Survivabilité dans les réseaux de transport de vidéo et d'audio sans dégradation de la qualité de service perçue par l'utilisateur

Stéphen Pirlot

▶ **To cite this version:**

Stéphen Pirlot. Survivabilité dans les réseaux de transport de vidéo et d'audio sans dégradation de la qualité de service perçue par l'utilisateur. Réseaux et télécommunications [cs.NI]. Université de Lorraine, 2016. Français. NNT : 2016LORR0082 . tel-01754662v2

HAL Id: tel-01754662
https://hal.science/tel-01754662v2

Submitted on 21 Nov 2016

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.

UNIVERSITÉ DE LORRAINE

Ecole doctorale IAEM Lorraine

Survivabilité dans les réseaux de transport de vidéo et d'audio sans dégradation de la qualité perçue par l'utilisateur

THÈSE

présentée et soutenue publiquement le 29 juin 2016

pour l'obtention du

Doctorat de l'Université de Lorraine
(mention Automatique, Traitement du signal et des images, Génie informatique)

par

Stéphen PIRLOT

Composition du jury

Président du Jury :	Philippe WEBER, Maître de Conférences HDR, Université de Lorraine
Rapporteurs :	Professeur Thierry GAYRAUD, Université Paul Sabatier Toulouse 3
	Professeur Antoine GRALL, Université de Technologie de Troyes
Examinateurs:	Professeur Jean-Marc THIRIET, Université Grenoble Alpes
	Eric GNAEDINGER, Maître de Conférences Université de Lorraine
	René KOPP, Ingénieur, TDF
Directeur de thèse :	Professeur Francis LEPAGE, Université de Lorraine

Centre de Recherche en Automatique de Nancy – UMR 7039
UFR ESSTIN

En partenariat avec TDF

Stéphen Pirlot : Survivabilité dans les réseaux de transport de vidéo et d'audio sans dégradation de la qualité perçue par l'utilisateur, 2016

Supervisors : Francis LEPAGE

Eric GNAEDINGER

René KOPP

Publicated : June 2016

Abstract

Audiovisual data traffic presents a great sensitivity to the failures. TDF Company which performs his own network to realize inter alia the National TV transportation wants to avoid failures to bring a high quality service. This is why the Company wants from one side to study by a theatrical approach the network resilience and from another side enhance the deployed solution to absorb the recorded increase of failures in the optical links between the network nodes.

Résumé

Le transport de contenu audiovisuel présente une très grande sensibilité aux pannes du fait de sa nature non élastique. La société TDF qui opère un réseau sur lequel elle réalise entre autres le transport des multiplexes de la Télévision Numérique Terrestre veut mieux maitriser l'évitement et le contournement des pannes pour fournir un service de grande qualité. Dans ce but, les travaux de recherche qui constituent cette thèse ont développé d'une part une approche théorique de la résilience du réseau et d'autre part une proposition d'amélioration de la solution actuellement déployée pour absorber l'augmentation constatée du taux de panne des liaisons optiques entre les nœuds du réseau.

Remerciements

Je remercie sincèrement les rapporteurs, Antoine Grall et Thierry Gayraud, pour leur travail d'examen de ce mémoire.

Un grand merci à Eric Gnaedinger pour l'encadrement de ma thèse et qui a su me guider après mes études d'ingénieur vers cette formidable aventure.

Merci à René Kopp pour l'encadrement de ma thèse à TDF et de m'avoir impliqué dans la grande histoire de TMS.

Mes remerciements à Francis Lepage également pour l'encadrement de ma thèse et son aide précieuse dans la rédaction de tous les écrits scientifiques.

J'adresse un remerciement général à toute l'équipe RUHD de TDF Metz et en particulier à Sylvain, Jean, Antoine, David et Philippe pour leur soutien.

Enfin je remercie profondément ma famille et surtout Emilie et ma Maman qui ont toujours été présentes quand j'en ai eu besoin et qui m'ont poussé à me lancer dans cette thèse.

Table des matières

Abstract 3

Résumé 3

Remerciements 5

Table des matières 7

Table des figures 10

Préface 15

Introduction 16

Chapitre 1 Les réseaux de transport vidéo et leur survivabilité 19

1.1. Présentation du métier de TDF 20

1.2. Un réseau robuste 21

1.3. La survivabilité d'un réseau audiovisuel 24

Chapitre 2 Résilience aux pannes du réseau 27

2.1. Contraintes fonctionnelles et opérationnelles 28

2.2. Amélioration du transport 29

2.2.1. Bidirectional Forwarding Detection 29

2.2.2. Operations, Administration et Management 31

2.3. Transport de données dans un réseau IP/MPLS 32

2.3.1. Services client et services réseau 32

2.3.2. Description des services réseau et intégration 36

2.4. Ingénieries protocolaires 37

2.4.1. L'enjeu du transport national de multiplexes TNT 37

2.4.2. Ingénierie Rapid Spanning-Tree Protocol (RSTP) 38

2.4.3. Ingénierie Multicast VPN (MVPN) 43

2.4.3.1. Description de la solution 43
2.4.3.2. Retour sur les cas de panne précédents 47
2.4.3.3. Faiblesses du MVPN 48
Chapitre 3 Analyse de la disponibilité du réseau 51
3.1. Etude de la disponibilité 52
3.1.1. Choix de modélisations et disponibilité 52
3.1.2. Arbres de défaillances 53
3.1.3. Chaines de Markov 54
3.2. Modélisation par Réseaux Bayésiens 55
3.2.1. Présentation 55
3.2.2. Modélisation de la disponibilité par RB 59
3.2.2.1. Construction du RB sans cycle 59
3.2.2.2. Modélisation des caractéristiques des réseaux IP 64
3.2.3. Modélisation des ingénieries protocolaires 65
3.2.3.1. Cas Simple 1 66
3.2.3.2. Cas Simple 2 69
3.2.3.3. Cas réel avec une seule destination 72
3.2.3.4. Cas réel multi-destinations 74
3.3. Simulation sous Modeler 76
3.3.1. Introduction à l'utilisation de Modeler 76
3.3.2. Cas simple 79
3.3.3. Cas réel 81
Chapitre 4 Proposition d'une nouvelle ingénierie 85
4.1. Limitations connues de la solution MVPN 86
4.2. Ingénierie MVPN+ 88

4.2.1. Présentation de la nouvelle ingénierie 88

4.2.2. Modélisation par RB 92

4.2.3. Emulation de la solution MVPN+ par MVPN+e 95

4.2.4. Simulation sous Modeler 96

4.2.5. Maquettage en laboratoire 97

4.2.6. Conclusion 101

Conclusion et Perspectives 102

Annexes 105

Annexe 1 : Détail du modèle en RB du cas simple 1 en RSTP 106

Annexe 2 : Représentation par RB du cas réel pour la solution MVPN. 110

Annexe 3 : Représentation par RB du cas réel pour la solution MVPN et plusieurs destinations. 111

Bibliographie 113

Liste des publications 117

Acronymes 118

Table des figures

Figure 1 : Topologie logique du réseau national TMS en Métropole 21

Figure 2 : Différentes conséquences sur les pertes pour TCP et UDP 22

Figure 3 : Exemple d'une topologie réseau dans l'Est 23

Figure 4 : BFD annonce aux autres protocoles l'état du lien 29

Figure 5: Echanges BFD 30

Figure 6 : Session BFD à travers un réseau opérateur tiers 30

Figure 7 : Comparaison des performances avec et sans BFD sur le temps de panne 31

Figure 8 : Répartition de quelques normes OAM 31

Figure 9 : Utilisation de services réseau sur TMS pour cloisonner le transport 33

Figure 10 : Les différents types de services proposés sur TMS 33

Figure 11 : Transport sécurisé par RSVP 34

Figure 12 : Transport sécurisé par LDP 35

Figure 13 : Diffusion de multicast dans un service de type VPLS. a) représentation physique. b) utilisation logique du réseau 36

Figure 14 : Transport depuis le client jusqu'à l'utilisateur final 37

Figure 15 : Topologie initiale et vocabulaire de TMS 38

Figure 16 : Les problématiques de transport avec deux sources à travers une topologie en boucles 39

Figure 17 : Sécurisation de la tête de réseau avec la solution RSTP 39

Figure 18 : a) Topologie fournie par RSTP. b) Diffusion par broadcast du multicast suivant la topologie 40

Figure 19 : Filtres anti-retour sur les routeurs pères 40

Figure 20 : Cas bloquants de doubles pannes dans une boucle principale 41

Figure 21 : a) Cas bloquant lors d'une panne en amont de TMS. b) Intégration d'un maillage dans une boucle 42

Figure 22 : Différences entre les MVPN. a) Topologie physique et client (en vert). b) MVPN classique avec un service simulant UN seul routeur pour le service. c) MVPN en VRF-Lite où chaque équipement physique porte un routeur virtuel. .. 43

Figure 23 : Répartition des domaines VPRN et VPLS avec leurs protocoles associés 44

Figure 24 : Construction de l'arbre PIM à travers les VPRN 45

Figure 25 : Diffusion du flux pour l'ingénierie MVPN 46

Figure 26 : Retour sur le 1er cas bloquant qui ne pose pas de problème au MVPN 47

Figure 27 : Retour sur le 2nd cas bloquant ne pose pas de problème au MVPN .. 48

Figure 28 : Sous-ensembles de deux ingénieries 48

Figure 29 : Différence de répartition de la diffusion dans la sous-boucle entre RSTP et MVPN 49

Figure 30 : Exemple d'analyse par arbres de défaillances 53

Figure 31 : Représentation d'un système sous forme de Chaînes de Markov 55

Figure 32 : Représentation d'un système de mélange avec des vannes 56

Figure 33 : a) Représentation graphique d'un système sous RB. b) Description du système représenté avec ses tables remplies 57

Figure 34 : Représentation par RB du système de vanne en incluant deux états de pannes différents 57

Figure 35 : Analyse par l'algorithme d'inférence du logiciel BayesiaLab 58

Figure 36 : Routeurs stratégiques 60

Figure 37 : Topologie simple représentée en RB 61

Figure 38 : Problème relatif à la taille de la TPC 61

Figure 39 : Construction du RB en conservant la logique définie 63

Figure 40 : Architecture proche de la réalité modélisée sous RB 63

Figure 41 : Alimentation du routeur B. a) Situation nominale. b) Situation secours. c) Situation panne 64

Figure 42 : Cas simple 1 66

Figure 43 : Modélisation par RB du cas 1 en RSTP 67

Figure 44 : Modélisation par RB du cas 1 en MVPN 68

Figure 45 : Cas simple 2 70

Figure 46 : Modélisation par RB du cas 2 en RSTP 71

Figure 47 : Topologie étudiée pour le cas réel, pour les deux solutions 72

Figure 48 : Représentation par RB du cas réel pour la solution MVPN 73

Figure 49 : Topologie du cas réel qui délivre le flux en plusieurs points 75

Figure 50 : Illustration de la mesure graphique du phénomène de bascule sur Modeler 78

Figure 51 : Représentation sous Modeler du cas simple 1 en RSTP 79

Figure 52 : Représentation sous Modeler du cas simple 1 en MVPN 80

Figure 53 : Représentation du cas réel sous Modeler en RSTP 82

Figure 54 : Simplification sous Modeler du cas réel 82

Figure 55 : Différence de diffusion vers D1 entre RSTP et MVPN 86

Figure 56 : Transport sur l'infrastructure en utilisant uniquement PIM 87

Figure 57 : Différence de diffusion dans le VPLS entre MVPN et MVPN+ 88

Figure 58 : Fonctionnement d'IGMP-Snooping dans un réseau local 89

Figure 59 : Fonctionnement de MPVN+ 90

Figure 60 : Différence de diffusion entre solution optimale entièrement en PIM et MVPN+ 91

Figure 61 : Différences d'analyse des trames Ethernet par les switchs 92

Figure 62 : Cas simple pour prouver l'intérêt de MVPN+ 92

Figure 63 : Représentation par RB du cas simple en MVPN+ 93

Figure 64 : Fonctionnement sur le cas réel de MVPN et MVPN+ 94

Figure 65 : Solution implémentable de MVPN+ en simulation et en maquette ... 95

Figure 66 : Représentation sous Modeler de la solution MVPN+e 96

Figure 67 : Différences entre VPRN, VPLS et Routed-VPLS 97

Figure 68 : Topologie utilisée pour l'analyse d'impacts à l'image 98

Figure 69 : Utilisation de MVPN et MVPN+e sur la maquette 99

Préface

Cette thèse a été élaborée dans un contexte CIFRE liant le laboratoire CRAN et l'entreprise TDF. Ce partenariat implique plus précisément les chercheurs de l'équipe ISET du CRAN et l'équipe de conception sur RUHD (Réseau Ultra-Haut Débit) de TDF Metz.

Le Centre de Recherche en Automatique de Nancy (CRAN)

Créé en 1980, le Centre de Recherche en Automatique de Nancy (CRAN) est une unité mixte de recherche (UMR 7039) commune à l'Université de Lorraine (UL) et au CNRS (Institut des sciences de l'information et de leurs interactions (INS2I) et Institut des Sciences de l'Ingénierie et des Systèmes (INSIS), Section 7 et section 28 du Comité National de la Recherche Scientifique). Il fait partie de la Fédération de Recherche Charles Hermite Automatique, Informatique, Mathématiques de Lorraine et du pôle scientifique Automatique, Mathématiques, Informatique et leurs Interactions (AM2I) de l'université de Lorraine.

Le CRAN est structuré en trois départements : SBS (Santé-Biologie-Signal), CID (Contrôle-Identification-Diagnostic), ISET (Ingénierie des Systèmes Eco-Techniques). Cette thèse a été préparée au sein du département ISET.

TDF France

Impliquées dans les domaines des télécommunications et de l'audiovisuel, l'entreprise TDF est en partie spécialisée dans le transport et la distribution des radios et chaînes de télévision en France métropolitaine et en outre-mer. Elle dispose notamment de son propre réseau IP/MPLS (MultiProtocol Label Switching) s'appuyant sur des infrastructures optiques dédiées, des liaisons Ethernet louées et des faisceaux hertziens indépendants.

L'une des missions de TDF est de transporter et diffuser à de nombreux points de services la TNT (Télévision Numérique Terrestre) ainsi que la radio FM. Mais l'entreprise poursuit aussi très activement sa diversification dans le domaine des télécommunications.

