Estimating SLAs Availability/Reliability in Multi-services IP Networks

Saida Benlarbi

Manager, System Reliability Engineering
Alcatel – IP Division
600 March Road, Kanata - Ottawa, Ontario, Canada K2K 2E6
Voice: (613)-784-6433
Saida.Benlarbi@alcatel.com

Abstract. Multi-Services IP Networks are being required to deliver unprecedented high volumes of diverse traffic that span two ends of the reliability requirements spectrum. On one end of the spectrum real-time services such as voice and real time TV require high sensitivity to delays and jitter. On the other end of the spectrum best effort services such as data content delivery services requires zero traffic losses and traffic integrity. This paper focuses on investigating the challenges of measuring the end to end service availability given the different layers of resilience in the hierarchical network architecture. It proposes a layered approach to modeling and measurement of multi-services IP networks from which composite availability/reliability estimation models combining convoluted levels of fault resilience can be derived. The resulting models can be readily used to show a Service Level Agreement reliability measure is met from both the service provider and the end user standpoints.

Keywords: Reliability, Availability, Service Level Agreement, Multi-service IP network, Markov Modeling.

1 Introduction

IP is becoming the next generation communication services delivery mean that makes service providers and Telecom operators face a number of networking design and reliability challenges. Multi-services IP networks are currently touted as being up to these challenges. However, they need to meet a set of design and reliability requirements in order to be carrier-grade performance and reliability hence secure low costs and increased profits for vendors, network operators and services providers [8],[1],[3],[10]. In particular, a multi-services IP network has to deliver high volumes of diverse traffic that span two ends of the reliability requirements spectrum. On one end of the spectrum real-time services such as voice or real time TV require high sensitivity to delays and jitter. On the other end of the spectrum best effort services such as data content delivery require zero traffic losses and high traffic integrity.

As service providers and network operators deploy these services they face the challenges of designing the IP network that is capable of supporting a number of

D. Penkler, M. Reitenspiess, and F. Tam (Eds.): ISAS 2006, LNCS 4328, pp. 30 – 42, 2006.

application service classes with predictable and/or guaranteed levels of service. In order to deliver predictable service levels that are bound to meet required Service Level Agreements (SLA)s every service class has to be defined in terms of availability/reliability/serviceability targets measured in terms of the network architecture design and traffic management parameters such as topology and network configuration dimensioning, latency, jitter, packet loss, and bandwidth.

Over decades of development, the Telecom industry came to agree on well established and standardized communication systems reliability estimation methods and techniques that allow quantifying their behavior and measuring it against service level agreement targets [7]. However, these estimation practices present a number of limits and challenges that need to be overcome in order to be able to leverage their use for multi-services IP networks SLAs estimation. For example, most of the currently industry used methods and techniques are based on connection oriented traffic moving that focuses on L1 (node hardware and Automatic Protection Systems) and L2 (link and connection protection) of the IP network whereas the availability/reliability models of multi-services IP network need to take into account the complexity and the intricacy of the various levels of the networking functions and their binding with the infrastructure behavior. Moreover, the service IP path failure/repair behavior has to be considered under network load performance conditions in order to demonstrate that an SLA is met under for given engineered bandwidth. One of the major issues in this respect is to be able to demonstrate that an end-to-end service path meets its SLA reliability targets under a given network dimensioning and services configuration. For example, how to show that an end-to-end service path meets 99.999% availability often coined from the well proven PSTN[1] reliability under average and worst case load? How to show that an IP path carrying voice traffic meets the tight voice requirement of 150ms max delay from mouth to ear dictated by the max window of a perceivable degradation in voice quality? How to show that an end-to-end IP path incurs zero packet loss for a real-time TV service?

Liu & Trivedi [1] propose a general framework for survivability estimation where one can distinguish various angles of network reliability focus for each of which a suitable reliability model can be constructed. However, it still does not answer the need for a binding view between the service behavior and the network behavior that has to be defined in order for service providers, network operators and vendors have a common service quantification mean. To answer this need we are currently investigating various design and measurement approaches that pave the way for building viable modeling and measurement techniques that answer specific SLAs quantification.

In this paper, we propose a layered approach to modeling and measurement of multi-services IP networks from which composite availability/reliability estimation models combining convoluted levels of fault resilience can be derived. The resulting models can be readily used to show an SLA is met from both the service provider and the end user standpoints.

