IP/MPLS network modeling using Bayesian networks to improve double failure recovery
Stéphen Pirlot, Eric Gnaedinger, René Kopp, Francis Lepage

To cite this version:
Stéphen Pirlot, Eric Gnaedinger, René Kopp, Francis Lepage. IP/MPLS network modeling using Bayesian networks to improve double failure recovery. IEEE International Conference on Industrial Engineering and systems Management IESM 2015, Oct 2015, Sevilla, Spain. hal-01237303

HAL Id: hal-01237303
https://hal.archives-ouvertes.fr/hal-01237303
Submitted on 3 Dec 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
IP/MPLS network modeling using Bayesian networks to improve double failure recovery

Stéphen PIRLOT\textsuperscript{1,2,3}, Eric GNAEDINGER\textsuperscript{1}, René KOPP\textsuperscript{3}, Francis LEPAGE\textsuperscript{1,2}
\textsuperscript{1}Université de Lorraine, CRAN, UMR 7039
Campus Sciences, BP 70239, Vandoeuvre-lès-Nancy
Cedex, 54506, France.
\textsuperscript{2}CNRS, CRAN, UMR 7039, France
\textsuperscript{3}TDF
1 rue Marconi – 57070 Metz, France.
(e-mail\textsuperscript{1,2}: firstname.lastname@univ-lorraine.fr)

Abstract— Protocols engineering of IP/MPLS networks are constantly improving with new separated features and new resilience mechanisms. In the transportation of audiovisual signals domain we must compose with multicast protocols which are designed from other scientific developments. This audiovisual traffic due to his non springy nature presents a very huge sensitivity to network recovery after a failure and these effects can be amplified by end devices (encoding, decoding and MPEG IP encapsulation). In this way when we choose between engineering solutions the unique criterion of availability is not enough, we must complete by an impact analysis on the service made by the network resilience technics. In this paper, we propose a first approach to analyze the behavior of different protocols engineering to improve selection. We propose using Bayesian networks to compare performance on different criteria and we will illustrate with two engineering models. The results focus on a real improvement of availability by choosing the adapted engineering solution.

Keywords — Protocol Modeling, Network Survivability, Bayesian Network, Engineering Choice, Availability, Dependability, Multicast Transport.

I. INTRODUCTION

A network service can be implemented using different ways considering topological and architectural views of the network, considering protocols accumulation and obviously considering client requirements on the quality of service. In the multicast transportation domain the protocols unified under the “multicast VPN” term have proved their fullness and are now available with different variants. Otherwise, the client requirements are rising while we are observing a clear fall of the performance about our transmission links which constitute the network infrastructure and especially on the availability point of view. Then we must strengthen the mesh of our network and improve our engineering solutions to use this entire new infrastructure for all point of service.

Networks specialized in audiovisual broadcasting possess particularities which are not a prerequisite for an efficient telecommunication network. Then a traditional network could be with a medium performance and could accept frequent rerouting or congestion on the contrary of an audiovisual network.

The goal of all networks is to be the more stable and the more resilient. In this context where we are talking about network survivability [1-2], the problems concerning failure resistance or cyber-attack are primordial. There are also other solutions as those based on autonomic networks [3-4] which consist to limit human interactions with the network. But these technics are not natively implemented in routers because of the long convergence time to a new steady state of autonomic systems. In addition we want that all recovery decisions of the network are totally automatic to react as fast as possible to a failure. Most of the time, engineers have different choices of implementation for the solution.

For the same physical structure, parts manufacturers allow to separate data for each client using network services related to a client. This possibility enables for each client to use his own resources and his own protocol engineering correctly adapted to his requirements.

Network services are implemented for each client and it is possible to adapt all the protocols for each client demand. In this context the customer is the final receiver on TV and clients are TV stations which pay for a broadcasting service.

Because of the innovation of technologies and all limitations, engineers are encourage to evolve engineering existing solutions to new innovative solutions which are bringing better performance. The choice of evolution and the comparison between two engineering solutions is most of the time conditioned by the experience of systems architects and with all the technical data given by parts manufacturers or by realizing prototype. The aim of this paper is to propose a decision support for the development of an engineering solution specialized in the multicast stream transportation guarantying all the above criteria. Although we could focus on every aspect of RAMS frameworks [5], only the customer availability will be considered. The first part will expose the modeling problematic and the target of this study. The second will explain the two engineering solutions, then the last part will present on simple cases how to apply this modeling solution and will show us on a real case the contribution of each solution to conclude this study.