Introduction

Le domaine des réseaux et les réseaux eux-mêmes sont en perpétuelles évolutions. Les cycles de vie des équipements et des technologies mises en œuvre se raccourcissent : le rythme des évolutions logicielles majeures est inférieur à trois ans et un équipement de type routeur est totalement obsolète au bout de dix ans voire au bout de cinq ans. Pour respecter les engagements de disponibilité, la topologie du réseau de TDF est passée d'une structure en boucle prolongée par des pendulaires à une structure majoritairement bouclée et partiellement maillée dans laquelle un point de présence dispose de deux à quatre chemins de raccordements.

Un réseau quel qu'il soit est soumis à plusieurs contraintes dont la première est évidement de fournir les services dans le respect strict des engagements de qualité de service (QdS) pris avec le client. Ces engagements de QdS, tel que le taux de disponibilité, reposent sur les performances de chaque élément constituant le réseau. Ainsi entrent en ligne de compte la fiabilité des équipements et celle des liens de transmission mais aussi la capacité de l'entreprise à maintenir le réseau en condition opérationnelle reposant sur l'efficacité de sa maintenance préventive et curative.

TDF a dû faire face ces dernières années à une recrudescence de pannes de ses liaisons louées chez les opérateurs du marché sans pouvoir inverser cette tendance. Cette importante augmentation de pannes et notamment de pannes multiples a mis en défaut les mécanismes de résilience du réseau qui initialement avaient été conçus pour résister à des pannes simples au sein d'une même boucle. L'arrêt de certains cycles de maintenance préventive n'a évidemment pas contribué à améliorer la situation. L'ingénierie initiale ne permettait plus de restituer les taux de disponibilité attendus au niveau des services clients.

Couplée à l'infrastructure réseau on trouve l'ingénierie protocolaire qui délivre les services réseau, appelés aussi services techniques, eux-mêmes support des services clients. L'évolution matérielle et logicielle des routeurs mis en œuvre a ouvert de nouvelles possibilités pour améliorer les mécanismes de résilience du réseau notamment en tirant plus efficacement parti du maillage du réseau. Ceci étant, fallait-il encore pouvoir choisir et évaluer objectivement les différents protocoles en lice.

Deux particularités propres au domaine de l'audiovisuel et de la radiodiffusion rendent la tâche plus complexe. La première est que les services

sont de type transport en temps réel unidirectionnel sur une topologie point vers multipoints et la seconde est la priorité donnée à l'évitement des impacts à l'image. En effet les chaines techniques audiovisuelles mises en œuvre ayant un effet multiplicateur sur le temps de cicatrisation du réseau, il s'agira de le réduire au minimum mais aussi de l'éviter au maximum. Il est rapidement apparu nécessaire de faire une analyse scientifique de la résilience du réseau permettant d'objectiver le choix de la nouvelle ingénierie protocolaire à mettre en œuvre.

L'étude présentée dans cette thèse se focalise sur la disponibilité des services nationaux de transport des multiplexes de la TNT. Il s'agit d'analyser le gain et la régression en disponibilité réseau conjointement avec la réduction ou l'accroissement des impacts à l'image.

Dans un premier temps la mission de TDF sera exposée pour présenter le contexte de l'étude. Nous expliquerons notamment ce qu'est un réseau audiovisuel et en quoi l'étude de la survivabilité du réseau est importante.

Un second chapitre, sur le thème global de la résilience aux pannes et de son amélioration, expliquera comment le réseau de TDF a été conçu. Nous rappellerons brièvement les contraintes auxquelles il est soumis. Puis seront évoqués les premières pistes d'amélioration de la résilience et en particulier deux protocoles additionnels qui renforcent la réactivité du réseau aux pannes. S'en suit un rappel sur les services réseau mis en œuvre qui précèdera la description des différentes ingénieries protocolaires déployées. La compréhension du comportement de ces protocoles est indispensable à leur analyse et leur modélisation réalisées dans le chapitre 3.

Le chapitre 3 sera consacré à l'étude scientifique d'analyse de la disponibilité des services de transport des multiplexes TNT suivant une méthode probabiliste. La modélisation du réseau viendra consolider et compléter une première analyse. Ce sont ces outils qui permettront d'objectiver les performances des différentes ingénieries protocolaires et nous guider dans nos choix ainsi que d'évaluer les propositions d'amélioration.

Enfin le chapitre 4 présentera et évaluera une proposition originale pour améliorer les performances obtenues avec les protocoles standards. Cette proposition consiste en une amélioration de la solution choisie par TDF qui n'est actuellement pas encore implémentée dans les routeurs.

Chapitre 1

Les réseaux de transport vidéo et leur survivabilité

Chapitre 1 Les réseaux de transport vidéo et leur survivabilité 19

1.1. Présentation du métier de TDF 20

1.2. Un réseau robuste 21

1.3. La survivabilité d'un réseau audiovisuel 24

1.1.Présentation du métier de TDF

Depuis 40 ans, TDF est le partenaire des médias et des télécoms. Avec ses 10 000 sites, son réseau RUHD (Réseau Ultra-Haut Débit), ses plateformes techniques et son savoir-faire développé sur des décennies, l'entreprise assure la diffusion des 35 chaînes de la TNT et des 900 radios FM, ainsi que le déploiement des réseaux des quatre opérateurs nationaux de téléphonie mobile.

La diversification dans les domaines des télécommunications et du multimédias a été amorcée depuis plusieurs années et s'est significativement accélérée ces cinq dernières années. Ainsi dès 2006, TDF s'est dotée d'un réseau IP/MPLS d'envergure nationale qui avait comme cahier des charges certes le transport de flux audiovisuels à des fins de diffusion et de contribution mais aussi la fourniture de services Ethernet et IP.

Aujourd'hui partagés sur TMS (Transport Multi-Services) et cloisonnées par la technologie MPLS, les multiplexes de la TNT, les radios et les services Ethernet sont transportés à travers une infrastructure contenant plus de 400 points de présence recouvrant le territoire français métropolitain (Cf Figure 1) mais aussi une grande partie des départements et territoires d'outre-mer. Le réseau a été initialement et prioritairement conçu pour transporter des flux audiovisuels. Il a dû notamment répondre aux contraintes temps réel et de qualité de service inhérentes à ce type de service mais aussi à l'optimisation drastique de la bande passante dont le coût croît exponentiellement lorsqu'on s'éloigne des grandes artères d'infrastructure télécoms.

Aujourd'hui le réseau cœur de TMS peut s'appuyer sur une infrastructure maitrisée car construite sur un réseau optique dédié (RUHD optique) directement opéré par TDF. Ce réseau optique est l'un des vecteurs important de croissance de l'entreprise dans le domaine des télécommunications avec la mise en place de Datacenter de proximité et de fourniture de services Ethernet à très haut débit (1GbE, 10GbE et 100GbE).

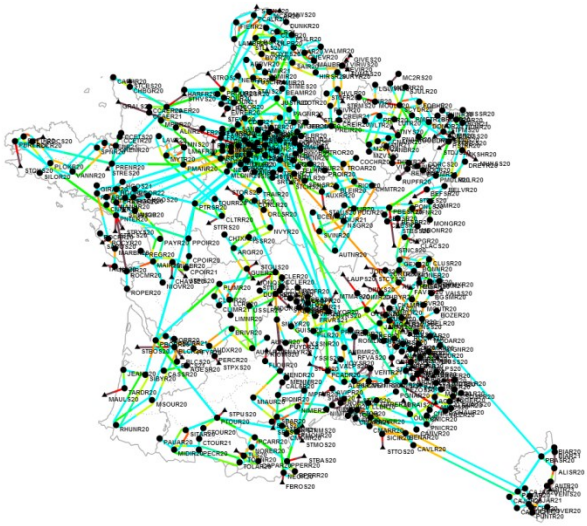


Figure 1 : Topologie logique du réseau national TMS en Métropole

Ainsi, le réseau est conçu pour la prise en charge de flux audiovisuels à partir de sources nationales et régionales pour les distribuer sur des sites répartis sur l'ensemble du territoire français. Outre les différentes technologies utilisées en tête de réseau[1] et en distribution, le transport lui-même est assuré par le réseau IP/MPLS pour, en particulier, minimiser les temps de latence et garantir une grande sûreté de fonctionnement.

Les clients de TDF visés par cette étude sont les groupes de chaines télévisées qui achètent un service de transport de leurs programmes télévisuels. L'utilisateur final est quant à lui le téléspectateur de ces chaines posté devant son téléviseur.

1.2.Un réseau robuste

La force de TMS est de permettre le transport des flux de manière indépendante. Afin d'éviter les interactions entre les flux transportés sur le réseau, on utilise la technologie MPLS pour cloisonner les données dans des services réseau. Chaque service réseau est une topologie vendue à un client adaptée à ses besoins (point-à-point, point-multipoints, multipoint-multipoint) et permettant de transporter un ou plusieurs flux à travers le réseau.

TMS gère la qualité de service en affectant une priorité à chaque flux. On peut ainsi classer les flux, permettant une répartition de la bande passante ajustée aux engagements de QdS.

[1] Dans la terminologie TDF, la tête de réseau est la source des flux

La gestion de la bande passante est telle que nous n'autorisons pas de surréservation pour éviter les situations de congestion. De façon classique nous gérons jusqu'à huit niveaux de priorité et attribuant l'un des plus élevés à l'audiovisuel.

L'utilisation de services et la prise en compte de la qualité de service permettent à TMS de transporter de manière contrôlée et sécurisée tout trafic à travers le réseau national. Cette notion de contrôle est très importante dans la mesure où les données transitent pour la plupart dans des flux UDP. Contrairement aux flux TCP communs sur les réseaux de l'Internet, les flux UDP sont fortement impactés par les pertes de paquets. En effet une perte de paquet sur TCP est protégée par le protocole contrairement à UDP où chaque paquet perdu est une donnée manquante au message final comme présenté en Figure 2.

Sur TMS, les nombreux flux UDP qui transitent dans le réseau sont sensibles à toutes les perturbations intrinsèques du réseau comme les reroutages ou les dégradations de liens. Les mécanismes de TMS permettent de sécuriser le transport mais chaque technique possède un temps de convergence induisant forcément la perte de paquets. Comme déjà évoqué, un capacity-planning[2] sans surréservation permet de se prémunir de toute congestion. Il est important de savoir que le phénomène de congestion entraine la perte de paquets. A noter que l'exercice de capacity-planning est facilité pour les flux audiovisuels car ils ont pour avantage que leur débit soit constant ou borné par les sources.

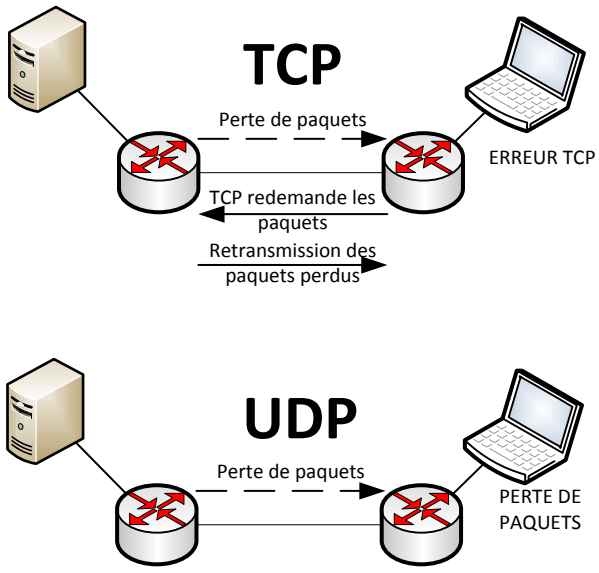


Figure 2 : Différentes conséquences sur les pertes pour TCP et UDP

[2] Le capacity-planning correspond à l'analyse du taux d'occupation des ressources du réseau et en particulier de la bande passante.

Le réseau TMS est constitué de routeurs et de liaisons s'appuyant sur différentes infrastructures : fibre optique en location, fibre optique dédiée et faisceau hertzien. Sur les fibres ou liaisons louées, les flux se retrouvent transportées par un tiers ce qui en complexifie la maitrise sur les aspects de diagnostic des pannes, de maintenance préventive et de gestion des interventions. Ces liaisons constituent l'essentiel des départs depuis la région parisienne vers la province. Les connexions régionales sont le plus souvent réalisées par des faisceaux hertziens TDF. A noter que ces derniers possèdent une bande passante significativement plus faible que les liaisons optiques, contraignant fortement le capacity-planning. Ces différences de supports physiques imposent aux ingénieurs de considérer des stratégies différentes de transport des flux en utilisant le réseau de la façon la plus optimale possible.

Sur la Figure 3 les liaisons louées sont représentées par des traits en noir épais et les faisceaux hertziens par des traits en ligne brisées.