Section 2 provides a mapping between the service view, the network functions view and the network infrastructure view. In section 3 we identify the four layers of network resilience and discuss the limitations of measuring multi-service IP network

[1] If not defined in this paper, the acronyms used are well established Telecom terms. The reader is advised to consult the Telecom literature for an exhaustive glossary.

availability/reliability and performance separately. In section 4 we show the need for using an integrated modeling approach that is more reflective of the network resilience layers contribution to the service availability/reliability. We then propose a layered approach that allows assessing the service availability/reliability in a multi-service IP network that help in demonstrating SLAs are met under given network load conditions and behavior.

2 Overview of Service Resilience in Multi-services IP Networks

As new communication technologies are developed new services can be created and the need to demonstrate they meet customer requirements becomes crucial in differentiating these technologies. Fig. 1 shows a simple mapping between data communication based services, the networking infrastructure that provides it and the networking functionality or service protocol that delivers it [1].

Multi-services data networks are designed in a hierarchical architecture where various resilience options are deployable. At the Physical Layer (L 1) of the network a number of transport options with different resilience characteristics are possible. A first option is the well established Telecom carrier transport systems TDM ring based on SONET and SDH. The second one which comes from the packet world is the packet rings where a range of options is available: token ring, FDDI, etc. Since Gigabit Ethernet packet switching at line rate is becoming the multi-services IP networks preferred traffic delivery method, Resilient Packet Ring (RPR IEEE 802.17) presents itself as the MAN/WAN transport option that leverages packet rings based on the TDM ring resilience concepts. Both categories offer physical protection since when a link is cut or a port is down traffic keeps on flowing through a redundant path. On a failure, the target switchover delays are typically of less than 50ms in order to meet the stringent requirements of time sensitive services.

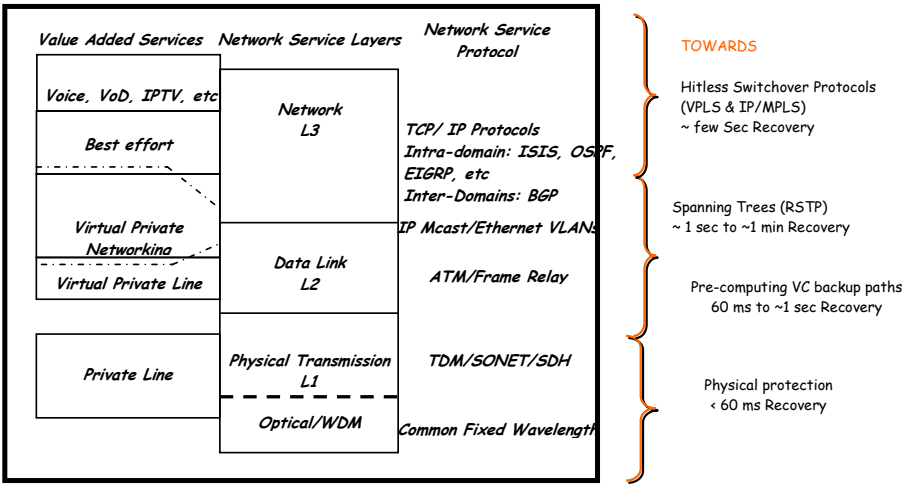

Fig. 1. Mapping Services, Networking Functionality and Network Infrastructure

At the Link Layer (L 2) of the network, technology choices are less diverse. ATM provides resilience by pre-computing backup paths that are activated within a given delay typically in the order of less than one second for switched Virtual Circuits (VC)s depending on the number of connections to reroute. Ethernet provides resilience through the re-computation of its spanning tree in the event of a failure (IEEE 802.1d). Because this mechanism may take a delay in the order of the minutes it fails to meet stringent real-time service recovery requirements. Recently it has been extended with the Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) with target convergence times of the order of the second.

At the Network Layer (L 3) of the network, the most common protocol option is IP. IP uses ICMP to detect and recover from L3 type of failures. The IP resilience is provided by the L2/L3 control protocol functions which maintain forwarding information, manage failure detections, perform topology discovery and routing table updates in the event of a network topology or load conditions changes. However, IP networking function must also rely on the Transmission layer (L4) to ensure a reliable delivery of the packet. Depending on where a given networking system is located in the network and on local preferences, different protocols are used: within the same domain, intra-domain protocol such as ISIS, OSPF, EIGRP, or RIP is used; between different domains, an inter-domain protocol is used with BGP being the most dominant. The L4 resilience is based on TCP functionality for connection based packet routing and UDP for connectionless packet routing. Hence, in case of a failure or poor network performance behavior the routing and network configuration information have to be re-computed.

