



HAL
open science

Modélisation d'un réseau IP/MPLS par réseaux Bayésiens pour améliorer le recouvrement d'une double défaillance

Stéphen Pirlot, Eric Gnaedinger, René Kopp, Francis Lepage

► **To cite this version:**

Stéphen Pirlot, Eric Gnaedinger, René Kopp, Francis Lepage. Modélisation d'un réseau IP/MPLS par réseaux Bayésiens pour améliorer le recouvrement d'une double défaillance. 6e Journées Doctorales / Journées Nationales MACS, JD-JN-MACS 2015, Jun 2015, Bourges, France. hal-01224925

HAL Id: hal-01224925

<https://hal.science/hal-01224925>

Submitted on 5 Nov 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.

Modélisation d'un réseau IP/MPLS par réseaux Bayésiens pour améliorer le recouvrement d'une double défaillance

Stéphane PIRLOT^{1,2,3}, Eric GNAEDINGER¹, René KOPP³, Francis LEPAGE^{1,2}

¹ Université de Lorraine, CRAN, UMR 7039

Campus Sciences, BP 70239, Vandœuvre-les-Nancy Cedex, 54506, France.

(e-mail: prénom.nom@univ-lorraine.fr)

² CNRS, CRAN, UMR 7039, France

³ TDF

TDF Metz – 1 rue Marconi – 57070 Metz, France.

rene.kopp@tdf.fr

Résumé— Les ingénieries protocolaires des réseaux IP/MPLS s'enrichissent constamment de nouvelles fonctionnalités de cloisonnement et de nouveaux mécanismes de résilience. Dans le domaine du transport de signaux audiovisuels nous devons en outre composer avec les protocoles multicast qui nécessitent du reste des développements spécifiques. Ce trafic audiovisuel du fait de sa nature non élastique présente une très grande sensibilité à la cicatrisation du réseau dont les effets peuvent être amplifiés par les équipements d'extrémité des chaînes techniques (codage, décodage et encapsulation MPEG IP). Ainsi lors du choix des ingénieries le seul critère de la disponibilité n'est pas suffisant, il faut le compléter par l'analyse d'impact sur le service provoqué par les phases de résilience du réseau. Dans cet article, nous proposons une première approche pour analyser le comportement de différentes ingénieries protocolaires à des fins de sélection. Nous proposons d'utiliser les réseaux Bayésiens pour en quantifier le gain et la perte de performances, nous l'illustrons sur deux ingénieries. Les résultats montrent une réelle amélioration de la disponibilité en choisissant l'ingénierie adaptée.

Mots-clés— Modélisation protocolaire, Survivabilité, Réseaux Bayésiens, Choix d'ingénierie, Disponibilité, Optimisation réseau, Transport multicast.

I. INTRODUCTION

Un service réseau peut être implémenté de différentes manières selon la topologie et l'architecture du réseau en place, selon les piles protocolaires disponibles et évidemment selon les exigences du client en matière de qualité de service. Dans le domaine du transport multicast les protocoles rassemblés sous le terme VPN multicast ont atteint un bon degré de maturité et sont maintenant disponibles avec plusieurs variantes. Par ailleurs, les exigences de nos clients se renforcent alors que nous constatons un net recul des performances des liaisons de transmission qui constituent l'infrastructure du réseau notamment en taux de disponibilité.

Nous devons donc renforcer le maillage du réseau et faire évoluer nos ingénieries pour mettre à profit la multiplicité d'adductions de nos points de service.

Les réseaux spécialisés dans la diffusion de l'audiovisuel possèdent des particularités qui ne sont pas toutes adressées par les réseaux de télécommunications. Ainsi un réseau traditionnel pourra être d'une performance moyenne et accepter des reroutages fréquents ou de la congestion pour ses trafics contrairement à un réseau dimensionné pour l'audiovisuel.

L'objectif de tout réseau est d'être le plus stable et le plus résilient possible. Dans ce contexte où l'on parle de survivabilité des réseaux IP [1-2], les problématiques de résistance aux pannes ou à des cyber-attaques sont primordiales. De plus on souhaite que les décisions de cicatrisation du réseau soient automatiques de manière à réagir le plus rapidement possible à une panne. Il arrive souvent que les ingénieurs se retrouvent confrontés à différents choix d'implémentation pour une même solution.

Pour une même infrastructure physique, les équipementiers permettent de cloisonner les données relatives aux clients au sein de services réseau propres à chaque client. Cette possibilité permet à chaque client de disposer de ses propres ressources et d'une ingénierie protocolaire adaptée à ses besoins.