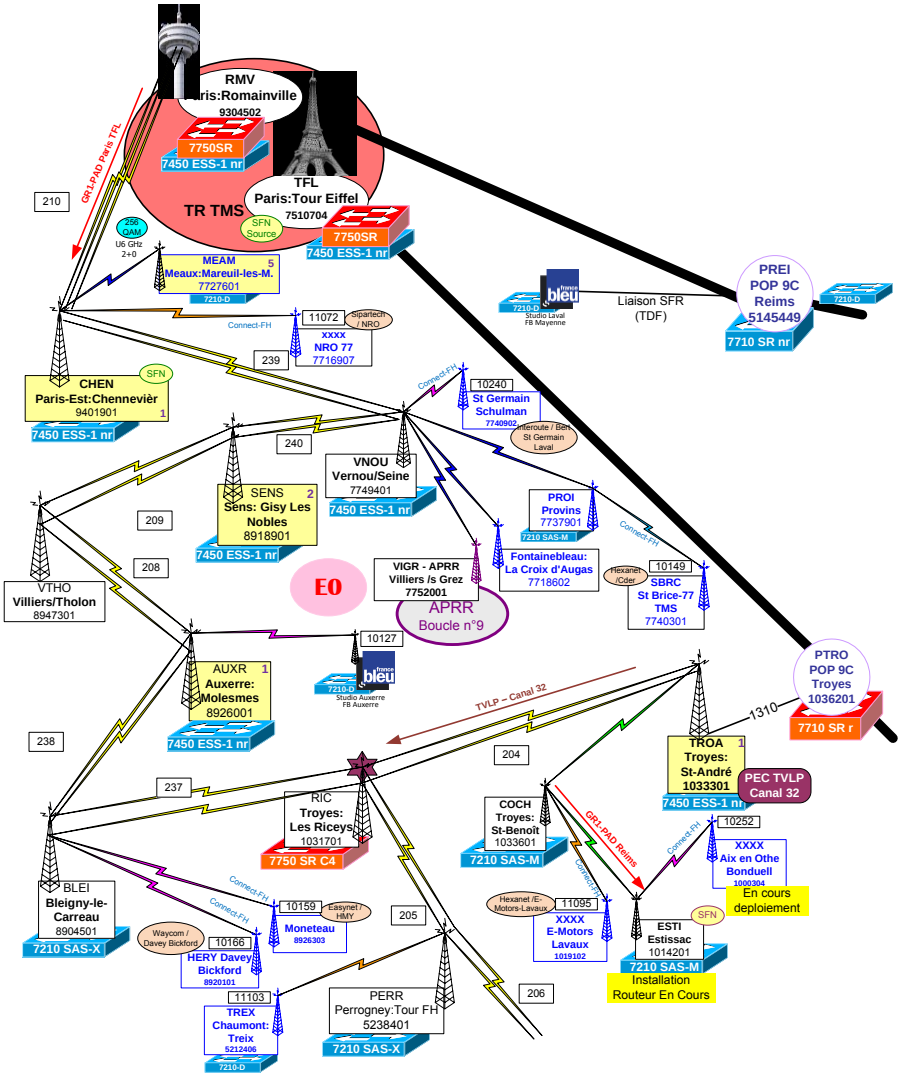


Figure 3 : Exemple d'une topologie réseau dans l'Est

1.3. La survivabilité d'un réseau audiovisuel

La survivabilité des réseaux inclut toutes les notions de résilience indispensables au bon fonctionnement du réseau TMS [1-4]. Tous les travaux relatifs à la survivabilité s'intéressent notamment à la faculté du réseau de résister à des pannes ou des attaques venant de l'extérieur du réseau. Ces concepts permettent aux réseaux de résister à des attaques militaires ou des catastrophes naturelles ou encore aux « crumble risks ». Mais pour le réseau TMS qui est un réseau autonome et sans lien avec Internet cette capacité n'est pas prioritaire. En revanche, il est important que ce réseau soit performant du point de vue de la disponibilité car c'est un critère observé par les clients. Une des caractéristiques d'un service audiovisuel est que sa qualité n'est pas seulement jugée par sa disponibilité, mais aussi par la durée de la convergence du réseau suite à une panne.

Dans le domaine de la survivabilité des réseaux, les réseaux autonomiques [5-6] ont pour atout d'être capables de converger vers une situation stable après chaque panne. Le réseau TMS ne s'approchera sûrement pas du comportement d'un réseau autonomique dont les principes ne sont pas encore déployés à grande échelle dans les algorithmes des routeurs mais surtout par le fait que ces réseaux possèdent des temps de convergence relativement longs par rapport aux réseaux classiques.

Bien qu'il existe d'autres solutions de transport via par exemple du streaming vidéo [7-8], les solutions basées sur RTP offrent des technologies efficaces pour le transport de vidéos et celles-ci sont en constante amélioration [9-11]. Les technologies IP possèdent leurs propres façons de transporter la vidéo comme dans le cas du Triple-play [12-14] mais ce sont souvent des options très gourmandes en bande passante. Le domaine de la diffusion de la TNT continue d'améliorer les solutions de diffusion [15] car les normes DVB-T restent encore parmi les technologies les moins chères du marché pour diffuser du contenu en masse. Dans cette étude nous allons plutôt nous focaliser sur l'aspect transport de flux multicast qui se développe sur les réseaux IP de manière classique [16-22] ou via des algorithmes de routages [23]. Mais ces études n'intègrent pas les fondements de la survivabilité que nous allons aborder ici. Il existe aussi des solutions adaptées aux architectures coopératives pour le transport de multicast [24] mais non applicables aux réseaux IP.

La mise en place d'une nouvelle ingénierie constitue une étude proche des travaux sur la survivabilité des réseaux. Le critère le plus important pour TDF est le respect des engagements de qualité (SLA : Service Level Agreement) dans le transport des multiplexes de la TNT car l'entreprise va devoir payer des pénalités s'ils ne sont pas respectés. Bien que le choix du SLA soit une donnée potentiellement à optimiser [25-26], notre étude va plus s'intéresser à son strict respect. La survivabilité du réseau va donc concerner d'avantage la disponibilité globale du réseau plutôt que de la capacité d'autoréparation souvent recherchée

dans les projets relatifs à la survivabilité des réseaux. Dans les travaux relatifs à la survivabilité on trouve aussi des études sur la dégradation des systèmes comme présenté dans [27] mais ce sont des problématiques qui intéressent plus les équipementiers.

Enfin il existe dans les réseaux optiques des solutions pour converger rapidement en cas de panne, permettant par exemple sur les réseaux OTN (Optical Transport Network) de cicatriser en moins de 50 ms [28]. Aussi le réseau n'utilisant pas uniquement du transport en fibre optique, ces technologies ne peuvent pas être mises en place sur l'ensemble du réseau pour des raisons évidentes de coûts. En outre ces technologies se prêtent plus difficilement aux topologies point-multipoints utilisées dans le monde de la TNT.

Chapitre 2

Résilience aux pannes du réseau

Chapitre 2 Résilience aux pannes du réseau 27
2.1. Contraintes fonctionnelles et opérationnelles 28
2.2. Amélioration du transport 29
2.2.1. Bidirectional Forwarding Detection 29
2.2.2. Operations, Administration et Management 31
2.3. Transport de données dans un réseau IP/MPLS 32
2.3.1. Services client et services réseau 32
2.3.2. Description des services réseau et intégration 36
2.4. Ingénieries protocolaires 37
2.4.1. L'enjeu du transport national de multiplexes TNT 37
2.4.2. Ingénierie Rapid Spanning-Tree Protocol (RSTP) 38
2.4.3. Ingénierie Multicast VPN (MVPN) 43
2.4.3.1. Description de la solution 43
2.4.3.2. Retour sur les cas de panne précédents 47
2.4.3.3. Faiblesses du MVPN 48

2.1.Contraintes fonctionnelles et opérationnelles

Sur TMS qui est un réseau de transport utilisant de nombreux supports (tels que les liaisons louées, liaisons dédiées, faisceaux hertziens), les contraintes sont exigeantes. D'une part les clients veulent la meilleure disponibilité pour l'utilisateur final. D'autre part TDF cherche à avoir le réseau le plus efficace en termes de rapport services rendus/coûts. De plus le transport des flux en UDP est connu pour être sensible aux erreurs. Enfin on cherche à minimiser les reroutages, sources d'impacts sur le flux reçu, sans affecter la disponibilité du service.

Toutes ces spécificités de l'audiovisuel ont été prises en compte dans la conception de TMS dans le but de respecter les SLA négociés. Ainsi les liaisons doivent être de très bonne qualité pour éviter au maximum les pertes de paquets car il s'agit d'autant de pertes au niveau vidéo pour l'utilisateur final. La congestion induit le même problème car une partie des paquets est retirée du système par les algorithmes de gestion de qualité de service provoquant aussi de la perte vidéo visible à l'écran. Enfin les situations de reroutages engendrent un état instable du réseau pendant lequel le réseau ne fonctionne plus correctement et cherche à établir une nouvelle situation de fonctionnement.

Suite à la recrudescence des pannes notamment sur les liaisons louées, TMS risque de ne plus respecter le SLA. Il est nécessaire de qualifier le service rendu de manière objective mais aussi d'envisager des actions d'amélioration de la résilience du réseau.

Pour cela, les actions envisageables peuvent porter sur les différents constituants du réseau TMS. L'aspect multi-structures est difficilement modifiable pour des raisons évidentes de coûts. On ne peut pas, par exemple, généraliser l'utilisation de la fibre dédiée qui offre certes les meilleures performances de transmission mais dont le coût est rédhibitoire. Les faisceaux hertziens restent souvent le seul moyen d'atteindre des sites éloignés.

La modification du type de protocole en passant d'UDP à TCP n'est pas envisageable car le transport des flux doit se faire à latence minimale. De plus certaines spécificités à la radiodiffusion, telle que la mise en œuvre de la technologie SFN (Single Frequency Network) nous contraint à des latences réseau faibles mais surtout déterministes et dans tous les cas inférieures à la seconde ce qui proscrit l'usage de protocoles tels que TCP.

Toujours sur cet aspect résilience réseau, au niveau des reroutages, il y a matière à amélioration. L'une des premières étapes consiste à identifier le chemin le plus court pour joindre deux points distants sur le réseau TMS. Ce principe élémentaire permet de diminuer le nombre de liaisons parcourues et donc de réduire les risques de reroutages. Il est mis en œuvre mais par configuration et non par décision autonome des protocoles implémentés. La plupart du temps la mise à jour n'a pas été réalisée suite aux nombreuses modifications de la topologie du

réseau. En termes de réactivité du reroutage, on peut envisager d'optimiser le fonctionnement des protocoles de routage comme OSPF (Open Shortest Path First) ou IS-IS (Intermediate System to Intermediate System). Ces protocoles utilisent des paramètres qu'il faut optimiser en tenant compte des performances et capacités des différents équipements déployés sur le réseau tout en préservant leur stabilité. MPLS offre des solutions d'optimisation à la fois du temps de détection de pannes et de celui de convergence ou de rétablissement de service. Ces techniques regroupées au sein de RSVP-TE (Ressource Reservation Protocol – Trafic Engineering) ne peuvent malheureusement pas être mises en œuvre car elles ne franchissent pas les aires IS-IS. Nous avons dû maintenir ce partitionnement en aires à cause de certaines limitations des équipements d'extrémité. Enfin il existe des protocoles additionnels qui viennent épauler les protocoles fédérateurs tels qu'IS-IS et RSVP en améliorant leur réactivité à la détection de panne. Deux d'entre eux sont décrits dans le paragraphe suivant.

2.2.Amélioration du transport

Dans ce paragraphe vont être examinées différentes pistes pour améliorer le fonctionnement du réseau en lui permettant de réagir plus rapidement. Le gain peut être obtenu en intégrant de nouveaux protocoles et en les faisant interagir avec les services actuels.

2.2.1. Bidirectional Forwarding Detection

Le protocole BFD (Bidirectional Forwarding Detection) est standardisé depuis Juillet 2010 via la RFC 5880 [29] et est actuellement supporté par les dernières versions des routeurs. Ce protocole de couche 3 du modèle OSI a pour but de contrôler l'état d'une liaison et d'avertir d'autres protocoles plus lents à réagir au changement de statut de la liaison.

Le protocole BFD utilise le transfert de messages spécifiques sur la liaison pour déterminer l'état du lien. Les messages sont envoyés à intervalles réguliers et la liaison est déclarée défectueuse si un certain nombre de messages n'est plus reçu. Il avertit alors d'autres protocoles (tels que RSVP, ISIS ou LDP) que la liaison est défectueuse et permet donc au protocole concerné d'être averti de l'état du lien sans attendre que son timer ne soit arrivé à expiration. Ce mécanisme permet de diminuer les temps de convergence de la reconfiguration réseau.

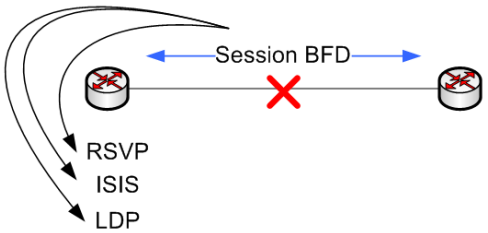


Figure 4 : BFD annonce aux autres protocoles l'état du lien

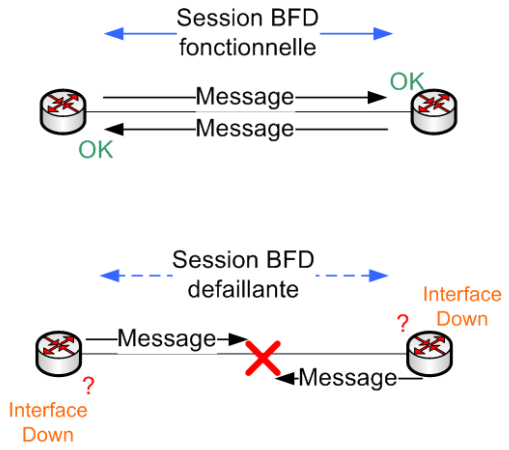


Figure 5: Echanges BFD

Le fonctionnement de BFD est basé sur des sessions : le protocole doit être implémenté de manière symétrique pour permettre un fonctionnement bidirectionnel. Une session BFD est établie si les deux routeurs activent le protocole sur leur liaison. Les routeurs s'envoient des messages avec une période minimale de 10ms et s'attendent à recevoir des messages (Figure 4 et 5).

Le protocole agit donc sur la convergence du réseau vers un état stable en détectant des pannes plus rapidement dans certains cas que sans BFD. Dans une situation simple où deux routeurs sont directement connectés à travers une fibre optique, en cas de panne de la fibre ce protocole n'apporte aucun gain de performance dans la mesure où les ports de cette liaison seront non fonctionnels et que les routeurs pourront alors prendre la décision du reroutage instantanément. Par contre dans le cadre de l'utilisation d'une fibre louée, les ports vont continuer de fonctionner car la connexion vers le réseau opérateur reste valide même en cas de panne dans son propre réseau comme le montre la Figure 6. Dans ce cas, les messages BFD vont bien partir de chaque routeur mais n'arriveront jamais à destination. C'est ainsi que BFD va prendre la décision d'interrompre la liaison logique de niveau 3 et d'alerter les protocoles de la perte de lien.