One main problem with L3 resilience is that it is coupled with a working routing protocol run at L4. If the latter fails, the routing system can no longer be active in reconfiguring the network topology and re-establishing new routes. Depending on the protocol used the recovery times in this case are in the order of 10s of minutes unless a duplication of devices and networking functions is put in place which of course comes with a high cost. The separation of the routing plane from the forwarding plane allows for a better resilience especially when a failure event impacts only the routing plane. In this case it is possible to try to restart the routing engine without impacting the service. The failure may then be recoverable with target recovery time in the order of 10 seconds. In this respect, many quick restart extensions have been added by the IETF to the common routing protocols. However, at GigE line rate switching, a failure translates in high impacts even in case of 10's of seconds of interruption as thousands of traffic flows and user/subscribers get cut from the service. Hence the network re-convergence may pose a number of performance tuning challenges. A much higher availability solution is to architect a fully redundant routing plane in a hot standby mode where regardless of the protocols running, the L3 and L4 protocol activities incur a hitless switchover in the event of a failure or poor network load behavior. This means the active and standby routing planes must maintain synchronized L3/L4 states and traffic management information so the traffic is handed over within 10's of milliseconds. Currently, VPLS and IP/MPLS network architecture designs are targeting L3/L4 recovery times in the order of few seconds.

3 Estimating Multi-services IP Networks Service Availability/Reliability

The main difficulty in modeling and estimating multi-services IP networks is to aggregate the measures from all the levels of networking functions and work with a viable model that reflects the network behavior from the service provider and the service user standpoints. The second difficulty is that for functions of L1 and L2 types, availability/reliability parameters can be easily distinguished from performance ones hence estimated separately. On the other hand, functions of L3 and L4 types exhibit most of the time a degraded performance state before they fail completely. This makes it difficult to distinguish between failures modes resulting in a complete loss of service (e.g. unreachable destination or link loss) and failures modes resulting in a partial loss or temporary corruption of the service (e.g. overflow of buffer capacity to forward traffic). Hence, demonstrating multi-services IP networks reliability and robustness requires a careful balancing act of probing and measurement of the various network layers resilience that are impacted by both scalability limits and failure events that affect the various networking layers.

As a first step of the estimation approach a careful definition and identification of the service affecting failure modes that can be generated by any of the L1 to L4 of the networking functions has to be laid out.

Figure 2 depicts the growing complexity and interactions that stem from failure modes dependencies which can originate at the different networking functions layers of the multi-service IP network. Failure modes attributable to particular hardware infrastructure, software system or network element running a particular network protocol have to be identified and assessed in terms of their effects on the network service layers which in turn have to be mapped to specific type of provider/end-user service failure effects.