Les services réseau étant implémentés pour chaque client, il est possible d'adapter les différents protocoles aux exigences de chaque client.

Ces nouvelles technologies et ces limitations incitent les ingénieurs à faire évoluer les ingénieries vers des solutions plus innovantes et qui semblent apporter de meilleures performances. Le choix de l'évolution et la comparaison entre deux ingénieries est très souvent conditionné par l'expérience des architectes réseau et des données techniques fournies par

les équipementiers ou par la réalisation de maquettes. L'objectif de cet article est de proposer une aide à la décision pour l'évolution d'une ingénierie pour le transport de flux multicast répondant aux critères ci-dessus. La première partie exposera la problématique de modélisation et les objectifs de l'étude, la seconde expliquera les deux ingénieries étudiées, enfin la dernière partie montrera sur des cas simples comment appliquer la modélisation et montrera sur un cas réel l'apport de chaque solution ainsi que les conclusions de l'étude.

II. MODELISATION PROTOCOLAIRE

L'étude de la disponibilité d'un service client repose sur l'analyse de l'infrastructure physique mais aussi et surtout de la manière dont les protocoles fonctionnent dessus. La disponibilité de l'infrastructure liée au service s'obtient à partir des taux de disponibilité de chaque constituant du réseau, pour notre cas des routeurs et des liaisons en fibre optique ou des faisceaux hertziens et à partir de la topologie qu'ils forment. Dans la mesure du possible les taux de disponibilité réels seront utilisés.

Il existe différentes approches pour modéliser la disponibilité d'un réseau IP en se basant sur l'infrastructure telles que l'arbre de défaillance, les chaînes de Markov ou encore les réseaux Bayésiens [3-6]. La disponibilité calculée est la même quel que soit le modèle utilisé. Dans cette étude nous emploierons des réseaux Bayésiens.

Très utilisés en sûreté de fonctionnement, les réseaux Bayésiens sont des modèles probabilistes mettant en évidence les caractéristiques d'un système ou sous-système. Il présente sous la forme d'un graphe orienté sans circuit les probabilités de fonctionnement des différents constituants et leurs interactions avec l'état général du système [7]. Ce genre de modèle est utilisé par les ingénieurs systèmes afin de calculer les risques sur des systèmes complexes comme des usines automobiles, des centrales nucléaires ou des avions de chasse. Les réseaux Bayésiens permettent de prévoir le comportement d'un système, de diagnostiquer les causes d'un phénomène observé dans le système mais aussi de contrôler les comportements d'un système.

Dans notre étude le système est un service audiovisuel délivré en un point. Nous allons chercher à quantifier sa disponibilité globale via les réseaux Bayésiens. Il est possible de créer un tel réseau en s'appuyant sur les caractéristiques physiques des équipements. Les liens représentent les dépendances entre les différentes variables (nœuds¹). Les nœuds du réseau correspondent à des variables aléatoires qui sont utilisés dans les calculs. Il existe deux types de nœuds :

- *les nœuds parents* : qui contiennent une distribution de probabilité (les valeurs des taux de disponibilités théoriques ou mesurés sont placées ici)
- *les nœuds enfants* : qui caractérisent des variables aléatoires sous la forme d'une table de probabilité conditionnelle (le nœud cible qui sera chez nous le nœud modélisant l'état du système est de ce type).

L'élaboration du réseau Bayésien est réalisée dans le but de retranscrire les comportements des différents protocoles. A propos de cette étude, on ne s'intéressera pas aux phénomènes de bascules et de convergences des protocoles qui peuvent durer plusieurs dizaines de secondes; on s'intéressera surtout à l'apport de la disponibilité de la nouvelle solution versus la

perte de stabilité du système (voir plus loin). Un modèle doit bien sûr représenter la réalité de manière fidèle. Pour cela il doit retranscrire le fonctionnement du protocole de manière simple et précise, ce qui implique d'utiliser un nombre de nœuds enfants suffisants.

Il s'agit d'une façon commune de renseigner un réseau Bayésien pour comprendre le comportement d'un système. A ce stade on reste au niveau d'une analyse d'arbre de défaillance. Parmi le choix des ingénieries, il est assez simple de savoir laquelle aura la meilleure disponibilité en analysant les cas de panne qui peuvent être gérés par telle ou telle ingénierie. Mais le modèle doit aussi pouvoir fournir d'autres paramètres de fonctionnement du réseau afin de qualifier les éventuelles pertes de performances.