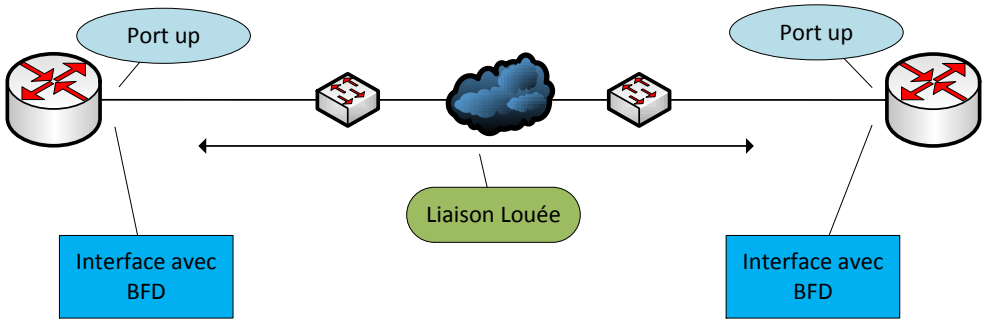


Figure 6 : Session BFD à travers un réseau opérateur tiers

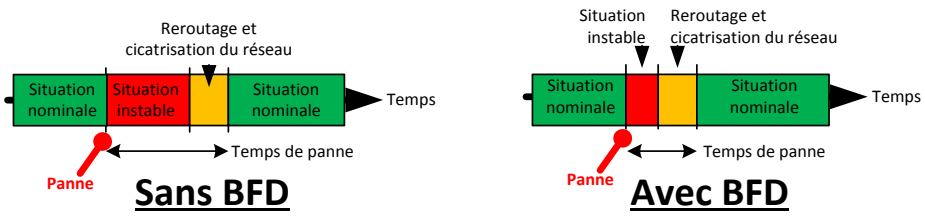


Figure 7 : Comparaison des performances avec et sans BFD sur le temps de panne

Le vrai intérêt de ce protocole consiste à améliorer le temps de détection de panne et minimiser la durée de la situation instable. BFD améliore la disponibilité globale du système car les mécanismes de reroutages se déclenchent plus rapidement.

Il y a enfin la capacité du protocole à détecter plus rapidement des pannes unidirectionnelles. En effet si l'une des deux fibres de la paire est abimée ou arrachée, l'un des deux routeurs ne recevra plus de message impliquant un reroutage, mais il va aussi annoncer à son voisin que son interface est inactive par un message « BFD session down ». Aussi le second routeur pourra prendre la décision d'un reroutage.

2.2.2. Operations, Administration et Management

Les outils OAM (Operations, Administration et Management) proposés par le Metro Ethernet Forum sont également installés dans les routeurs suite au déploiement des standards sur les réseaux. Il existe plusieurs types d'OAM régis par les normes ITU-T Y.1731, IEEE 802.1ag, IEEE 802.1ah et bien d'autres et chacun apporte des outils de diagnostic ou des mécanismes de surveillance du réseau. Les OAM utilisent la couche 2 du modèle OSI et plus particulièrement la partie Ethernet.

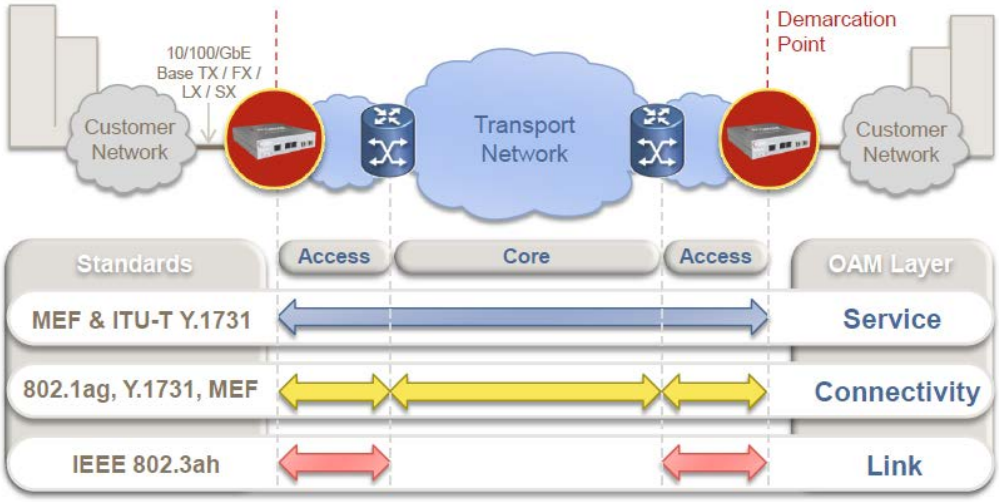


Figure 8 : Répartition de quelques normes OAM

La partie ITU-T Y.1731 s'intéresse plus précisément au diagnostic du transport (au sens du réseau de cœur) en intégrant la communication avec le client. Ces outils permettent par exemple de tester dans un réseau de commutateurs si l'adresse MAC d'un client est bien transportée à travers le réseau opérateur. Ce sont surtout des outils intégrés aux routeurs d'aide au diagnostic lors de panne.

Pour l'IEEE 802.1ag qui surveille la partie connectivité, les outils OAM permettent l'installation de sondes sur les équipements pour surveiller l'état du réseau. Ces fonctions sont uniquement à but informatif pour prévenir l'exploitation du réseau qu'une situation dégradée ou qu'une panne existe. Ces sondes peuvent effectuer des tests de manière répétée pour estimer la qualité du service rendu au client et donc le respect du SLA. Elles embarquent la possibilité de prévenir les sondes OAM que possède le client et aussi d'accepter toute information provenant d'un opérateur tiers fournies via les protocoles OAM.

Une autre approche est fournie par la norme IEEE 802.3ah qui se place au niveau physique. Il est possible de configurer cet outil pour qu'il se comporte d'une manière équivalente à BFD. Le port va envoyer des messages de type OAM 802.3ah à son voisin avec une certaine fréquence. Si le voisin détecte un nombre de messages consécutifs perdus, il peut prendre la décision de désactiver le port ce que ne fait pas BFD. Ainsi cette protection est efficace contre les pannes d'une liaison physique directe. Par conséquent elle ne permet pas de détecter les pannes de liaisons sur des fibres louées car les équipements de l'opérateur tiers masquent la liaison physique.

2.3. Transport de données dans un réseau IP/MPLS

2.3.1. Services client et services réseau

Lorsqu'un client souhaite se raccorder à TMS pour transporter son flux à travers le réseau de TDF, il lui est proposé un service réseau adapté à ses besoins.

La notion de service réseau est importante à prendre en considération. Chaque service vendu à un client correspond à un service réseau parfois appelé service technique. Chaque service réseau est une entité propre et permet d'identifier et d'isoler les données envoyées par chaque client. Pour être plus précis, à chaque service réseau on attribue des tunnels qui lui sont propres et ne contenant que les données d'un seul client. Ainsi les données utilisant le même support physique se retrouvent cloisonnées et sont transportées de manière indépendante comme montré dans la Figure 9.

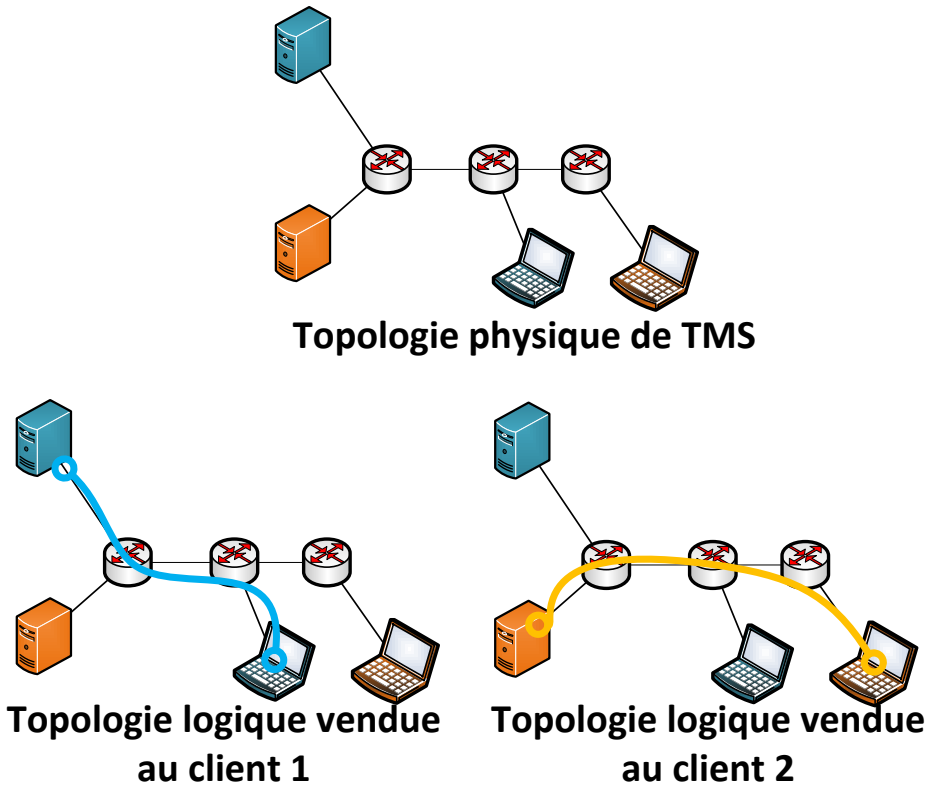


Figure 9 : Utilisation de services réseau sur TMS pour cloisonner le transport

Le cloisonnement est l'une des spécificités des services réseau, mais ils sont également caractérisés par un type. Par exemple pour le client désirant un service point à point le plus transparent possible, un service réseau niveau 1, sans apprentissage MAC appelé VLL (Virtual Leased Line) sera proposé. Les VLL se décomposent en plusieurs types en fonction du support à émuler, une liaison point à point Ethernet est fournie par un service appelé Epipe (Ethernet Pipe). D'autres clients vont avoir besoin d'une topologie point vers multipoint sans routage, TDF vend alors un service réseau niveau 2 avec apprentissage MAC appelé VPLS (Virtual Private Lan Service) [30]. Ceux ayant besoin de routage achèteront un service réseau niveau 3 avec routage appelé VPRN (Virtual Private Routed Network) [31].

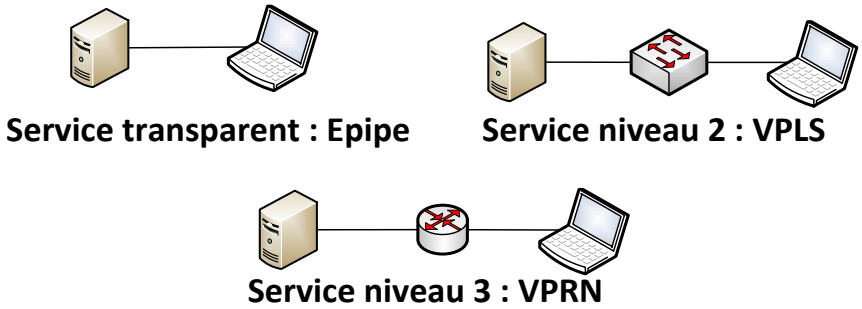


Figure 10 : Les différents types de services proposés sur TMS

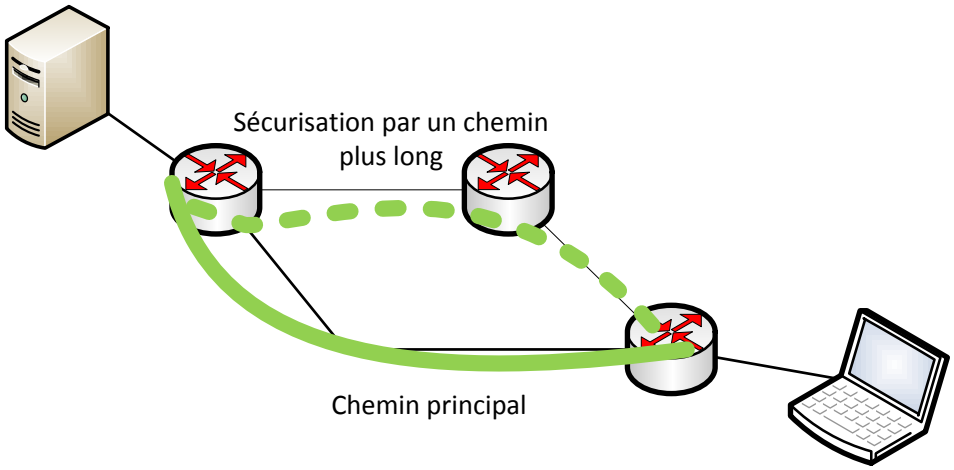


Figure 11 : Transport sécurisé par RSVP

Les services réseau peuvent être utilisés de manière composée, ainsi un service VPLS peut être connecté à un service VPRN. En effet certains clients demandent un service utilisant du routage à Paris mais pas en région.

Certains services réseau comme les VPRN ne sont pas disponibles sur tous les routeurs. Deux gammes de routeurs ont été déployées : des routeurs « Cœur de réseau » et des routeurs « d'Accès ». TMS utilise environ 50 routeurs de « Cœur de réseau » et 350 routeurs en « partie Accès ». Cette dichotomie est historique et induite par le coût des équipements : en effet un routeur doté de l'ensemble des fonctionnalités de niveau IP est un routeur puissant et complètement redondé dont le prix est de cinq à dix fois supérieur aux équipements d'accès.

Enfin l'utilisation de services réseau permet une redondance du transport en utilisant plusieurs chemins. Pour une même topologie vendue au client, il est possible de sécuriser le transport à travers le réseau. Dans l'exemple de la Figure 11, la topologie est un transport point à point et le client souhaite une sécurisation[3] de son trafic. MPLS et RSVP permettent de créer des tunnels sécurisés prédéfinis pour ce genre de contrat. On définit un chemin principal et jusqu'à sept chemins de secours indépendants permettant une sécurisation efficace du transport. Dans les faits, uniquement un ou deux chemins de secours les plus indépendants possibles sont utilisés.