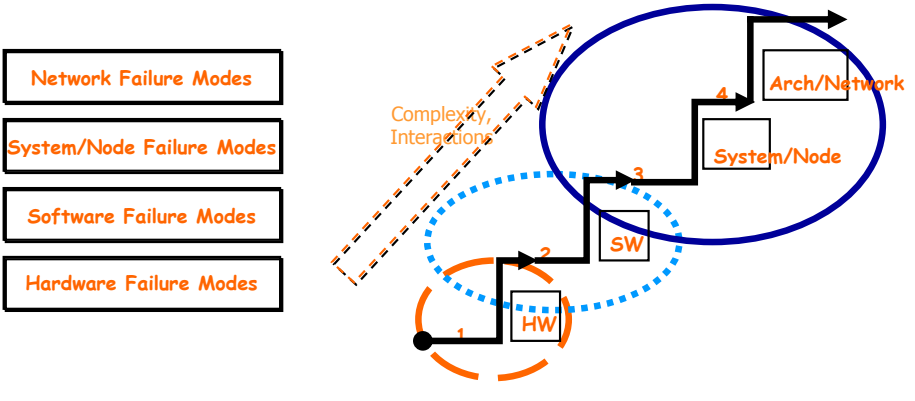

Fig. 2. Networking Function Failure Modes Complexity and Interactions Levels

3.1 Models for L1 and L2 Types of Resilience

Two major modeling approaches are used to evaluate networking systems availability: discrete-event simulation or analytical modeling [5]. A discrete-event simulation model mimics dynamically detailed system behavior to evaluate specific measures such rerouting delays or resources utilization. An analytical model uses a set of mathematical equations to describe the system behavior. The measures are obtained from solving these equations, for e.g. the system availability, reliability and Mean Time Between Failure (MTBF). The analytical models can be divided in turn into two major classes: non-state space and state space models. Three main assumptions underlie the non-state space modeling techniques: the system is either up or down (no degraded state is captured), the failures are statistically independent and the repairs actions are independent. Two main modeling techniques are used in this category: Reliability Block Diagram (RBD) and Fault Trees. The RBD technique mimics the logical behavior of failures whereas the fault tree mimics the logical paths down to one failure. Fault trees are mostly used to isolate catastrophic faults or to perform root cause analysis.

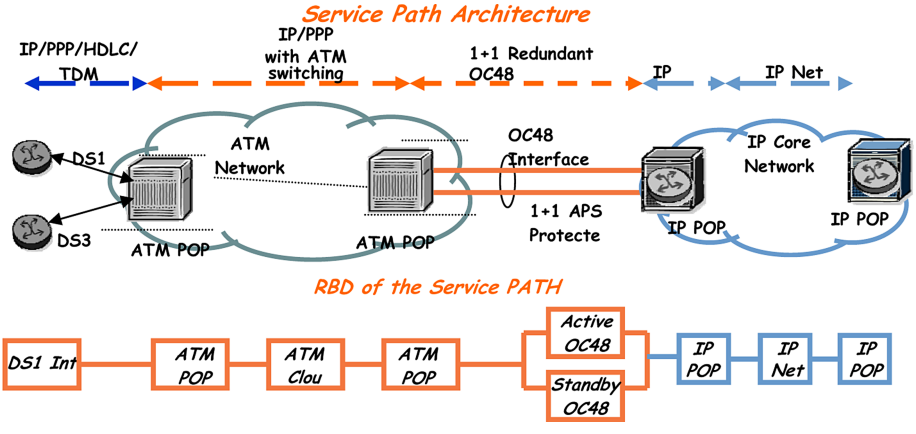

Fig. 3. Example of a Multi-Services IP Path RBD

RBD is the most used method in the Telecom industry to estimate the Reliability/Availability of the L1 and L2 type of resilience in a networking system [7]. It is simple to develop and grasp and it does reflect typical L1/L2 reliability behavior as network functions at these level are either up or down. It is also a straightforward mean to isolate the network single points of failure. An RBD captures a network function or a deployed service as a set of inter-working blocks (e.g. a SONET ring) connected in series and/or in parallel to reflect their operational dependencies. In a series connection all the components are needed for the block to work properly i.e. any of them goes down the function/service goes down. In a parallel connection at least one of the components is needed to work for the block to

work. Given the failure rate λi of a block i and the Mean Time to Repair (MTTR) μ, the steady state availability of the block is given by:

$$A_i = \frac{MTBF_i}{MTBF_i + MTTR} = \frac{\lambda_i}{\lambda_i + \mu}$$

Fig. 3 shows an example of a service path RBD.

The path is composed of a DS3 source point then traverses and ATM network then gets out to an IP network ending on an IP point of presence (PoP) through a protected OC48 link. The availability of the IP path can be simply estimated as:

$$A_{path} = \prod_i A_i = A_{DS3} A_{PoP}^2 A_{ATM\_Net} A_{OC48} A_{IP\_PoP}^2 A_{IP\_net}$$

And the availability of the OC48 link is estimated by:

$$A_{OC48} = 1 - (1 - A_{SimplexOC48})^2$$

3.2 Models for L3 and L4 Type of Resiliency

One of the major drawbacks of the RBD technique is its lack of reflecting detailed resilience behavior that can significantly impact the resulting estimated Reliability/Availability. In particular, it is hard to account for the effects of the fault coverage of each functional block and for the effect of L2 and L3 type of resilience parameters such as detection and recovery times and reroute delays. For e.g. in the IP path of Fig. 3, to estimate the ATM sub-path availability we need to create a model that is reflective of the ATM nodes detailed resilience behavior and their capability of rerouting the traffic around a failed node.