III. PROTOCOLES ETUDIÉS

Avec cette étude, on va chercher à décider quelle ingénierie protocolaire est plus intéressante en se basant sur des données théoriques. Dans un réseau dimensionné pour transporter de l'audiovisuel, les contraintes techniques sont fortes sur certains critères. De plus il est question de solutions de diffusions à travers le réseau complet pour atteindre des points de services parfois distants de plus de 1000 km. Pour que tout fonctionne, des flux multicast sont utilisés car le service de distribution est de type point vers multipoint. Il existe maintenant différentes façons de transporter des flux multicast sur un réseau IP/MPLS et chacune a ses avantages. Historiquement, il existe une solution implémentée pour la diffusion de programmes nationaux, mais il est envisagé de migrer vers une ingénierie plus récente.

La première se base sur une solution de protection en anneau (telle que RSTP [8]) et sera appelée solution en boucles imbriquées. La seconde utilise des techniques de distribution en arbre appelée arbre de diffusion.

A. Ingénierie en boucles imbriquées

Cette solution utilise une architecture en boucles imbriquées (boucle principale S1-S2-A-B et sous-boucle A-D-B) et dans chaque boucle une protection de l'anneau est implémentée (Figure 1). Les routeurs se comportent comme des commutateurs dans ce cas. La boucle principale est gérée comme une simple boucle par RSTP. La sous-boucle est vue par RSTP comme une boucle car le protocole considère que la liaison entre A et B est toujours opérationnelle et donc la coupure RSTP ne peut exister que dans la sous-boucle A-D-B. Le flux est pris en charge aux deux sources (Routeurs S2 et S1) et est diffusé en broadcast dans tout le réseau en suivant la topologie RSTP (les croix montrent où se situent les coupures RSTP). Une seule source est active à la fois mais il est possible de choisir celle qui fonctionne.

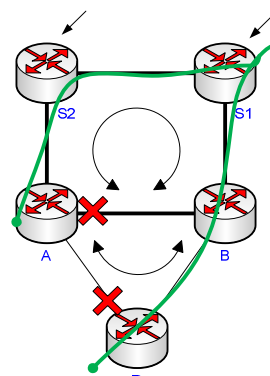


Fig 1. Exemple de diffusion broadcast dans une architecture de boucles imbriquées

¹ Dans cet article, la terminologie *nœud* fait toujours référence à un nœud du réseau Bayésien et non d'un réseau de télécommunication.

Afin de protéger le réseau d'une congestion globale, il existe des filtres anti-retours sur les routeurs faisant la jonction entre les différentes boucles (ici A & B). Ces filtres empêchent le trafic circulant dans la sous-boucle de retourner dans la boucle principale, limitant les risques de tempête de broadcast à la sous-boucle et non au réseau complet.

Cette ingénierie est assez simple et caractéristique d'un flux ayant besoin d'être diffusé sur un réseau global. Elle réagit très bien aux cas de simples pannes, mais possède certains cas de blocages en cas de double panne. La Figure 2 montre deux cas de panne bloquants.

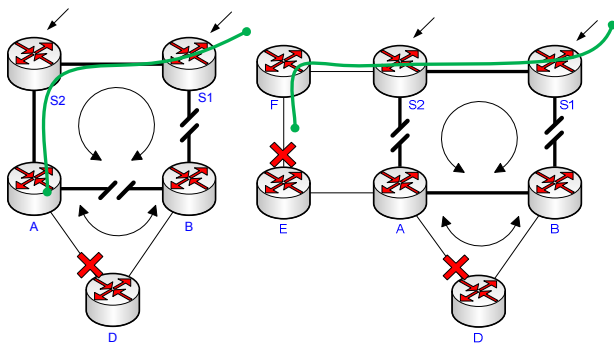


Fig 2. Deux cas de panne bloquants pour les boucles imbriquées

Dans le premier cas, pannes des liaisons A-B et S1-B, il n'y a pas de panne dans la sous-boucle, donc la protection de la sous-boucle ne s'active pas et le routeur D ne peut plus obtenir le flux. Dans le second cas, pannes des liaisons S2-A et S1-B, il n'y a pas de panne dans la sous-boucle ouest donc pas de changement de topologie donc le flux reste bloqué au routeur F. Il y a également les filtres anti-retours qui bloqueraient le flux s'il arrivait à passer jusqu'au routeur A. Le constat de cette panne est qu'il n'est pas possible pour une sous-boucle de réalimenter la boucle principale.

De plus cette architecture en boucles imbriquées ne permet que l'utilisation de boucles et donc seulement deux injections dans une sous-boucle. Enfin il n'est possible de gérer que deux sources nationales et il est impossible de mettre en place une source locale.