RSVP est un protocole rapide pour sécuriser les flux à travers le réseau. Une fois la panne détectée, il peut réagir en moins de trois secondes pour rediriger le trafic dans un autre tunnel. Moyennant quelques optimisations il est même possible de rediriger le trafic en moins d'une seconde. Le vrai attrait de RSVP

[3] La terminologie métier utilise sécurisation pour parler d'augmentation de la sûreté de fonctionnement

pour TDF est de permettre l'établissement de tunnels prédéfinis ce qui facilite grandement, par la connaissance des chemins suivis, la gestion de la bande passante. Par contre cette méthode n'est pas très flexible car il faut définir manuellement, saut par saut, quel chemin le tunnel doit emprunter. Si l'on insère un nouveau routeur dans le réseau entre deux routeurs, tous les tunnels passant par ce nouveau routeur doivent être mis à jour. A noter que RSVP possède une possibilité de fonctionnement dynamique basée sur RSVP-TE mais non disponible dans TMS car les messages de « Traffic Engineering » ne se propage pas sur les topologies multi-aires de IS-IS.

Il existe une alternative à la définition stricte des chemins pour l'établissement des tunnels, c'est l'utilisation pour leurs créations du protocole LDP (Label Distribution Protocol). Ce protocole crée un tunnel en se basant sur le protocole de routage (tel que OSPF ou IS-IS) pour trouver le chemin le plus court vers une destination. Il est beaucoup moins réactif que RSVP car il peut s'écouler jusqu'à trente secondes de coupure entre une panne et le rétablissement d'un nouveau tunnel. En outre, ce degré de liberté laissé au réseau peut être antagoniste avec notre exigence de maitrise de la bande passante permettant d'éviter les situations de congestion. Les outils de capacity-planning modélisent mal le comportement du protocole LDP. Actuellement il n'est utilisé que pour des débits très faibles, inférieur à 1Mbps. Il n'est pas utilisé en priorité sur TMS car nous souhaitons limiter le nombre de services de ce type utilisé sur chaque artère du réseau.

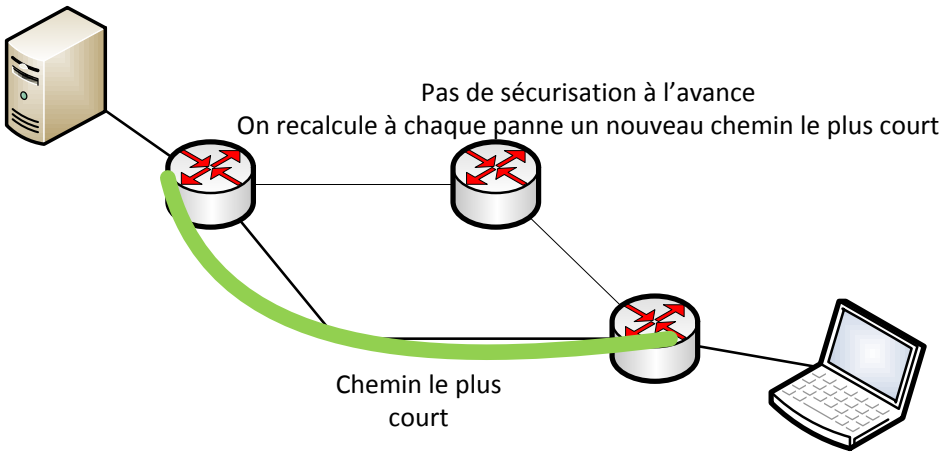


Figure 12 : Transport sécurisé par LDP

2.3.2. Description des services réseau et intégration

Le choix du type de service réseau pour chaque client consiste à remplir le quintuplet suivant :

$$\{Topologie\ souhaitée\ ;\ Nombre\ de\ points\ de\ livraison\ ;$$

$$Direction\ du\ trafic\ ;\ Débit\ utile\ ;\ Sécurisation\ souhaitée\}$$

Ces paramètres sont nécessaires pour définir le design du service final. Dans la plupart des cas, la topologie est de type point à point si bien que les théories précédentes s'appliquent facilement. Mais dans le cadre de topologies point vers multipoint ou multipoint vers multipoint, cela peut être insuffisant.

Les topologies multipoints peuvent êtres très différentes car le flux peut être bidirectionnel entre les points de services ou s'appuyer sur du multicast. Sur TMS, l'essentiel des topologies multipoint possèdent une source et plusieurs destinations alimentées en multicast. Ainsi il est exclu d'utiliser un service Epipe car il y a plusieurs destinations et on choisit de se limiter à un service VPLS car plus apte à faire transiter du multicast. Le flux est alors diffusé sur la topologie VPLS qui constitue un arbre de diffusion, tout comme le ferait un commutateur, mais en suivant des tunnels, voir la Figure 13. Enfin, en fonction du débit et de la nécessité de cicatriser rapidement, on utilise des tunnels crées par LDP ou RSVP pour le transport.

Le principe des protocoles BFD et OAM peuvent aider à améliorer la survivabilité du réseau en optimisant la détection de panne entre deux routeurs. Ces protocoles vont permettre à RSVP et LDP de réagir plus rapidement pour commuter vers un circuit viable lorsqu'il existe.

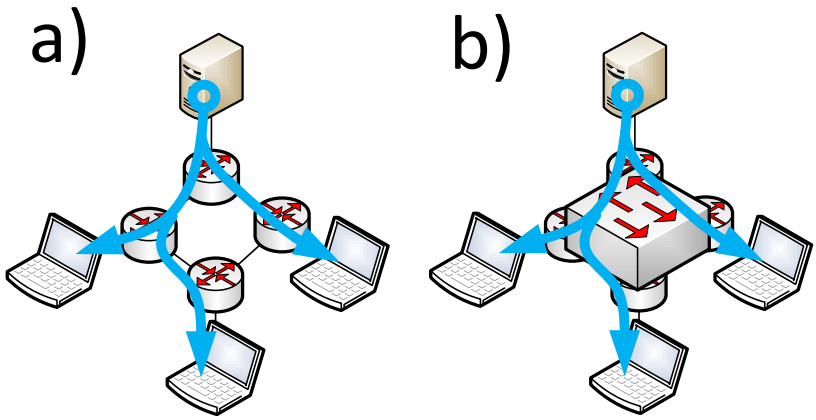


Figure 13 : Diffusion de multicast dans un service de type VPLS. a) représentation physique. b) utilisation logique du réseau

2.4.Ingénieries protocolaires

Dans le métier de TDF, on emploie souvent le terme d'ingénierie protocolaire pour définir l'ensemble de la solution fournie au client. Elle explicite notamment tous les protocoles mis en œuvre ainsi que la topologie du service réseau.

2.4.1. L'enjeu du transport national de multiplexes TNT

Chaque multiplexe représente un débit de 30 à 35 Mbps qu'il faut distribuer vers un peu plus de 150 points de diffusion. Ces points de diffusion peuvent alimenter de quelques centaines de milliers à plusieurs millions de foyers. On comprend alors l'enjeu que représente la sécurisation de ce type de transport. Le transport est alors sécurisé de multiples façons comme le résume la Figure 14 :

- Mise en place d'une tête de réseau (source) redondante sur deux sites distincts : au Fort de Romainville (Les Lilas) et le site de la Tour Eiffel (Paris)
- Transport sécurisé à travers le réseau TMS en utilisant au mieux la topologie mise en place
- Sécurisation de la réception sur le site de diffusion par satellite.

Sur la Figure 14 toute la partie encadrée représente le réseau Ethernet/IP TMS. C'est sur cette partie que se focalise l'étude.

A noter que le réseau est alimenté avec au moins deux sources et on peut considérer que la topologie est de type multipoint vers multipoint.

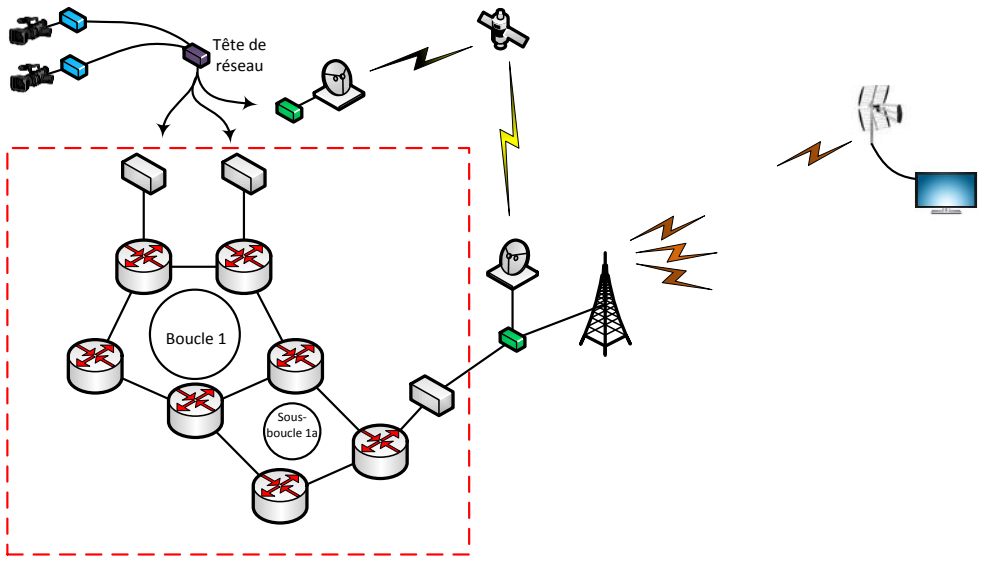


Figure 14 : Transport depuis le client jusqu'à l'utilisateur final

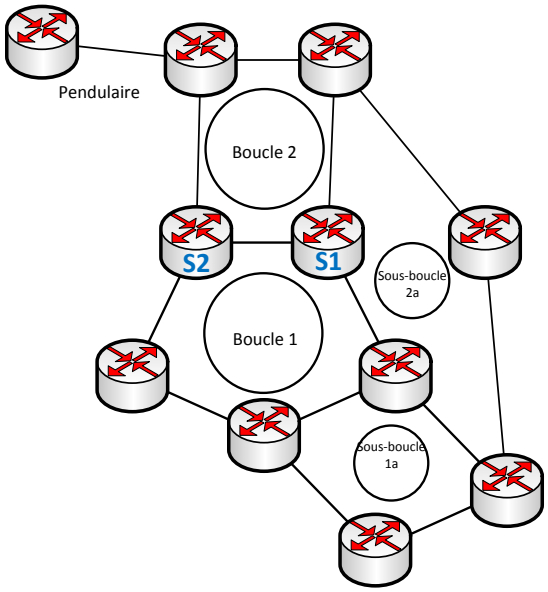


Figure 15 : Topologie initiale et vocabulaire de TMS

2.4.2. Ingénierie Rapid Spanning-Tree Protocol (RSTP)

La topologie initiale de TMS était basée sur des boucles imbriquées. C'est le protocole RSTP qui prenait en charge la sécurisation de l'ensemble du transport. La Figure 15 définit la terminologie employée dans cette ingénierie. Une boucle est une topologie de routeurs en anneau contenant les deux sources nationales. Une sous-boucle correspond aussi à une topologie en anneau mais elle s'appuie sur au moins deux routeurs membres d'une boucle ou sous-boucle. Enfin un pendulaire est une topologie contenant des routeurs non bouclés. L'ouverture logique des boucles de niveau 2 est gérée par le protocole STP (Spanning-Tree Protocol) et sa variante optimisée RSTP.

Le transport s'articule autour des deux sources S1 et S2 situées au centre du réseau, en région parisienne. Du fait de la redondance de sources et donc de la topologie multipoint vers multipoint, il faut mettre en place une solution particulière.

On utilise deux sources qui émettent un flux en multicast sur une topologie de niveau 2 utilisant des boucles. Ainsi deux problèmes sont alors facilement visibles :

- Les deux sources vont se brouiller si elles émettent le flux en même temps car le flux est du broadcast dans une topologie niveau 2.
- Si on veut tirer profit de la sécurisation de la boucle, il faut mettre en place une protection par anneau telle que RSTP [32], sinon le flux va faire le tour de la boucle à l'infini créant une tempête de broadcast.

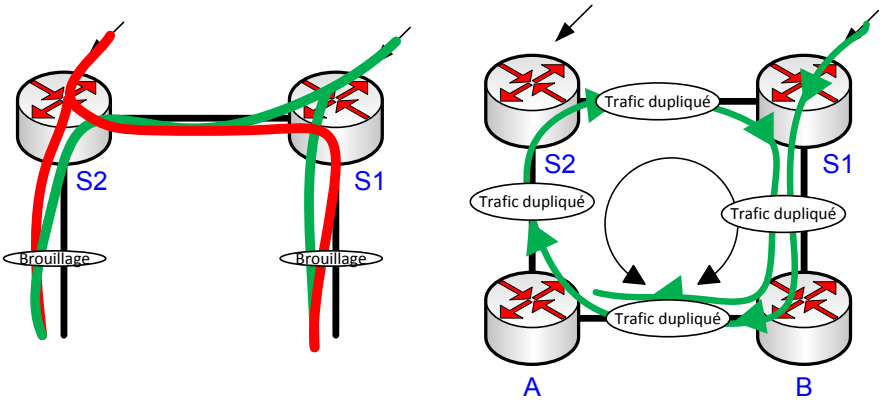


Figure 16 : Les problématiques de transport avec deux sources à travers une topologie en boucles

La première problématique se résout en mettant en œuvre une sécurisation pour que les deux sources n'émettent pas simultanément. Pour cela le protocole PIM (Protocol Independent Multicast) [33] est utilisé, il sélectionne une source en fonction d'une préférence préétablie. La redondance PIM doit être effectuée en amont du service VPLS car c'est un mécanisme de niveau 3. Elle peut être gérée en amont par deux équipements distincts comme dans la Figure 17 en a) ou dans les mêmes équipements qui portent le service VPLS et la sécurisation de niveau 3 comme montré en b).

Pour ce qui est du trafic dupliqué, la solution choisie se base sur le protocole RSTP qui est un protocole permettant d'éviter les boucles sur un réseau de commutateurs. Ainsi chaque boucle possèdera un point de coupure Spanning-Tree pour éviter les tempêtes de broadcast.