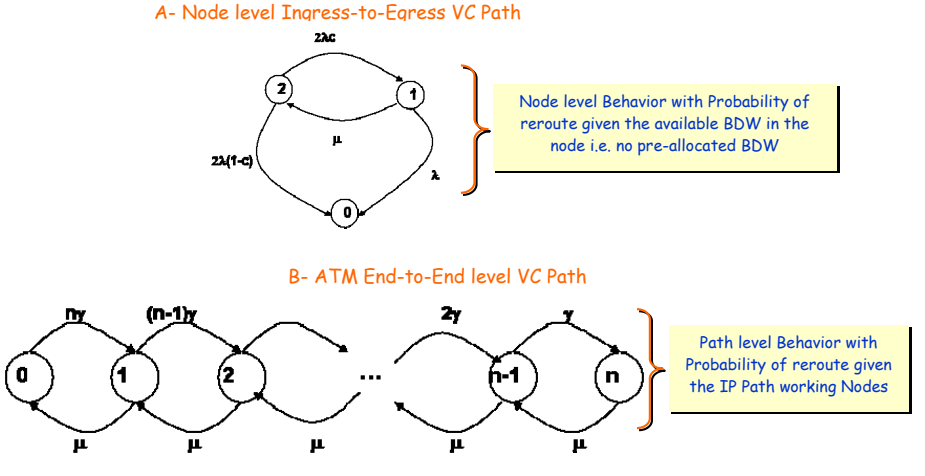

Fig. 4. Markov chain Modeling of an ATM VC Path Reliability Behavior

State space modeling allows tackling complex reliability behavior such as failure/repair dependencies and shared repair facilities. Among these techniques Markov chains has been established as a proven and reasonably easy to use approach in the Telecom industry [7]. Let's consider the ATM VC sub path of our Fig. 3 service path example. Fig. 4 shows the Markov chain models that we have used to estimate the end-to-end VC path availability in order to demonstrate it does meet 99.999% availability under a target node bandwidth available for reroute.

In order to better reflect the L2 resiliency and how it gets impacted by the available node bandwidth to reroute traffic around failed nodes, we constructed a composite Markov chain that mimics the ATM VC path states based on the ATM node behavior. In Fig. 4-B, let γ be the ATM node failure rate and μ the MTTR. The ATM VC path is up if at least one of the n ATM nodes is operational. After a node failure, the VC gets rerouted if the node traffic load allows it. For k=0, 1, …, n-1, state k represents the VC path is up and the failed node has enough bandwidth to reroute, but k out of n nodes are down because either the node is down or it has no available bandwidth to reroute the traffic. State n represent the VC path is down i.e. all the ATM nodes in the path are down or none of them can reroute the traffic. The path availability is estimated as $A_{\mathbf{path}} = 1 - U_{\mathbf{path}}$ and the $U_{\mathbf{path}}$ its unavailability is defined as a function of n, the number of nodes in the path.$U_{\mathbf{path}}$ can be computed using the steady state probability πi of each state i as:

$$U_{path} = \pi_n = \frac{\rho^n n!}{\sum_{k=0}^{n} \rho^k \frac{n!}{(n-k)!}}$$

$$A_{path} = 1 - \pi_n = \sum_{k=0}^{n-1} \rho^k \frac{n!}{(n-k)!};$$

$$\pi_{n-1} = \frac{\rho^{n-1}(n-1)!}{\sum_{k=0}^{n} \rho^k \frac{n!}{(n-k)!}}; \qquad where\ \rho = \frac{\gamma_{node}}{\mu}$$

$$\lambda_{path} = \gamma_{node} * \frac{\pi_{n-1}}{1-\pi_n} \Rightarrow \lambda_{path} = \gamma_{node} * \frac{\rho^{n-1}(n-1)!}{\sum_{k=0}^{n-1} \rho^k \frac{(n-1)!}{(n-k)!}}$$