II. PROTOCOL MODELING

Availability study for a client’s service is based on the physical infrastructure analysis but it is especially based on the way of all protocols work in. Availability of the
infrastructure bound to the service is obtained from the availability of each component of the network, for our case routers and links in optical fiber or microwave and from the constituted topology of these elements. When it is possible, the real availability of these elements will be used.

There are many approaches to model the availability of an IP network depending on the physical infrastructure like fault-tree-analysis, Markov chains or Bayesian networks [6-9]. Measured availability will be the same for each used model. In this study we will concentrate on Bayesian networks.

Very used in dependability field, Bayesian networks are probabilistic models utilized to focus on some precise characteristics of a system or a sub-system. They present in the form of directed acyclic graphs all the functional probabilities of the different elements and their interactions with the general state of the system [10]. This kind of model is used by system engineers to model hazards of complex systems as automobile factories, nuclear power plants or fighter jets. Bayesian networks allow predicting the global system behaviors, to diagnose the reason of a noticed phenomenon in the system but also to control the system behaviors.

In this study we will focus on the system’s behavior and we will look for modeling global availability of the system with Bayesian networks. It is possible to create such network by using the physical characteristics of the components. Links represent dependencies between the different variables (nodes1). The nodes of the network correspond to the random variable used in the calculations. It exists two kinds of nodes:

- **Parent node**: which contain a probabilistic distribution (the value of each component’s availability, theoretical or real, is placed here)
- **Child node**: which characterize random variables in the form of conditional probability table (the target node, will be for us the node which modeling the system’s state, is this kind of node).

Elaboration of the Bayesian network is realized in order to faithfully reproduce the behavior of the different protocols. About this study, we will not be interested by switchover phenomenon and protocols’ convergence that can last some tens seconds; we will especially focus of the gain of availability of the new solution versus the loss of system’s stability (see below). A model must evidently represent faithfully the real system. For this it must present the protocol’s features simply and accurately, this implies a model using enough child nodes.

This way is the common way to complete a Bayesian network to understand the system’s behavior. At this point we remain at the level of a fault tree analysis. When we are choosing for engineering solutions, it is quite simple to know which case will have the best availability by analyzing all the possible failures that each engineering solution can deal with. But modeling the solution must give additional functional parameters of the network to qualify some eventual loss of performance.

### III. STUDIED PROTOCOLS

With this study, we are looking for some decision about which engineering solution provides the best quality of service basing on theoretical data. In a network dimensioned for audiovisual transportation, technical constrains are strong on certain criteria. In addition we are talking about broadcasting solution through an entire network to reach services’ points separated more than 1000 km using hundreds of routers. For everything working, we use multicast streams because the client wants a point to multipoint service. Today we have at disposition different kind of transportation of multicast streams over an IP/MPLS network and each solution presents its own advantages. Historically, it exist an implemented solution over the network for broadcasting national programs, but it is planned to change for a more recent engineering solution.

The first solution is based on a ring protection (as RSTP solutions [11]) and is called imbricated rings solution. The second solution uses multicast broadcasting solutions and is called multicast tree solution.

#### A. Imbricated rings solution

This solution uses imbricated rings architecture (main ring S1-S2-A-B and sub-ring A-D-B) and on each ring an own ring protection is implemented (Figure 1). Routers behave as switches in this case. The main ring is managed as a simple ring by RSTP. The sub-ring is treated by RSTP as a ring because the protocol consider that the link between A and B is always operational and so the RSTP blocking port can only exists over the sub-ring A-D-B. The stream is generated by the two sources located on the routers S2 and S1, and it is broadcasted over the entire network using the topology made by RSTP (the cross on the scheme shows us the RSTP blocking ports). Only one source can be active at a given time but it is possible to choose which one works.

In order to protect the network from a global congestion, engineers conceive this solution with special filters on the routers which join different rings (here A & B). These filters are blocking broadcasted data circulating on the sub-ring to supply the main ring, limiting broadcast storm phenomena to the sub-ring only and not over all the network.

![Fig 1. Broadcasting sample in the imbricated rings architecture](image)

---

1 In this paper, the node terminology always refers to a Bayesian network node and not at a telecom network node.
This engineering solution is quite simple and is well dimensioned for broadcasting a stream over the global network. It reacts rapidly to simple failures, but possesses some blocking cases with double failures. The Figure 2 explains two blocking situations.