Cette solution se retrouve confrontée à une recrudescence des pannes et notamment de doubles pannes voire triples. Pour y remédier, un renforcement de l'architecture par bouclage et dans le prolongement par maillage s'est engagé. L'ingénierie en boucles imbriquées ne pouvant exploiter pleinement cette densification du réseau nous avons opté pour une solution avec arbre multicast, permettant de solutionner ces cas de panne et ainsi améliorer grandement la disponibilité du système.

B. Ingénierie avec arbre multicast

Une ingénierie protocolaire est toujours étudiée par rapport à l'infrastructure physique. Ainsi cette solution s'appuie sur deux niveaux fonctionnels : le niveau VPRN [9] qui va simuler des routeurs virtuels et le niveau VPLS [10] qui va simuler des commutateurs virtuels. La dichotomie est historique et technique car seuls les routeurs les plus puissants (les plus près des sources) peuvent utiliser le VPRN, les autres utiliseront le niveau VPLS (cela représente plus de la moitié des équipements du réseau). La Figure 3 présente la dichotomie et les techniques utilisées pour faire transiter le multicast.

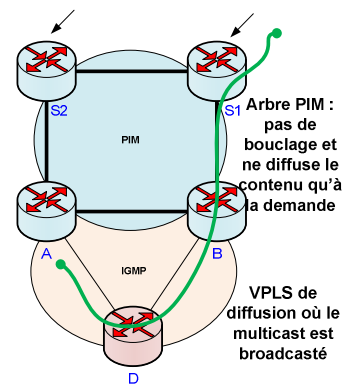


Fig 3. Présentation de la solution utilisant un arbre de diffusion multicast

Au niveau du flux multicast, il est diffusé dans les VPLS par broadcast provenant d'un seul et unique routeur virtuel. Pour les VPRN, le protocole PIM [11] gère un arbre multicast afin de ne diffuser le flux qu'aux routeurs connectés à des clients ou des VPLS demandant le flux (via le protocole IGMP [12]).

L'apport important de la solution est que toutes les adductions d'un point de service pourront être mises à contribution pour renforcer le niveau de résilience. A noter que l'on peut aussi exclure des adductions. En outre, les VPLS peuvent alimenter les routeurs virtuels afin d'éviter l'isolement d'une partie du réseau avec une double panne mal localisée. Tant qu'il existe physiquement une solution pour distribuer le flux aux routeurs de destination, le système pourra fonctionner. Enfin il est possible d'utiliser plus de deux sources principales.

Ainsi les deux cas de pannes évoqués dans le paragraphe A sont solutionnés par cette nouvelle ingénierie : cela représente un gain incontestable de disponibilité pour le système.

Cependant du point de vue fonctionnel, tous les routeurs d'un même VPLS (donc d'une sous-boucle) vont se retrouver alimentés par le même routeur virtuel. Cela représente une faiblesse par rapport à la solution historique car avant, la moitié de la sous-boucle se retrouvait alimentée d'un côté tandis que l'autre moitié était connectée à une autre partie du réseau (Figure 4).

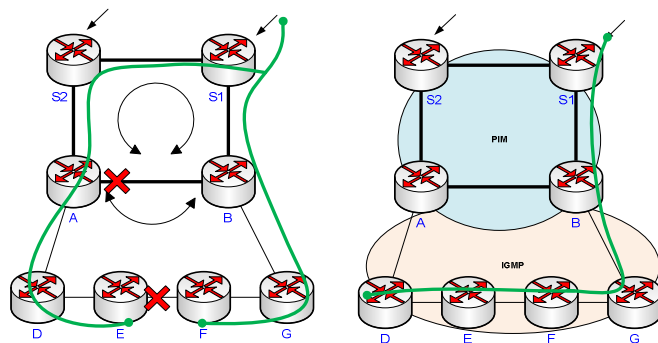


Fig 4. Diffusion dans les deux ingénieries

Le système peut se retrouver affaibli par le fait qu'un grand nombre de routeurs se retrouve dépendant d'un seul routeur (ici B). Certes l'ensemble du VPLS basculera sur l'autre routeur (dans notre cas sur A), mais tous les points de service de ce VPLS subiront un impact lié à cette bascule.

Nous mettons ici en évidence le compromis à établir entre le gain en taux de disponibilité et la régression en termes de performances liés aux impacts de bascule.