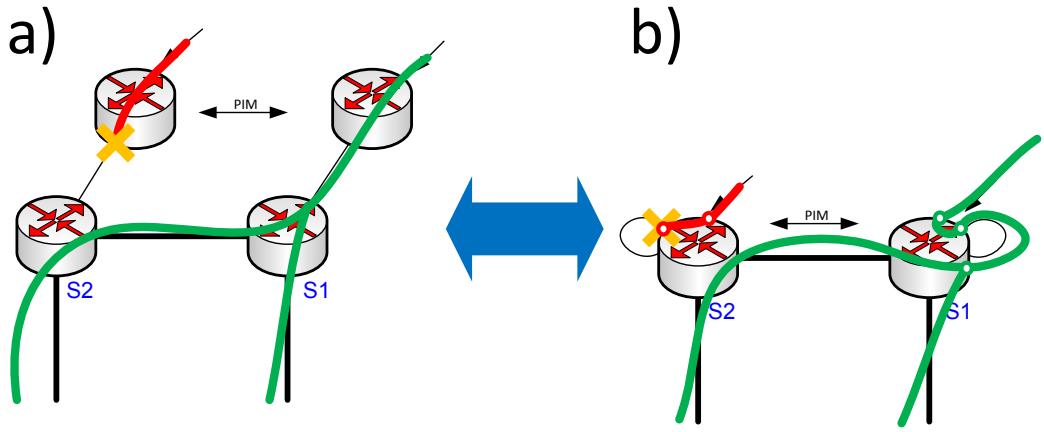


Figure 17 : Sécurisation de la tête de réseau avec la solution RSTP

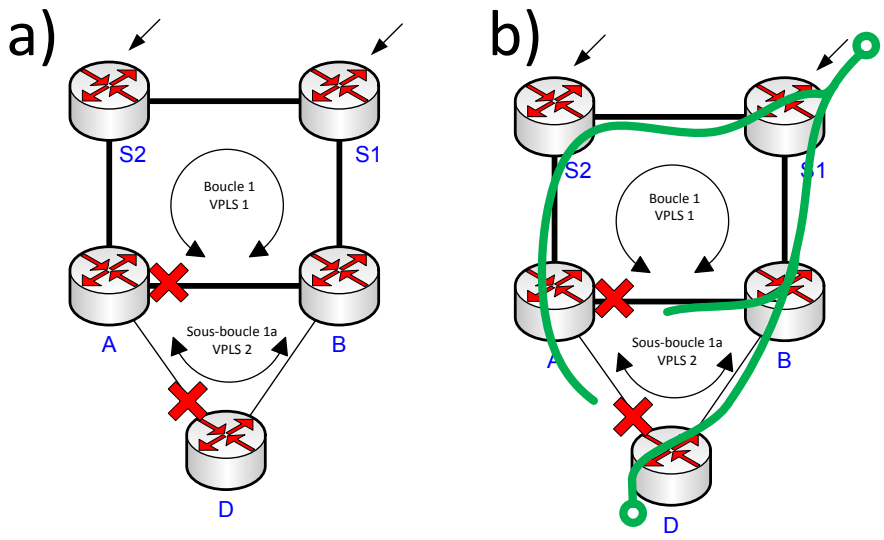


Figure 18 : a) Topologie fournie par RSTP. b) Diffusion par broadcast du multicast suivant la topologie

Pour renforcer la sécurité de fonctionnement on n'utilise pas un VPLS global mais plusieurs VPLS chaînés. Sur la Figure 18 la topologie fait apparaitre deux boucles : une boucle principale VPLS 1 et une sous-boucle VPLS 2. On appelle routeurs pères les routeurs A et B qui sont à la frontière des deux services. Les routeurs pères sont chargés de délimiter les deux VPLS mais ils sont aussi garant du bon fonctionnement du réseau. Dans le cas d'une erreur de configuration RSTP entrainant une tempête de broadcast dans une sous-boucle, les routeurs pères bloquent tout flux venant de la sous-boucle par un mécanisme de filtrage. Ainsi tout trafic cherchant à « remonter » dans la boucle principale sera supprimé protégeant le reste du réseau de la panne générale.

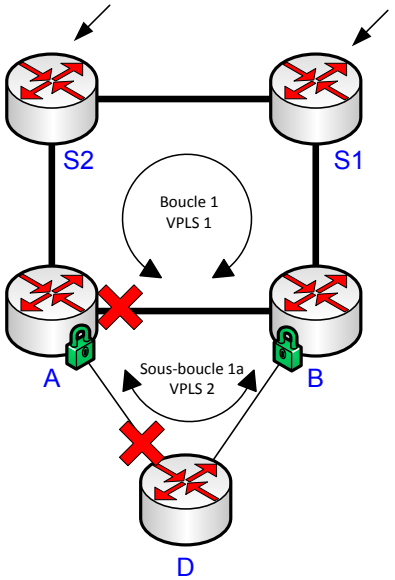


Figure 19 : Filtres anti-retour sur les routeurs pères

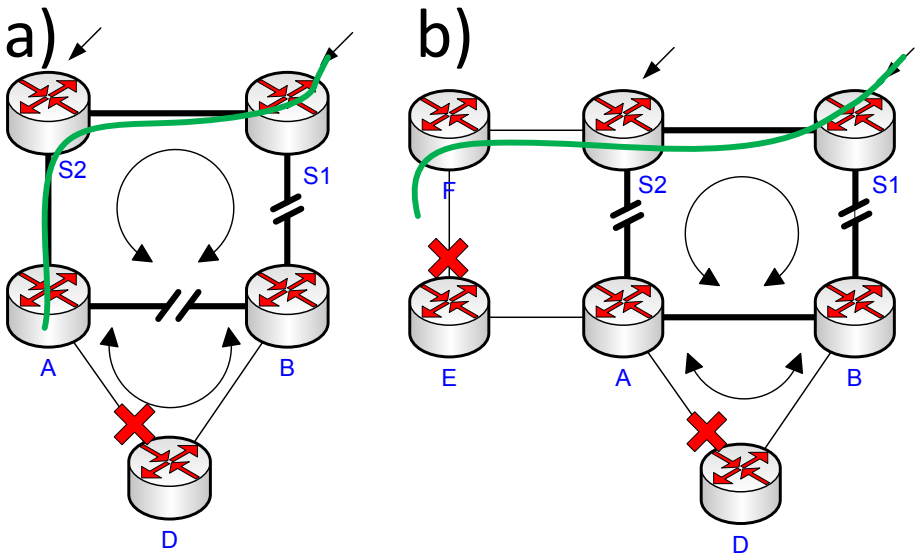


Figure 20 : Cas bloquants de doubles pannes dans une boucle principale

Cette ingénierie n'a été mise en place que dans le contexte du transport de la TNT car elle est relativement lourde à gérer et chaque nouvelle sous-boucle vient complexifier la solution. Cette ingénierie devait essentiellement faire face à des pannes simples au sens un seul lien en panne à un instant donné dans une boucle. Avec l'apparition des doubles pannes, plusieurs cas bloquants ont été mis en évidence.

Le premier cas bloquant provient d'une double panne dans une boucle qui alimente une sous-boucle. Sur la Figure 20 (a) cette double panne correspond à une coupure de la liaison AB et une coupure de la liaison S1B. Il existe physiquement une façon d'alimenter la sous-boucle via le routeur A. Mais vu qu'il n'y a aucune panne dans la sous-boucle ADB, la coupure RSTP entre A et D est maintenue empêchant tout flux provenant de A d'alimenter la sous-boucle.

Pour le second cas bloquant tel que décrit sur la Figure 20 (b) la double panne se localise encore sur la boucle principale mais il existe physiquement une solution d'alimentation par la boucle ouest représentée par S2FEA. Même constat que dans a), il n'existe aucune panne sur cette boucle ouest donc la coupure RSTP entre E et F n'a pas de raison de s'interrompre, empêchant tout trafic de passer du routeur F au routeur E. De plus l'existence des filtres anti-retours rendent impossible le fait qu'une sous-boucle puisse alimenter la boucle principale dans ce cas.

Enfin il existe un dernier cas bloquant pour la prise en charge du flux aux têtes de réseau. En effet la solution actuelle utilise le protocole PIM entre les deux routeurs portant la source. Une panne directe de l'équipement relié à TMS est détectée et permet une bascule automatique, mais la détection d'absence de flux reste problématique car non identifiable par TMS. Le port connecté à

l'équipement qui fait la transition du monde audiovisuel vers le monde IP reste opérationnel, bloquant la détection de la panne. Le contenu est seulement absent et le routeur S1 est incapable avec PIM de le détecter pour forcer la bascule sur S2. Ce cas bloquant est présenté en Figure 21 (a)

Cette solution « boucles imbriquées » n'utilise que des boucles et dans le cas de nouvelles liaisons venant intensifier le maillage, il est parfois compliqué d'intégrer ces liaisons sous la forme de nouvelles boucles. Dans l'exemple de la Figure 21 (b), une nouvelle liaison peut être réalisée entre le routeur C et le routeur D et l'existant constitue une sous-boucle ADB. Il est impossible d'intégrer dans la boucle actuelle cette liaison ; il faut donc découper cette topologie en deux sous-boucles en une boucle ADC et une sous-boucle BDC. C'est un cas particulier d'une insertion de liaison qui ne crée pas d'anneau ; pour la logique de RSTP cette topologie est représentée par une sous-boucle. Ici pour un routeur cette solution n'est pas intéressante et ainsi cette liaison ne sera pas exploitée par l'ingénierie RSTP.

Plusieurs faiblesses de l'ingénierie « boucles imbriquées » ont été décrites dont celle de ne pouvoir tirer bénéfice d'un maillage du réseau et la défaillance de résilience en présence de double panne dû à l'utilisation du protocole RSTP. Par ailleurs plusieurs mises à jour successives des logiciels des routeurs ont permis la mise en œuvre d'une nouvelle génération de protocole MVPN : le VPN Multicast.

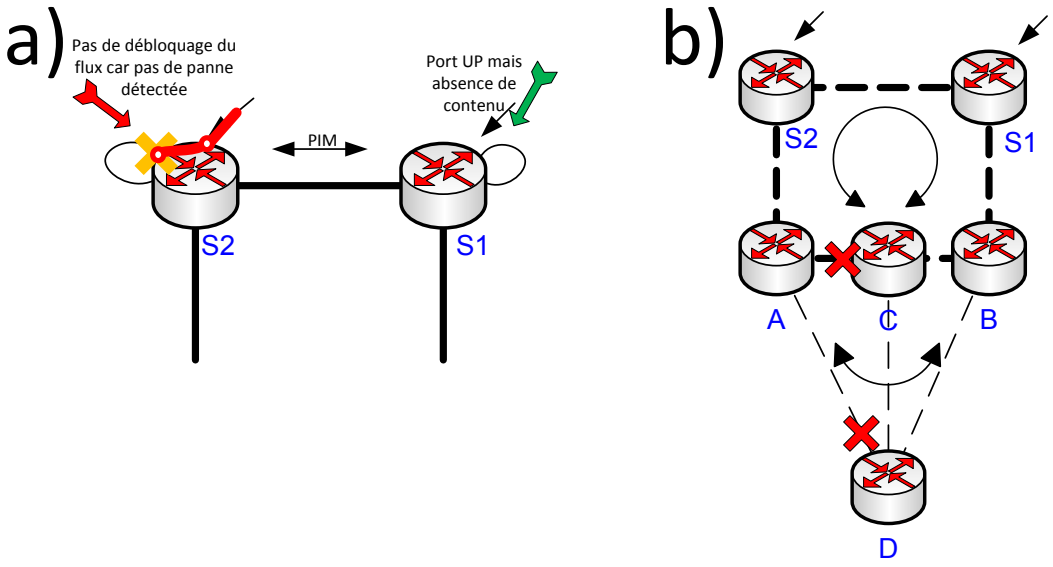


Figure 21 : a) Cas bloquant lors d'une panne en amont de TMS. b) Intégration d'un maillage dans une boucle

2.4.3. Ingénierie Multicast VPN (MVPN)

Les solutions MVPN sont différentes et ont toutes pour objectif de transporter du contenu multicast dans des VPN. Elles s'appuient sur des protocoles liés au multicast tels que PIM et IGMP (Internet Group Management Protocol) [34] pour transporter de manière efficace les flux multicast.

Le premier protocole MVPN appelée Draft-Rosen [35] utilisait des tunnels GRE (Generic Routing Encapsulation). Il a été très vite écarté par TDF car non compatible avec les exigences de rapidité de convergence. Actuellement plusieurs autres implémentations sont disponibles et sont arrivées à maturité.

2.4.3.1. Description de la solution

Parmi les techniques MVPN disponibles, la plupart proviennent de solutions se basant sur le protocole BGP (Border Gateway Protocol) qui n'est pas encore activé sur TMS. Ces solutions ont été testées et écartées pour laisser place à une solution MVPN originale, non testée au préalable par Alcatel-Lucent mais tout de même approuvée par leurs experts : MVPN VRF-Lite (VPN Routing and Forwarding).

Avant même de parler du transport du multicast, il faut noter que le fonctionnement d'un VPRN classique n'est pas identique à celui d'un VPRN en VRF-Lite. Un VRPN classique utilise BGP pour échanger les routes à apprendre et l'ensemble forme une sorte de grand routeur disposant d'interfaces réparties géographiquement. La principale différence pour un VPRN en VRF-Lite est que chaque instance du service est locale au routeur et prend ses décisions en fonctions des échanges avec les autres instances du service. Pour simplifier on peut considérer que les VPRN en VRF-Lite simulent des routeurs virtuels uniques s'échangeant des routes au travers d'un protocole de routage (voir Figure 22).

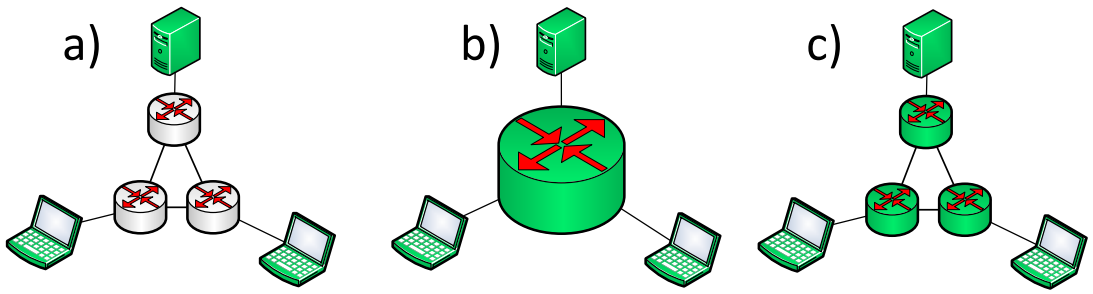


Figure 22 : Différences entre les MVPN. a) Topologie physique et client (en vert). b) MVPN classique avec un service simulant UN seul routeur pour le service. c) MVPN en VRF-Lite où chaque équipement physique porte un routeur virtuel.