In the first case (a), there is no failure in the sub-ring, so the sub-ring’s protection is not activated and the router D can’t get the stream. In the second case (b), there is no failure on the west ring so the broadcast is blocked on the router F.

There is also the filter on the router A which will block the stream to the west ring so the broadcast is blocked on the router F.

In addition this architecture in imbricated rings allows only the ring usage and so there are only two injections possible for a sub-ring. Finally it is only possible to handle two national sources so it is impossible to use some local source.

This solution is exposed to a recrudescence of simple failures and especially on double or triple failures. To find a solution, we must reinforce the architecture with more interconnection. The imbricated rings solution cannot completely take advantage of this network densification so we opt for another solution, the multicast tree solution, which solve these failure cases and clearly improve the system availability.

B. Multicast tree solution

A protocol engineering solution is always studied in relation to the physical infrastructure. Then this solution lean on two functional layers: the VPRN [12] layer which emulate virtual routers and the VPLS [13] layer which emulates virtual switches. The dichotomy is historical and technical because only the most powerful routers (nearest routers of the sources) can use VPRN features; the others will use the VPLS layer (this represents about half of the network components for our network). Figure 3 presents the dichotomy and the used technics to transport the multicast stream.

About the multicast stream, it is broadcasted in the entire VPLS from a single and unique virtual router. For the VPRN side, the PIM protocol [14] builds a multicast tree based on the multicast demands to distribute the stream only to the routers with a connected client or to the routers connected to VPLS which require the stream (using IGMP protocol [15]).

The main contribution of this solution is that every connection of a service point will be able to be used to reinforce the resilience of the system; we also can exclude some links of this service. Furthermore, VPLS can supply the stream to the VPRN layer to avoid the isolation of a part of the network because of a misplaced double failure. So as a physical solution exists to distribute the stream to the destinations, the system will work. Finally it is possible to use more than two main sources.

Then both of the cases presented in the paragraph A are solved by this new engineering solution: it represents an incontestable gain of availability for the system.

Anyway from the functional point of view, all the routers from a same VPLS (so all the members of a sub-ring) will be supplied by the same virtual router. This represents a true weakness in comparison of the historical solution because the blocking port is always positioned at the half of the ring so half of the routers are supplied from a side of the ring, and the other half are supplied by the other side of the ring (Figure 4).

The system can be weakened because many routers in the VPLS side are bound to a unique router which forwards the stream (in this situation the router B). Admittedly all the VPLS members will topple over the second router (here the router A), but all of the points of the service in this VPLS will be impacted by this switchover.

We are focusing on the compromise to establish between the gain of availability and the regression in term of performance linked to switchover mechanism.
IV. MODELING SOLUTIONS

As indicated above, we will use Bayesian networks to model availability of the two engineering solutions. But to model the fact that a system is more sensitive about rerouting considerations (or switchovers), we will use multi-states characteristics of Bayesian networks. As a matter of fact, each node of the Bayesian network (or random variable) possesses different values, and the choice is not limited to Boolean values as “Working” or “Not working”. For example let’s take a control valves system which his mission is to let pass a liquid stream or to block it. A valve possesses three states: Working, Blocked in opened position, Blocked in closed position. According to different failures cases, the system can still function and these functional conditions could be used. This theory is able to be applied to our case. We will use estimated availability with the domain (here only one router).

The source streams which come at S1 & S2 will always be available and we will use estimated availability with the following values:
- Router availability = 0.999999
- Link availability = 0.9995

On Figure 5 we note that in the second solution, the VPRN side is not usable on the router D. The broadcast will be done by the router B which will broadcast on the entire VPLS domain (here only one router).

In the following examples, we will show that this state utilization will permit to quantify the loss of availability on the nominal way versus the gain of global availability. In other words, is the availability of the system enough increasing to balance the rise of rerouting probability?

A. Feasibility demonstrating

Here we are going to show that this modeling way is feasible and corresponds to an expected behavior with obvious cases. In the following situations, the two sources S1 & S2 will have a stream at disposal and the studied router will be the router D located on the bottom on the scheme. The solution in imbricated rings will be placed on left and the multicast tree solution on the right.

The stream follows the same way on nominal situation in both solutions and the new engineering solution will not degrade any performance. The only difference between these solutions is about failure detection. Indeed if the router B is isolated in the first solution, there will not have any rerouting and the system will be in failure state (cf. Fig 2).