IV. MODELISATION DES SOLUTIONS

Comme indiqué précédemment, on va utiliser les réseaux Bayésiens pour modéliser la disponibilité des deux ingénieries. Mais pour modéliser le fait qu'un système est plus sensible que l'autre aux reroutages (ou bascules), on va utiliser les caractéristiques multi-états des réseaux Bayésiens. En réalité, chaque nœud d'un réseau Bayésien (ou variable aléatoire) peut avoir différentes valeurs, et ce choix ne se limite pas à des états booléens tels que « Fonctionne » ou « Ne fonctionne pas ». Par exemple prenons un système de vannes qui a pour mission de laisser passer un liquide ou de le bloquer. Une vanne possède trois états : Fonctionne, Bloquée en position ouverte, Bloquée en position fermée. En fonction des différents cas de pannes, le système peut continuer de fonctionner et ces conditions de fonctionnement peuvent être utilisées.

Cette théorie est applicable à notre cas. On va utiliser trois états pour modéliser des comportements de bascules et les cas de pannes :

- *Etat nominal* : Lorsqu'il n'y a aucune panne sur le chemin principal, le flux utilise ce nœud. C'est l'état normal de fonctionnement.
- *Etat secours* : Lorsqu'une panne se produit sur le chemin principal, le système étant structuré pour résister à n'importe quelle panne, ce dernier continue de fonctionner mais dans un état dégradé, impliquant des reroutages. Pour prendre en compte cet état dégradé, cet état fonctionnel a été créé. Le système continue de remplir sa fonction dans cet état.
- *Etat panne* : Enfin lorsque le système est soumis à deux pannes ou plus qui empêchent le système de fonctionner, le nœud est déclaré en état de panne.

Dans les exemples ci-dessous, on va montrer que cette utilisation d'états va nous permettre de quantifier la perte de disponibilité en chemin nominal versus le gain de taux de disponibilité global. En autres termes, la probabilité de fonctionnement du système augmente-t-elle assez pour compenser la hausse de probabilité de reroutage ?

A. Démonstration de faisabilité

Ici on va chercher à montrer que cette façon de modéliser les solutions est réalisable et conforme à ce qui est attendu avec des cas évidents. Dans les cas suivants, les deux sources S1 & S2 auront le flux à disposition et le routeur étudié sera le routeur D placé en bas de chaque schéma. L'ingénierie en boucles imbriquées est placée à gauche et la solution en arbre est sur la droite.

En termes de taux de disponibilité estimés, les flux sources arrivants sur S1 & S2 sont toujours disponibles et on utilisera aussi les données suivantes :

- *Disponibilité routeur* = 0.99999
- *Disponibilité de la liaison* = 0.9995

Sur la Figure 5 on note que dans la seconde solution, la partie VPRN n'est pas présente sur le routeur D. La diffusion se fera par le routeur B qui diffusera dans tout le VPLS (ici un seul routeur).

Le flux suit le même chemin en situation nominale aussi la nouvelle solution ne dégradera aucune performance. La seule différence se fait au niveau de la détection de panne. En effet si le routeur B se retrouve isolé dans la première solution, il n'y aura pas de reroutage et on sera dans un cas de panne (cf. Fig 2).

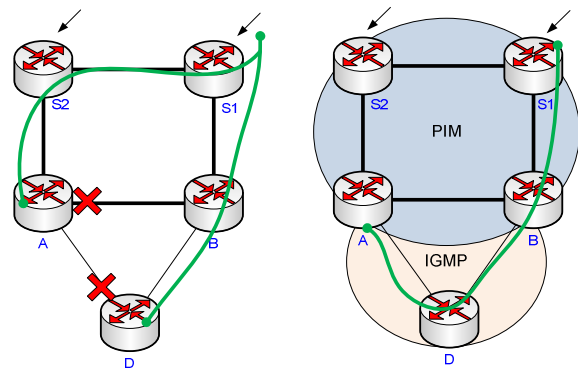


Fig 5. Premier cas pour prouver la faisabilité

Lors de la modélisation en réseau Bayésien de la solution en arbre telle que présentée en Figure 6, on peut y retrouver les différents constituants en tant que nœuds parents (en bleu) et des variables aléatoires créées pour faciliter l'agrégation des possibilités de traitement du flux modélisée par les nœuds enfants (en jaune).

