change. But this requires that the network has sufficient transfer capacity allocated for the corresponding traffic class. Whether this is handled by overdimensioning or admission control is a difficult question. In practice both may be needed. A third main group in Figure 4 could be "Providing/quaranteeing/maintaining sufficient capacity to E2E paths". To some extent, however, this is implicit in path characteristics.

1) Routing protocol performance.: Routing is the act of moving data across an internetwork from a source to a destination. Without routing only single hop paths could exist. *A routing domain* is a portion of an internetwork under common administrative authority. We restricted the scope of this study

[5]Note that the "only to" is a security issue.

TABLE I
DNS PERFORMANCE

Metric(s)	Measurable?	Controllable?	Action?
Network delay(s)	By active probing	Intra-domain delay bounded by RTT	
Processing delay(s)	Benchmarking RFC 2544	In the deployment phase	
Accuracy ratio	Estimable	Optimization is possible	Affecting to TTL_{DNS} values of RRs
Overhead	By Monitoring DNS traffic volume		Filter DNS traffic
DNS server(s) downtime(s)	By active probing	By redundancy	Increase redundancy

TABLE II
DHCP PERFORMANCE

Metric(s)	Measurable?	Controllable?	Action?
Address abundance		Lease Time Optimization is possible	Forcing release of unused leases or increasing dynamic address pool size
Network delay	By active probing	Bounded by RTT	
Processing delay	Benchmarking RFC 2544	In the deployment phase	
DHCP server(s) downtime(s)	By active probing	By redundancy	Increase redundancy

to single domain SLAs since performance of the routing can (currently) be efficiently affected only by a single authority and inside a routing domain. One missing piece of extending this study to SLAs that cover more than one domain is the lack of a protocol that could be used to transfer sensitive dependability information between domains in real-time.

With certain protocols, routing domains can be further divided into routing areas, but intradomain routing protocols are still used for switching within and between these routing areas. Single area SLAs could also be possible.

Convergence is the process of agreement, by all routers after a topology change in the network, on optimal routes and the convergence delay in Table III is the speed of this convergence. In [3] the authors argue that fine tuning of the timers of the IS-IS routing protocol is possible and that it affects to the convergence delay of that protocol. The Benchmarking Working Group has defined benchmarking tests for basic Open Shortest Path First (OSPF) routing protocol in RFC 4061.

Routing can be based on several metrics: path length, reliability, delay, bandwidth, load and communication cost. For example, a path that minimize PLR between the source and the destination need not minimize delay. When these metrics are monitored they can be given as input to the routing protocol. To some extent a router may maintain these metrics.

2) Monitoring E2E path characteristics: The present author is generally advocating the use of the One-Way Active Measurement Protocol (OWAMP), defined in RFC 4656, for active probing since we have comprehensively tested and used an implementation of OWAMP from http://e2epi.internet2.edu/owamp. Another OWAMP implementation is available in www.av.it.pt/jowamp/. The main point is that OWAMP is a tool that both the operator and the customer can use. It is not clear whether the customer could use the Bidirectional Forwarding Detection (BFD) protocol, (IETF work in progress), for the service availability tests. Recently the Two-Way Active Measurement Protocol (TWAMP) has achieved the RFC status,

TABLE III
ROUTING PROTOCOL PERFORMANCE

Metric(s)	Measurable?	Controllable?
PLR RFC 2680	OWAMP RFC 4656	Possibly by path change
Delay RFC 2679	OWAMP	Possibly by path change
Delay Variation RFC 3393	OWAMP	Possibly by path change
Convergence delay	Benchmarking RFC 4061	In a simple topology
Connectivity (In case of BE) RFC 2678	OWAMP	By topological redundacy

RFC 5357, but so far we have no experience with it. The use of TWAMP may reduce synchronization requirements.

Regarding active probing in general there are many restrictions and requirements for a good protocol:

1) Active probing is intrusive, hence the level of intrusiveness must be minimized.
2) Active probing consumes available bandwidth, hence the total amount of active probing traffic in the whole network must be minimized.
3) For different purposes different probe sending schedules are needed. Sending schedule defines the inter-probe sending times. This time could be fixed, random, or combination of fixed and random (bursty).
4) Some level of synchronization between the source and the destination clocks is always required since, for example, detecting PLR requires rough knowledge of delay.
5) The active probes should include sequence numbers since it should be possible for a receiver to decide when a packet is lost. Then also Packet Loss Pattern metric of RFC 3357 and Packet Reordering metric of RFC 4737 can be obtained from the measurement probes. The latter is needed if out-of-order delivery is specified in the SLA.
6) Active probes should be indistinguishable from ordinary traffic. Otherwise the network may treat them differently which greatly reduces any changes to make justified inference from active measurements.
7) Authorization is needed to restrict the active probing traffic.