The node failure rate γ is estimated using the Markov chain depicted in Fig. 4-A. It takes into account the probability of reroute given the available bandwidth in the node and the node infrastructure behavior. State2 represents the node is up and a failure is either covered with a probability c of reroute success, or not covered with (1-c) probability of not rerouting because of lack of bandwidth. A fault is covered if it is detected and recovered from without taking down the service. State1 represents the node is up but in simplex mode with no alternative routes. State0 represents the node down (all routes failed or no capacity available). The node mean time between failures (MTBF) can be estimated by:

$$MTBF = \frac{\lambda(1+2c)+\mu}{2\lambda(\lambda+\mu(1-c))}$$

We have run the model on a network composed of an average of 5 to 6 nodes end-to-end VC path and with an MTTR of < 3 hours and demonstrated that 99.999% VC path availability is reached only if the probability of reroute success is at least 50% given the way the bandwidth has been engineered. Fig. 5 show the resulting availability as function of the probability of re-route given the number of the nodes on the path.

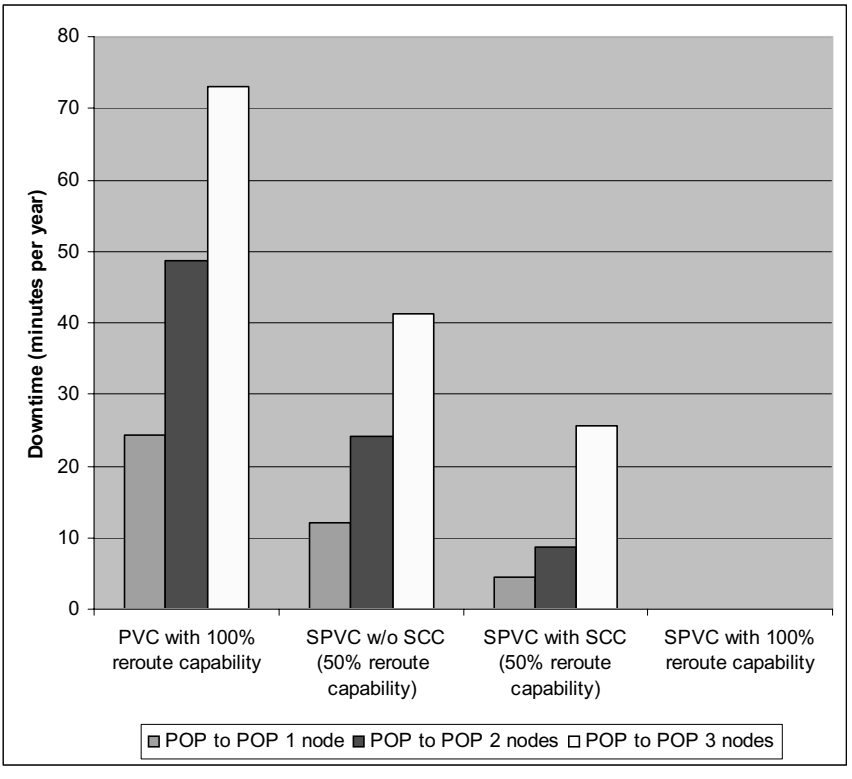

Fig. 5. Service Downtime vs. ATM VC path Reroute Capability

A similar approach to ours has been used in [5] to estimate the service availability for the purpose of a network architecture tradeoff analysis.

4 Towards a Hierarchical Approach for Service Availability Modeling and Measurement

At 10GE line rate packet switching, IP networks service availability is tightly dependent on both the infrastructure it is deployed on, the way it is deployed and the

way the bandwidth is engineered. Separate reliability and performance models do not answer the need to reflect the interdependencies between the L2, L3 and L4 failure modes. For example, in the ATM VC path model of Fig. 4, we have assumed the reroute delay times were quite negligible in terms of service downtime impacts. This is a realistic assumption for an ATM path where recovery times are of the order of the sub second. However, if we wanted to account for the impact of the reroute delays on the path availability as it is the case for a L3/L4 type of resilience behavior, we need to construct a Markov chain that details the path behavioral states when it is in recovery because of reroute delays due to reroute protocols states recovery and re-convergence times.