Les technologies MVPN utilisent les services de type VPRN incluant du routage dans le service. Du fait de la différence de routeurs entre « cœur de réseau » et « accès », il y a deux niveaux de service. Les routeurs de cœur utilisent du routage pour acheminer les flux multicast alors que les routeurs de la partie accès utilisent des techniques de niveau Ethernet. Ces routeurs se comportent plutôt comme des switchs.

Comme présenté précédemment, le VPRN constitue un réseau de routeurs virtuels capable de transporter les flux multicast avec le routage et le protocole PIM. Le VPLS sert à diffuser le contenu à la presque totalité des points de service et également à relier les VPRN entre eux. On obtient alors un service avec un cœur (prise en charge) en VPRN et du protocole PIM, et une partie accès utilisant des VPLS et le protocole IGMP ainsi que sa variante IGMP-Snooping. Pour rappel, le cœur de réseau est défini par les routeurs de tête de réseau en région parisienne et par l'ensemble des routeurs situés dans les POP (Point Of Presence) des grandes villes en s'appuyant sur une infrastructure optique. La partie accès est plutôt répartie en région et s'appuie sur des faisceaux hertziens.

Le protocole PIM est responsable dans la partie VPRN de la constitution d'un arbre de diffusion pour le transport du multicast. On utilise PIMv3 en mode SSM (Source-Specific Multicast). Ce protocole a été choisi en raison du fonctionnement des deux têtes de réseau et des passerelles correspondantes (cf. 2.4.1 et Figure 14) qui annoncent la même source aux deux routeurs sources S1 et S2. En effet, le même contenu est diffusé sur le réseau à partir de deux équipements.

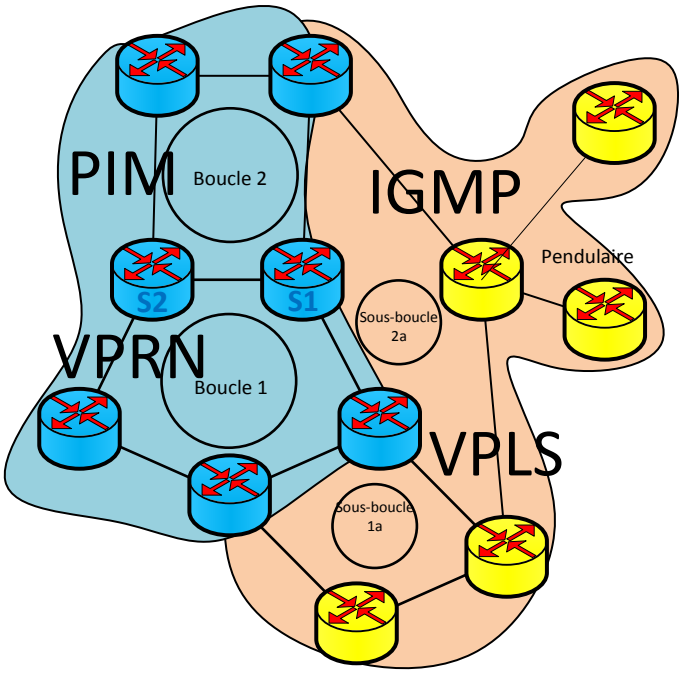


Figure 23 : Répartition des domaines VPRN et VPLS avec leurs protocoles associés

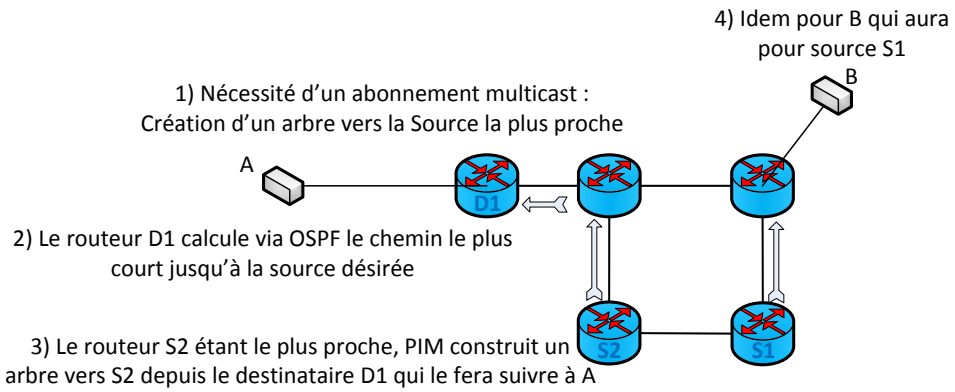


Figure 24 : Construction de l'arbre PIM à travers les VPRN

En mode SSM il est nécessaire de préciser la source du flux et surtout comment la joindre. Cela peut être fait par routage comme dans la solution choisie à l'aide du protocole OSFP qui est implémenté dans les VPRN pour échanger des routes entre les différentes instances des VPRN. PIM-SSM construit donc son chemin le plus court depuis la destination jusqu'à la source en se basant sur le protocole de routage, choisissant ainsi le chemin le plus court jusqu'à l'une des sources. La construction de l'arbre PIM peut être résumée par la Figure 24. Il est important de noter que l'arbre se construit jusqu'à la source la plus proche, ce qui permet d'intégrer une ou plusieurs sources alors qu'en RSTP on se limitait à deux sources. Le choix de la source devient alors impossible et les multiples sources que l'on va utiliser fonctionneront en même temps.

Mais la principale caractéristique de cette solution est l'utilisation de VPLS qui ne sont pas capables d'utiliser OSPF ou PIM en combinaison avec des VPRN. Dans le domaine VPLS on va utiliser IGMP-Snooping sur les VPLS et IGMP sur les routeurs porteurs de VPRN à la frontière avec des VPLS (appelés routeurs pères).

L'une des autres limitations des routeurs de la partie accès est qu'ils ne peuvent pas utiliser IGMPv3 dans leurs services mais seulement IGMPv2. Etant donné qu'on utilise PIMv3 en mode SSM, il est nécessaire de spécifier la source dans les abonnements mais IGMPv2 ne le permet pas. Ainsi on doit utiliser une « translation » pour que le mécanisme PIM puisse fonctionner et cette fonction est portée par les routeurs pères.

Enfin pour des raisons de redondance, il peut exister plus d'un routeur père pour chaque VPLS. Vu que le multicast se comporte comme du broadcast sur la topologie VPLS, il est impératif que seul un unique routeur père diffuse le flux dans le VPLS. Cette fonction est garantie par PIM qui va échanger des informations entre les routeurs pères au sein du VPLS pour savoir quel routeur père sera diffuseur principal. Aussi pour que les demandes d'abonnement puissent joindre tous les routeurs pères on utilise IGMP-Snooping qui permet de suivre et

d'agir sur les échanges IGMP au sein du VPLS. Cette fonction est mise en œuvre par chaque membre du VPLS.

Il est intéressant de remarquer que les protocoles PIM et OSPF sont accélérés par BFD qui est activé au sein des VPRN. L'intérêt de BFD, qui a été décrit dans le paragraphe 2.2.1, est d'accélérer la détection de panne afin qu'OSPF et PIM convergent plus rapidement. Cela permet dans les VPRN d'accélérer la reconstruction d'un nouvel arbre et dans les VPLS de basculer en moins d'une seconde d'un routeur père à un autre. BFD ne modifie pas le comportement de l'ingénierie MVPN mais permet des temps de coupures plus faibles.

La Figure 25 résume la diffusion du flux multicast pour l'ingénierie MVPN. Dans le VPRN, le flux est envoyé sans broadcast seulement à ceux qui en ont besoin (ici uniquement P1) et dans le VPLS le flux est diffusé sur toute la topologie pour joindre D1, D2 et D3. Les routeurs pères P1, P2 et P3 échangent via PIM en utilisant la topologie VPLS des informations pour savoir qui doit diffuser dans le VPLS.

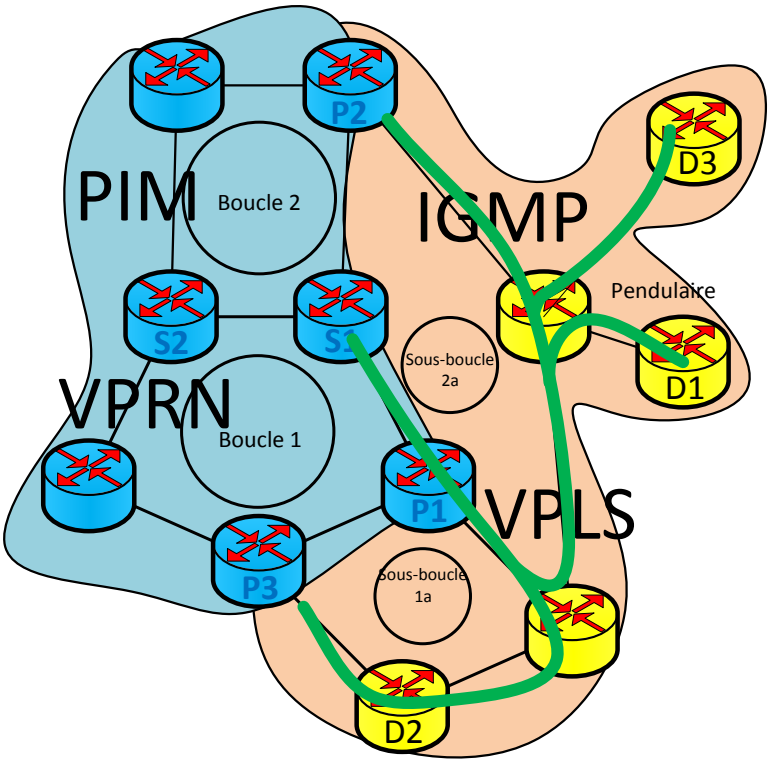


Figure 25 : Diffusion du flux pour l'ingénierie MVPN

2.4.3.2. Retour sur les cas de panne précédents

Cette ingénierie a été conçue pour remplacer l'ingénierie existante et doit donc répondre aux mêmes exigences tout en résolvant les problèmes de la solution actuelle.

La Figure 26 illustre le cas d'une double panne dans la boucle principale : une coupure de la liaison S1-B et une de la liaison A-B. Physiquement il existe un chemin pour joindre les deux sources depuis le routeur D à travers le réseau mais il ne pouvait être utilisé dans la solution RSTP. Dans la nouvelle ingénierie le routeur B est le routeur principal en situation nominal ce qui signifie qu'il gère les abonnements IGMP pour son VPLS mais aussi qu'il est chargé de construire l'arbre PIM dans la partie VPRN. Avec cette situation de panne particulière, le routeur B est toujours capable de gérer les abonnements IGMP et de construire l'arbre PIM à travers le VPLS. Ainsi le flux va arriver au routeur B en passant par D qui sera capable de récupérer le contenu au passage car le multicast est diffusé par broadcast à travers la topologie VPLS. Normalement le routeur B est censé distribuer à son VPLS le flux multicast qu'il vient de recevoir mais dans ce cas le flux provient du même port que celui sur lequel le routeur est censé l'envoyer. Cet envoi est opportunément bloqué par les mécanismes multicast. Une dernière remarque est que la source du flux change et passe de S1 à S2 car S2 devient plus proche de B suite à ces pannes.

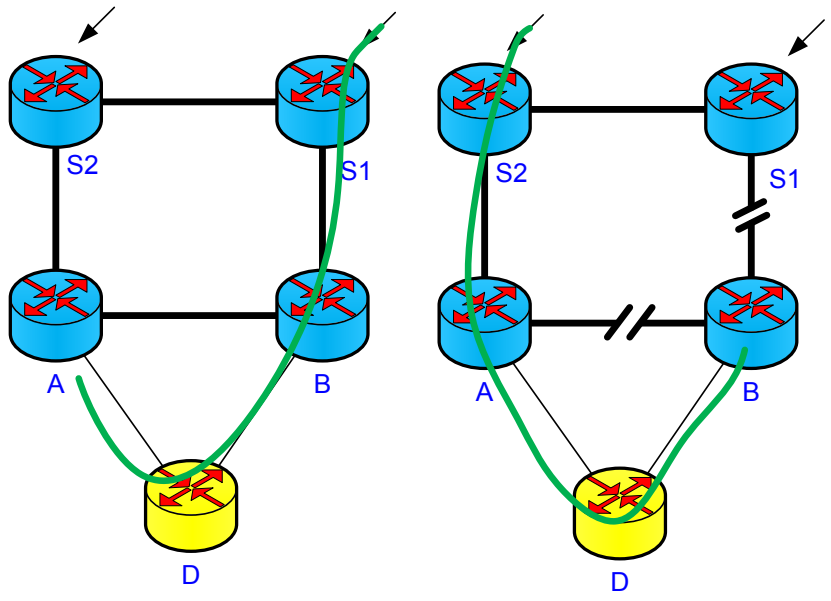


Figure 26 : Retour sur le 1er cas bloquant qui ne pose pas de problème au MVPN

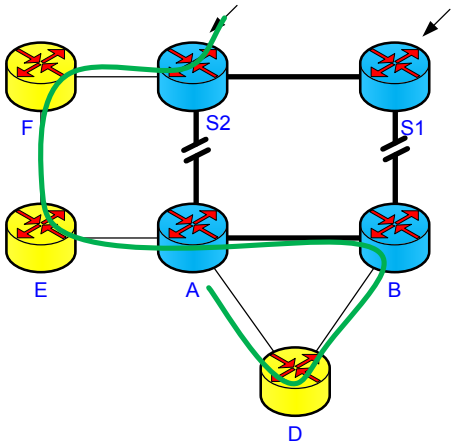


Figure 27 : Retour sur le 2nd cas bloquant ne pose pas de problème au MVPN

Il existe un deuxième cas bloquant dans l'ingénierie RSTP qui est solutionné par MVPN tel qu'illustré par la Figure 27. Ici le routeur B est encore le routeur principal pour alimenter le VPLS qui distribue le flux pour le routeur D. Avec cette double panne le routeur B est capable de demander le flux via A et le VPLS qui alimente les routeurs E et F pour construire l'arbre en passant par ces routeurs. Ensuite le routeur B distribue le flux comme en situation nominale.