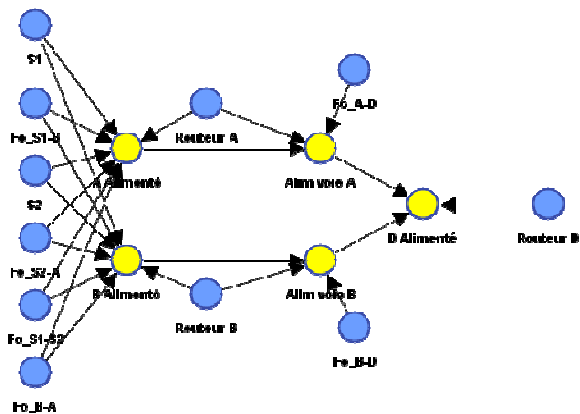


Fig 6. Modèle Bayésien de la solution en arbre du premier cas

Pour simplifier l'analyse, on va vérifier si chaque partie du réseau va être apte à obtenir le flux. Par exemple, le nœud « A Alimenté » aura comme table de vérité :

- *Etat nominal* : jamais car le routeur A fournit le flux uniquement si B n'est plus apte à le faire.
- *Etat secours* : si les routeurs S2 et A ainsi que la liaison entre S2 et A fonctionnent, ce nœud sera dans cet état.
- *Etat de panne* : Tous les autres cas.

On peut alors selon ce principe compléter le modèle et faire de même pour l'ingénierie en boucles imbriquées en prenant en compte le cas de panne bloquant de l'isolement du routeur B. Il est simple de comparer les performances à l'aide de l'algorithme d'inférence inclus dans les logiciels de modélisation des réseaux Bayésiens. On obtient les probabilités de fonctionnement du service sur le routeur D rassemblées dans la Table I.

TABLE I
PROBABILITES D'ETATS POUR LE PREMIER CAS

Solution	Boucles	Arbre	Δ
Nominal	0.99897028	0.99897028	0
Secours	0.001018685	0.001019199	0.000000514
Panne	0.000011035	0.000010521	0.000000514

Ce modèle permet de voir directement le gain de disponibilité en comparant la probabilité de se trouver en cas de panne entre les deux solutions. Il s'agit bien sûr d'un cas théorique avec des valeurs estimées et c'est pourquoi on observe un gain si faible (environ 16s/an).

Maintenant que l'on a pu constater que le modèle est bien capable de montrer le gain de disponibilité, on va chercher à montrer sur un exemple défavorable ce que l'on perd.

B. Etude sur un cas défavorable

Dans cette partie, on cherche un cas où le comportement sera vraiment différent avec les deux ingénieries comme présenté dans la Figure 7.

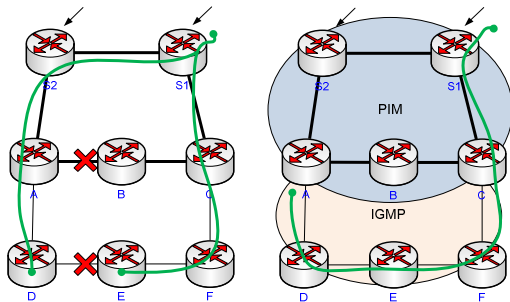


Fig 7. Second cas, défavorable à la nouvelle solution

Dans cette topologie, avec une architecture en boucles imbriquées, on comprend facilement comment le flux arrive jusqu'à D en raison de la protection des anneaux. Pour la partie en arbre, c'est le routeur C qui est garant de la distribution dans le VPLS, ainsi tous les routeurs du VPLS reçoivent le flux de C. Il s'agit là d'un cas défavorable car on voit que pour atteindre la source, le routeur D est lié au

fonctionnel de toute la chaîne passant par C. Par contre on aura toujours un gain de disponibilité car la nouvelle solution corrige encore le problème d'isolement du routeur A (fournisseur de flux à D pour la solution en boucles).

Les résultats de la modélisation en réseaux Bayésiens sont résumés dans la Table II.

TABLE II
PROBABILITES D'ETATS POUR LE SECOND CAS

Solution	Boucles	Arbre	Δ
Nominal	0.99846081	0.9979516	0.00050921
Secours	0.001527375	0.002037358	0.000509983
Panne	0.000011815	0.000011042	0.000000773

On obtient un résultat intéressant : dans cet exemple la disponibilité est améliorée mais au détriment de la probabilité de se trouver dans l'état nominal. On gagne 24s/an de disponibilité sur les 373s/an (+6.4%) que l'on avait dans la première solution. Alors qu'on augmente le risque de se trouver en situation de reroutage de 4,5h/an sur les 13.4h/an (+33.6%) de la solution en boucle. Ce cas est défavorable car en augmentant la probabilité des reroutages, on dégrade les performances pour un réseau audiovisuel.

La partie suivante va permettre de quantifier l'apport de la nouvelle solution sur une infrastructure inspirée d'un cas réel.

C. Essai sur un cas réel

Cette partie va montrer comment la nouvelle ingénierie pourrait être déployée sur un réseau réel et on peut voir comment la nouvelle ingénierie va contribuer à régler des problèmes de doubles pannes bloquantes. L'architecture est présentée en Figure 8.