When modeling with Bayesian networks the multicast tree solution as presented in Figure 6, we can find different elements as parent nodes (in blue) and some random variables created to easily aggregate treatment possibilities of the stream represented as child nodes (in yellow).

To simplify the analysis, we will check if each part of the network is able to get the stream. For example, the node “A Supplied” has for truth table:
- Nominal state: Never because the router A only broadcast the stream if B is not able to do it.
- Rescue state: If router S2, router A and also the link between S2 and A work, the node will be in this state.
- Failure state: Every other case.

With this principle we can complete the model and do the same for the imbricated rings solution by considering the blocking case of the isolated router B. It is quite simple to compare the performance by using the inference algorithm included in Bayesian modeling software. We get the working probabilities of the service on the router D reassembled in the Table I. The Δ column presents the differences.

This model can directly show the availability gain by comparing probabilities to be in a failure state between the two solutions. It is a theoretical case with estimated values and that is why we are observing a light gain (approx. 16s/year).

Now considering that this model is able to show the gain of availability, we are looking to highlight what we are losing with an unfavorable case.
with the ring protection. For the multicast tree solution, it is the router C which distributes the stream over the VPLS, and then all the VPLS side routers will get the stream from the router C. Because of this behavior we are in a negative situation by the fact that the router D is able to get the stream in the nominal way by passing the routers chain from the router C. Anyway we still have a gain of availability because the new solution still can correct the failure case of isolated router A (which forwards the stream to the router D in the imbricated rings solution).

The results of this model with Bayesian networks are resumed in the Table II.

Here we have an interesting result: in this example the availability is improved but we observe a loss of probability to be in the nominal state. We win 24s/year of availability with the new solution on the 373s/year (+6.4%) that we got in the actual solution. Then we increase the risk to be in a rerouting situation of 4.5h/year on the 13.4h/year (+33.6%) of the ring solution. This case is unfavorable because by extending rerouting risks, the performance decreases for the audiovisual network.

The next part will permit to quantify the performance of the new solution with an infrastructure based on an inspired real case.

C. Modeling a real situation

This part will show us how the new engineering solution will be able to be deployed over a real network and we will see how it contributes to solve double failures that are actually blocking in the existing solution. The architecture is shown in Figure 8.
With this study based on a real architecture, first of all we observe a gain of 164s/year which correspond to a 28.4% gain compared to the 557s of annual failure. On the rerouting side, we note an improved probability to be in a rescue state of 24min/year against the 27.7h/year which correspond of an increase of 1.4% of rerouting. This difference with the precedent case comes from the fact that the main ring can be supplied by the sub-ring in the multicast tree solution.

This illustrate that in this real case the availability improvement is more important than the increase of the rerouting probability. In this way, the new engineering solution works as expected. This study quantifies the gain and the inconvenient of the new engineering solution. It will be extended to the entire network and already reassure the choice to develop this new solution.

V. CONCLUSION

Multi-states characteristics of Bayesian networks provide us a deeper analysis than a simple fault tree analysis study. This paper presents its practical application on a network in a telecommunication context. For implementing a new protocol engineering solution, we could quantify at the same time availability benefits aspects but also the compensation inducted by switchovers situations. The results are in favor of the new engineering solution by introducing new routers with improved features, placed on an optimal way to reduce undesirable effects.

The future of this study will be generalized in that way to generally optimize the network architecture. This modeling solution highlights benefits and losses of each solution by using real data. We could imagine apply this technique to estimate the gain on other modalities, and precise decisions. With this study, the instant switchover phenomenon was not taken into account even it is a problematical topic on audiovisual networks; the following of this work will be able to be concerned by this.

VI. THANKS

This work is performed in a PhD thesis context in collaboration between CRAN and TDF, and more precisely with the conception team of TDF Metz (France).

VII. GLOSSARY

| IGMP | Internet Group Management Protocol |
| MPEG | Moving Picture Experts Group |
| MPLS | MultiProtocol Label Switching |
| Multicast VPN | Multicast over VPN |
| PIM | Protocol Independent Multicast |
| RSTP | Rapid Spanning Tree Protocol |
| VPLS | Virtual Private LAN Service |
| VPN | Virtual Private Network |
| VPRN | Virtual Private Routed Network |

REFERENCES