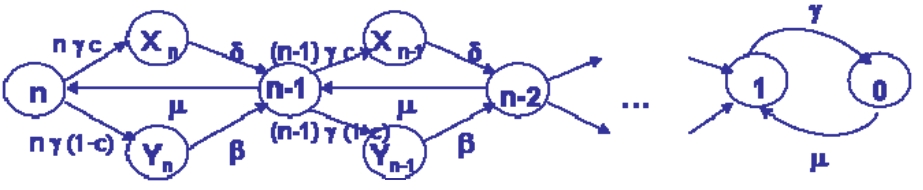

Fig. 6. Markov chain Model of a Service IP Path Reliability Behavior with Reroute Delays

Fig. 6 shows an example of such a Markov chain we have created to estimate the service IP path availability from end-to-end in a multi-services IP network given the reroute delays. The network is designed as a typical resilient VPLS architecture targeted for triple play solution with RSTP rings deployed at the metro access and with IP/MPLS routing at the metro core.

Let γ be the failure rate of the IP node, and μ its MTTR. A node failure is covered with a probability c and not covered with probability 1-c. After a node covered fault the path is up in a degraded mode until a release of the active routing engine activities to the standby one is complete and the traffic is running through the new active routing engine. However, after an uncovered fault, the path is down until the failed node is taken out from the path and the network reconfigured itself with a new routing table regenerated and broadcast. The routing engine switchover time and the network reconfiguration time are assumed to be exponentially distributed with means 1/δ and 1/β respectively. The routing engine switchover time is in the order of the second. However, the path reconfiguration time may be in the order of the minutes. These two parameters are assumed to be small compared to the node MTBF and MTTR hence no failures and repairs are assumed to happen during these actions. The path is up if at least one of its n nodes is operational. The state i, $1 \le i \le n$, represents node i is operational and n-i nodes are down waiting for repair. The states Xn-i and Yn-i ($0 \le i \le n-2$) reflect the path recovery state and the path reconfiguration state respectively. The path availability A(n) is computed as a function of the number of nodes n given by its unavailability computed from the steady state probability πi of each state i as:

$$UA(n) = 1 - \sum_{i=1}^{n} \pi_i$$

We have run our model to show that the end-to-end IP path meet 99.999% voice service availability for various target network dimensioning and an average and max reroute delays. We are currently running the model with various failures/recovery scenarios to characterize the service availability behavior given different network dimensioning targets and variable reroute delays.

However, with pure reliability models it still would not be possible to show the impact of various performances levels at various functional/operational states. On the other hand modeling the performance separately from the reliability misses to reflect failure/repair behavior and makes it difficult to demonstrate an SLA is met under a given engineered bandwidth. A key practical question in network dimensioning for optimal service availability that meet tight SLAs is to estimate the right number of nodes per service path for the optimal load levels that impact the reroute capabilities. To answer such question composite models which combine reliability to performance behavior modeling need to be tailored. These models have to capture the effect of functional degradation based on both performance and availability failure events. An approach to build such models is to use Markov Reward Models [6] which are Markov chains augmented with reward rates r_i attached to the failure/repair states. Different reward schemes can be devised to account for the impact of performance features on the availability. For example for the IP path dimensioning, we are investigating the use of the Markov chain in Fig. 6 augmented with a reward system where ri =1 for the down states and ri=f(p_i,q_i) where p_i is the probability to drop traffic in case of service impacting packet loss and q_i is the service recovery time given i operational nodes in the path and f an appropriately chosen function that reflects the relationship between congestion and recovery time. The recovery time can be defined in turn as a function of the network delay and its jitter.

The state space technique may still suffer from a number of practical limiting factors. As the modeled block complexity grows, the state space model complexity may grow exponentially. For e.g., in the case of the ATM path model we have used a simplified time discrete Markov chain that does not distinguish between hardware and software failures i.e. we assumed the same recovery times for both. It also assumes a common repair facility for the all the nodes (same MTTR for all the nodes). In order to mimic such complex behavior very large Markov chain are needed. This makes the numerical solution of these models a daunting task. Currently, a number of techniques are explored in order to help in limiting the complexity of the numerical resolution of such chains. These techniques include structured analysis of Markov Chains such as the approximation techniques based on fixed point computations, bounding techniques, and hybrid techniques combining simulation and transient numerical analysis.