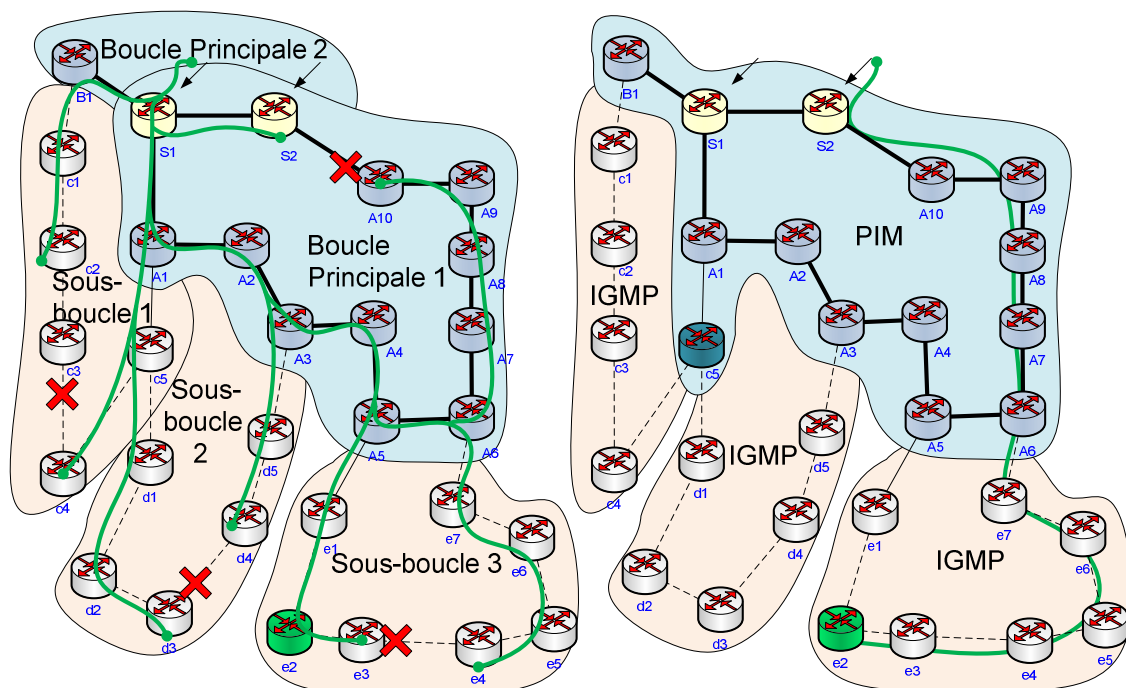


Fig 8. Etude sur un cas réel

On découvre une boucle principale liant les deux routeurs sources S1 et S2 et trois sous-boucles dont deux reliées sur la partie gauche de la topologie. Le routeur visé par cette étude est e2 qui est coloré en vert sur les schémas. On utilisera des liaisons en fibre optique (lien complet) avec la disponibilité annoncée plus haut et des faisceaux hertziens (liens en pointillés) avec une disponibilité de 0.9999.

L'ingénierie actuelle en boucles imbriquées est présentée sur la gauche. On y retrouve les quatre coupures RSTP aux endroits les plus éloignés des sources sauf pour la boucle principale. A propos de la nouvelle solution que l'on peut retrouver sur la droite, il y a eu un changement de classe de routeur en c5 pour que ce routeur soit apte à porter un VPRN et ainsi limiter la taille de la partie VPLS. Car il ne faut pas oublier que tous les routeurs d'un même VPLS auront une seule source active et il paraît sensé de dire que plus un VPLS est étendu plus les risques de reroutage pour ses points de service sont grands. On obtient alors trois VPLS distincts et le VPLS où se trouve le routeur e2 est indépendant des deux autres. Un autre changement notable est que le flux n'est plus distribué dans la sous-boucle cible depuis A5, mais depuis A6.

On va s'intéresser à l'apport de la nouvelle ingénierie qui va permettre de réalimenter la boucle principale si un cas de double panne impacte la boucle principale mais que physiquement il existe une solution par une sous-boucle pour alimenter la destination (en effet si a10 et a2 tombent en panne, il existe une solution via c5-d1-d2-d3-d4-d5 pour réalimenter la boucle principale). Cela apporte un nouveau gain de disponibilité et la modélisation permet de constater de quel ordre elle est : voir Table III.