These requirements affect to active E2E path monitoring capability.

One main question is how much the customer need and can measure path characteristics. Essentially the customer should be able to trust to the operator and to the SLA. However, active probing in general must be possible for the customer. Especially, a connectivity or path availability test must be possible for the customer. This may require the inclusion of certain DNS or DHCP performance objectives in the SLA.

Another issue is how well the E2E path characteristics are measured with active probing. How to generally guarantee, for example, that active probes really traverse along the intended path. Should we use a more built-in passive methods and, if so, then what these methods would be.

One problem is the amount of data that needs to be processed in real-time. In case of problems this data easily starts to accumulate, both for the operator and for the customer.

3) Router(s) performance.: The Benchmarking Working Group of IETF has provided Benchmarking Terminology for Resource Reservation Capable Routers in RFC 4883. According to RFC 4883 the processing delay(s) related to router(s) performance of Figure 4 could further be divided into Best-Effort Traffic delay(s) and Distinguished Traffic Delays(s). For the methodology to measure such values in the benchmarking sense, for example in the service deployment phase, the RFC 2544 is a general reference. The RFC 2544 defines Benchmarking Methodology for Network Interconnect Devices.

TABLE IV
ROUTER(S) PERFORMANCE

Metric(s)	**Measurable?**	**Controllable?**
Router(s) downtimes	By active probing	By redundancy
Processing delay(s)	Benchmarking RFC 2544	In the deployment phase
Packet Loss due to queue drops		

The packet loss due to queue drops in Table IV is an open issue. Fo example, all dropped packets are not necessarily of equal value.

4) Routing performance in SLA: The routing performance of Figure 4 is essentially the same concept as the path availability in [3]. However, in order to correlate with the customer experience there must be a method also for the customer to verify E2E connectivity, that is, to measure path availability. This requirement of "minimal" test of availability implies minimal available bandwidth and minimal requirements for the path characteristics.

V. CONCLUSIONS AND FURTHER RESEARCH TOPICS

We have provided a practical framework for characterizing and measuring IP network service availability and for developing (preferable autonomous) OAM methods.

Our contributions can be listed as

- We made a practical study of SLAs with a focus on correspondance between the customer experience, SLA objectives and the possibility to verify the SLA objectives.
- We illustrated the layer and cross-layer view of service availability by examples.
- We analyzed IP network service availability concept by splitting it to smaller pieces with the aim that the smallest pieces were measurable with well defined metrics. For the operator it is important to monitor these metrics in order to locate failures and to try to improve the performance of the network.

Correspondance between the customer experience means that there must be a method for the customer to test or measure IP-availability. For this reason we included DNS and DHCP performance in the concept of IP-availability. The requirement of the existence of such a method implies minimal bandwidth, loss and delay requirements.

Further research topics include

- To improve the concept of IP-availability. Figure 4 is not intended to be complete yet. There are issues that do not yet have a clear widely accepted metric.
- Some metrics could be used as defining a state transition between the available and unavailable states like in Figure 1, other metrics are more benchmarking type that are used to indicate initial confidence level of the service.

A prototype of the IP-availability in terms of the simple model of Figure 1 is needed.

- To stydy dependability communication between domains. One of the main problems is the lack of a trusted method to exchange sensitive information between the SLA partners in real time.

REFERENCES

[1] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, January-March 2004.

[2] W. Zou, M. Janic, R. Kooij, and F. Kuipers, "On the availability of networks," in *BroadBand Europe 2007*, Antwerp, Belgium, 3-6 December 2007.

[3] S. Bhattacharyya, C. Diot, G. Iannacone, A. Markopoulou, and C.-N. Chuah, "Service Availability in IP Networks."

[4] D. Medhi and K. Ramasamy, *Network Routing, Algorithms, Protocols and Architectures*. Morgan Kaufmann, 2007.

[5] L. Yuan, K. Kant, P. Mohapatra, and C.-N. Chuah, "A Proxy View of Quality of Domain Name Service," in *Infocom 2007*.

[6] V. Brik, J. Stroik, and S. Banerjee, "Debugging DHCP Performance," in *IMC'04*, IMC. Taormina, Sicily, Italy: ACM, October 25-27 2004, pp. 257–262.

[7] M. Khadilkar, N. Feamster, M. Sanders, and R. Clark, "Usage-Based DHCP Lease Time Optimization," in *IMC'07*, IMC. San Diego, California, USA: AMC, October 24-26 2007, pp. 71–76.