Our current view is to reduce the Markov Chain network resilience modeling complexity by taking advantage of the communication network specifics based on known information abot its functional and topological behaviors. Since the levels of traffic and the levels of reliability required at each layer of the network architecture are different even though the same service runs across all the layers, a hierarchal modeling approach can be used to aggregate the various layers of resilience behavior in the network with the level of details required for each layer. As we illustrated it in the previous section, the first layer of the modeling consists of defining an RBD that describes the basic functional blocks of the service. Then in turn each functional

block can be estimated by using either a pure availability/reliability model if it is an L1 or L2 type of functional block or a composite model that reflects both the availability and performance if it is a L3 or L4 type of functional block. Hence the choice of the modeling technique suitable for a networking resilience level is now dictated by the need to account for the impact of the resilience parameters on the service availability, the level of details of the node/network/service behavior to be represented and the ease of construction and use of the set of models.

In summary the steps of the approach is as follows:

a) partition the service path into sub paths, each sub path operating according to a set of respective network functions;
b) estimate a reliability measure for each sub path according to the network functions parameters and constraints that impacts it;
c) estimate the service reliability measure over the end to end path as the aggregate of the sub paths reliability measures.

Based on this hierarchical modeling approach, one can show tight reliability/availability SLA targets are met under a given network designed infrastructure with a given engineered bandwidth to provide a set of value added services each one predictable through a set of network functions scalability and robustness attributes.

For example, to engineer the required bandwidth in a resilient network architecture, reliability combined with performance modeling will help in two main aspects. First, it will help identifying and eliminating single points of failure by design. Second, it will help in constructing the optimal and cost effective resilience behavior by design and implementation choices where the network service will gracefully continue operating in the face of a wide variety of traffic anomalies, fault conditions, or operational changes to the network.

5 Summary and Future Directions

In this paper we showed that a multi-services IP network has different layers of resilience. They are basically tied up to the networking infrastructure deployed and the way the latter is engineered to handle the offered services. We have then discussed the issue of estimating the contribution of the 4 different layers of the network resilience to the reliability of the network architecture and the services it offers. We have discussed in particular the challenges posed by measuring the service availability/reliability given the effects of failure modes rooted in both the network infrastructure and the performance behavior of the network. We have then proposed a service availability modeling approach based on a layered structure using increasingly powerful and detailed analytical models that aggregate availability/reliability measures which can be estimated from each resilience layer with the suitable modeling technique. The multi-layered approach combines state-space and non-state space analysis techniques to aggregate availability/reliability measures that can be estimated and proven to meet tight SLA's.

There are a number of investigation leads that we are currently pursuing. Among these, our next step is to run various experiments with our approach to validate and calibrate its viable use for SLAs estimation in terms of end-to-end IP path service

availability/reliability. For example, it would be useful to understand the scalability and limits of the method with the network dimensioning or the mix and makeup of services deployed changes. Second, in validating and calibrating our modeling approach we would like to compare it to the currently used Markov Chain structured analysis approaches.

References

1. P. Buchholz and G. Ciardo , “Tutorial on Structured analysis of Markov chains”; 1st International Conference on the Quantitative Evaluation of Systems (QEST) 2004; September 2004, University of Twente, Enschede, The Netherlands
2. R. Bynum, “Generic Data Communications Services Models” ; IEEE 10GigE p802.3ae and EFM 802.3ah Task Forces; June 2001
3. IETF group work on IP over Resilient Packet Rings (iporpr), http://www1.ietf.org/html.charters/iporpr-charter.html
4. Y. Liu and K.S. Trivedi. A General Framework for Network Survivability Quantification. 12th GI/ITG Conference on Measuring, Modeling and Evaluation of Computer and Communication Systems (MMB) and 3rd Polish-German Telegraphic Symposium (PGTS), Dresden, Germany, September 2004
5. Y. Liu, V. B. Mendiratta, and K. S. Trivedi. Survivability Analysis of Telephone Access Network. 15th IEEE International Symposium on Software Reliability Engineering (ISSRE'04), November, Saint-Malo, Bretagne, France
6. J. Muppala, R. Fricks, and K. S. Trivedi. Techniques for System Dependability Evaluation. Computational Probability, W. Grassman (ed.), pp. 445-480, Kluwer Academic Publishers, The Netherlands, 2000
7. Telcordia GR-512-CORE, issue 2, 1998; GR-929-CORE issue 8, 2002
8. M. Tortorella, Reliability Challenges of Converged Networks and Packet-Based Services. Industrial Engineering Working Paper, February 5th, 2003
9. K.S. Trivedi, “Probability and Statistics with Reliability, Queuing and Computer Science Applications; John Wiley &Sons Publisher, Second Edition, 2002
10. http://www.vpls.org/