TABLE III
PROBABILITES D'ETATS POUR LE CAS REEL

Solution	Boucles	Arbre	Δ
Nominal	0.996824298	0.996784525	0.000039773
Secours	0.003157427	0.003202403	0.000044976
Panne	0.000018276	0.000013072	0.000005204

Avec cette étude basée sur une architecture réelle, on observe tout d'abord un gain de 164s/an ce qui correspond à un gain de 28.4% par rapport aux 577s de panne annuel. Au niveau des reroutages, on observe une probabilité d'être en situation de secours en augmentation de 24min/an contre les 27.7h/an estimées correspondant à une augmentation de 1.4% des reroutages. Cette différence avec le cas précédent provient du principe que l'une des sous-boucles peut réalimenter la boucle principale dans le cas de l'architecture en arbre.

Cela montre bien que dans ce cas réel le gain de disponibilité est plus important que l'augmentation de la probabilité de reroutage. Ainsi la nouvelle ingénierie tient bien ses promesses.

Cette étude quantifie à la fois l'apport et les inconvénients de la nouvelle ingénierie. Elle sera étendue à l'ensemble du réseau et d'ors et déjà conforte le choix de migration.

V. CONCLUSION

Les caractéristiques multi-états des réseaux Bayésiens permettent une analyse plus beaucoup plus complète qu'un simple arbre de défaillance. Cette étude a permis de montrer son application dans un contexte de réseaux de télécommunications. Pour l'implémentation d'une nouvelle ingénierie protocolaire, nous avons pu ainsi quantifier à la fois les aspects gain en taux de disponibilité mais aussi et surtout la contrepartie induite par les impacts des bascules. Les

résultats sont en faveur de la nouvelle ingénierie et moyennant l'introduction de nouveaux routeurs placés de façon optimale on pourra réduire les effets indésirables.

L'étude sera poursuivie et généralisée dans ce sens pour optimiser globalement l'architecture du réseau. Cette façon de modéliser les protocoles met en évidence les gains et les pertes de chaque solution en utilisant des données réelles. On peut imaginer appliquer cette technique pour estimer les apports sur d'autres modalités, et préciser les aides à la décision. Lors de cette étude, on ne se préoccupe pas encore des phénomènes de bascules non-instantanées qui sont souvent problématiques dans les réseaux spécialisés pour l'audiovisuel ; la suite de ces travaux pourraient permettre ce genre d'analyse.

VI. REMERCIEMENTS

Ces travaux sont effectués dans le cadre d'une thèse CIFRE en collaboration entre le CRAN et TDF et plus précisément avec l'équipe de conception de TDF Metz.

REFERENCES

- [1] Poul E. Heegaarda, Kishor S. Trivedib. Network survivability modeling. *Computer Networks*. Volume 53, Issue 8, Pages 1215–1234, 2009.
- [2] James P.G. Sterbenza, David Hutchisonb, Egemen K. Çetinkayaa, Abdul Jabbara, Justin P. Rohrer, Marcus Schöllerc, Paul Smithb. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*. Volume 54, Issue 8, Pages 1245–1265, 2010.
- [3] Qitao Gan, Bjarne E. Helvik. Dependability Modelling and Analysis of Networks as Taking Routing and Traffic into Account. Next Generation Internet Design and Engineering. IEEE NGI 2006. Valencia. Espagne. 2006.
- [4] A. Bobbioa, L. Portinalea, M. Minichinob, E. Ciancamerlab. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering & System Safety*. Volume 71, Issue 3, Pages 249–260, 2001.
- [5] P. Weber, G. Medina-Oliva, C. Simon, B. Lung. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence*. Volume 25, Issue 4, Pages 671–682, 2012.
- [6] Abdeljabbar Ben Salem, Alexandre Muller, Philippe Weber. Dynamic Bayesian Networks in system reliability analysis. *Fault Detection, Supervision and Safety of Technical Processes*. Volume 1, Pages 444–449, 2007.
- [7] Andrew Gelman, John B. Carlin, Hal S. Stern, David B. Dunson, Aki Vehtari, Donald B. Rubin. *Bayesian Data Analysis, Third Edition*. CRC Press, Boca Raton, 2013.
- [8] D. Levi, D. Harrington. Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol. *RFC 4318*. 2005.
- [9] B. Gleeson, A. Lin, J. Heinanen, G. Armitage, A. Malis. A Framework for IP Based Virtual Private Networks. *RFC 2764*. 2000.
- [10] M. Lasserre, V. Kompella. Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling. *RFC 4762*. 2007.
- [11] B. Fenner, M. Handley, H. Holbrook, I. Kouvelas. Protocol Independent Multicast - Sparse Mode (PIM-SM) : Protocol Specification (Revised). *RFC 4601*. 2006.
- [12] B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan. Internet Group Management Protocol, Version 3. *RFC 3376*. 2002.