Enfin contrairement à l'ingénierie RSTP, la nouvelle solution peut gérer plus de deux routeurs pères pour un VPLS.

2.4.3.3. Faiblesses du MVPN

En raison de la dichotomie des structures VPRN et VPLS utilisées, l'ingénierie MVPN s'appuie sur des ensembles plus grands. En effet dans l'ingénierie RSTP un sous-ensemble est définit par une sous-boucle et ses pendulaires alors pour la nouvelle solution ce sont les routeurs pères porteurs de VPRN.

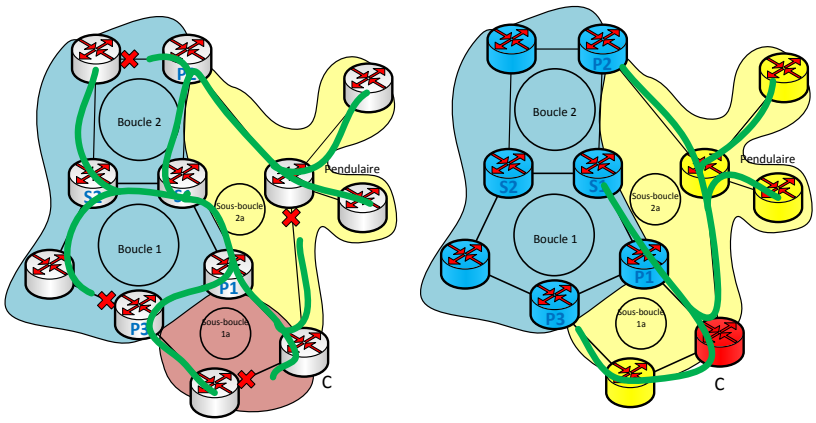


Figure 28 : Sous-ensembles de deux ingénieries

Il est toutefois possible de remplacer certains routeurs de la « partie accès » comme le routeur C en rouge dans la Figure 28 par des routeurs type « routeur de cœur », pour permettre de réduire la taille des ensembles mais cela nécessite un investissement. De plus lorsque le sous-ensemble devient vraiment imposant comme dans la Figure 29, le système est moins fiable car un seul routeur va diffuser pour tout l'ensemble même s'il existe un chemin plus court pour joindre la source. Dans la solution RSTP il était possible de placer la coupure STP à l'endroit le plus efficace afin que chaque routeur destination se retrouve au plus proche possible d'une source. Cela a un impact direct sur la disponibilité du service car le routeur D1 est plus éloigné de la source et donc sa probabilité de subir un reroutage ou une bascule est plus forte.

Ce problème de sensibilité aux reroutages est l'une des préoccupations du réseau TMS. Pour rappel le trafic audiovisuel est très sensible à la perte de paquet et supporte donc mal les reroutages : chaque perte de paquet se traduit par un impact sur l'image. Cela peut se quantifier par le fait qu'une bascule de transport IP de l'ordre de 1s impacte pendant une durée d'environ 4s la réception finale.

Ces comportements ne peuvent être analysés objectivement que par une quantification de la probabilité de fonctionnement de l'état « nominal » et de celle de fonctionnement de l'état dit de « secours » tout à fait fonctionnel. Ainsi la nouvelle ingénierie apporte apriori un gain de disponibilité globale car elle résout certains cas bloquants mais ce gain n'est-il pas contrebalancé par le fait que cette solution induit une augmentation de la fréquence des reroutages ? Le Chapitre 3 est consacré à répondre à cette question.

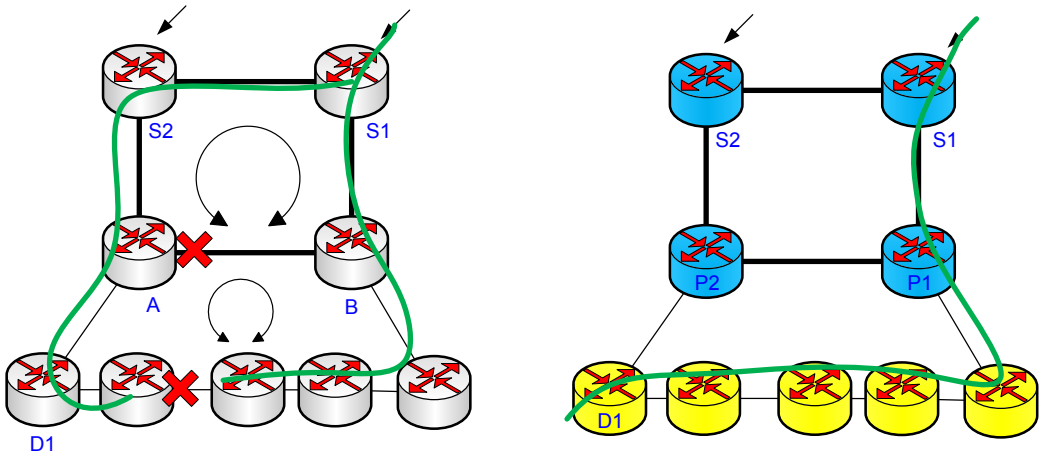


Figure 29 : Différence de répartition de la diffusion dans la sous-boucle entre RSTP et MVPN

Chapitre 3

Analyse de la disponibilité du réseau

Chapitre 3 Analyse de la disponibilité du réseau 51
3.1. Etude de la disponibilité 52
3.1.1. Choix de modélisations et disponibilité 52
3.1.2. Arbres de défaillances 53
3.1.3. Chaines de Markov 54
3.2. Modélisation par Réseaux Bayésiens 55
3.2.1. Présentation 55
3.2.2. Modélisation de la disponibilité par RB 59
3.2.2.1. Construction du RB sans cycle 59
3.2.2.2. Modélisation des caractéristiques des réseaux IP 64
3.2.3. Modélisation des ingénieries protocolaires 65
3.2.3.1. Cas Simple 1 66
3.2.3.2. Cas Simple 2 69
3.2.3.3. Cas réel avec une seule destination 72
3.2.3.4. Cas réel multi-destinations 74
3.3. Simulation sous Modeler 76
3.3.1. Introduction à l'utilisation de Modeler 76
3.3.2. Cas simple 79
3.3.3. Cas réel 81

3.1.Etude de la disponibilité

3.1.1. Choix de modélisations et disponibilité

Suite à de précédents travaux sur TMS, il a été possible de quantifier la disponibilité annuelle moyenne des équipements élémentaires du réseau. Les valeurs utilisées dans cette étude listées dans la Table 1 sont des données réalistes mais pour des raisons de confidentialité les valeurs réelles ne seront pas communiquées. Nous n'intégrons pas les données liées à la maintenance préventive ni celles liées aux interventions programmées. Elles tiennent uniquement compte des pannes et phénomènes non-contrôlés.

Ces disponibilités représentent des moyennes basées sur la topologie du réseau TMS. En effet certain routeurs sont redondés avec deux cartes de contrôle et deux alimentations provenant de sources différentes ce qui améliorent leur taux de disponibilité. Pour les liaisons louées, l'engagement des opérateurs tiers est souvent plus faible que celui retenu pour mener l'exercice d'analyse. Pour les faisceaux hertziens, une moyenne de trois bonds est fréquente même si certaines liaisons sont directes. Il existe aussi d'autres technologies utilisées sur TMS comme des liaisons XDSL dont l'engagement de qualité de service est significativement en retrait par rapport aux valeurs retenues mais elles ne sont pas utilisées dans le cadre du transport des multiplexes nationaux.

Il existe de nombreuses méthodes pour analyser la disponibilité d'un système qui peuvent être réparties en deux approches : par modélisation probabiliste ou par simulation. La première catégorie vise à appliquer des données probabilistes (telles que les taux de panne, les taux de réparation, la durée moyenne d'un arrêt, …) afin d'estimer la durée d'indisponibilité alors que la seconde se focalise sur la représentation virtuelle numérique du réseau soumise à un profil de pannes pour mesurer l'indisponibilité. Dans les deux cas nous allons avoir besoin d'outils utilisés en sûreté de fonctionnement pour modéliser finement et fidèlement le comportement du système.

Table 1 : Liste des taux de disponibilité utilisés dans l'étude

Equipement	Indisponibilité associée	Indisponibilité annuelle
Routeur Alcatel (gamme routeur « d'accès »)	**10^{-5}**	**5.26 min**
Liaison Faisceau Hertzien (moyenne de 3 bonds)	**$5.\ 10^{-5}$**	**26.3 min**
Liaison Louée Fibre Optique (moyenne 80km)	**10^{-4}**	**52.6 min**

Toutes les techniques utilisent les principes de causalité traduites par des graphes. L'analyse systémique permet un découpage du système pour un traitement par graphes. Cette approche permet une étude d'un évènement redouté en intégrant tous les composants du système.

Même si des méthodes de calcul analytiques existent [36-37], le calcul manuel devient vite inenvisageable pour un réseau de grande taille comme TMS qui peut intégrer plusieurs centaines de constituants interconnectés suivant une topologie bouclée et maillée. Pour la partie simulation il faut choisir un outil qui sera capable d'intégrer au maximum les comportements du réseau. Pour la partie modélisation probabiliste il existe de nombreux choix possibles allant des outils du monde de l'entreprise aux outils encore en développement. Dans les parties suivantes seront seulement présentées les modélisations par Arbres de défaillances, Chaines de Markov et Réseaux Bayésiens.

3.1.2. Arbres de défaillances

L'analyse par Arbres de Défaillances est très répandue dans les entreprises pour l'analyse de risques et offre aussi la possibilité d'étudier la disponibilité. Ils permettent de représenter de façon synthétique l'ensemble des combinaisons d'évènements qui peuvent conduire à une défaillance, comme l'illustre la Figure 30.

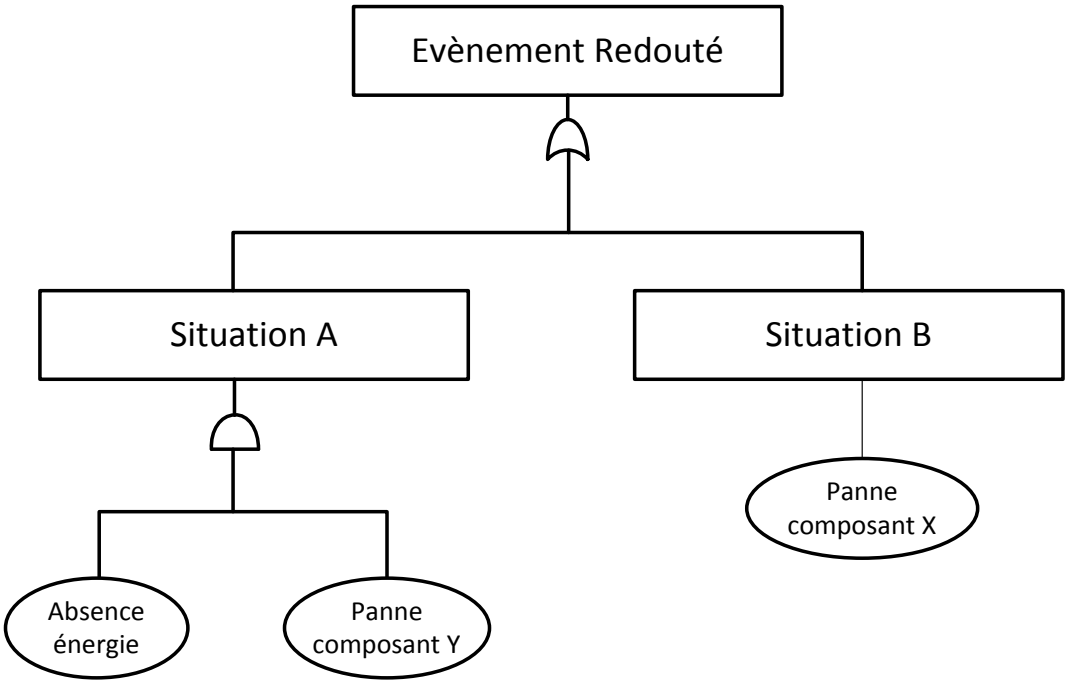


Figure 30 : Exemple d'analyse par arbres de défaillances

Cette méthode permet l'intégration de différents niveaux qui peuvent ensuite être à leur tour découpés et vérifiés par une nouvelle étude par arbre de défaillances. Ainsi le système est découpé en de nombreux sous-systèmes qui représentent le fonctionnement du système et ses points faibles. La construction des arbres de défaillances se base sur la décomposition du système en risques et les causes associées. On retrouve ainsi en haut de l'arbre l'évènement redouté (la panne du système ou la perte de contrôle du système par exemple) et en bas les éléments qui constituent le système. Cette méthode possède des limites comme le fait qu'un élément du système ne peut apparaitre qu'une fois et qu'il ne peut être relié à différents constituants. Cela implique le fait qu'il soit impossible de traiter des éléments interdépendants bien que certaines propositions le permettent en adaptant le modèle [38]. Aussi les arbres de défaillances ne gèrent que des variables booléennes ce qui fait que certains états du système ne peuvent être représentés. Par exemple un état de panne ne peut être décomposé en deux états de panne, une « panne réparable » et une « panne non réparable ». Pour le modèle ces deux états sont résumés dans la variable booléenne : état ne fonctionne pas. Il est impossible de représenter la dynamique du système comme une vanne qui peut être en panne en position ouverte ou fermée.

Ces limites cantonnent cette méthode à des systèmes simples, et elle ne peut s'appliquer à des systèmes complexes comme des centrales nucléaires, des avions militaires de dernière génération ou encore des réseaux télécoms. C'est pourquoi pour analyser la dynamique de ces systèmes on fait appel aux Chaines de Markov.

3.1.3. Chaines de Markov

Une Chaine de Markov est une représentation du système par états où chaque nœud correspond à un état du système et chaque arc représente une probabilité de passer d'un nœud à l'autre. Cette modélisation peut être utilisée pour représenter la disponibilité d'un système. Les probabilités de transitions sont appelées λ pour les probabilités de panne et μ pour les probabilités de réparation. La représentation graphique permet de visualiser le comportement d'un système mais le traitement s'effectue à l'aide d'une représentation matricielle des données.

Dans l'exemple de la Figure 31 les états sont séparés en deux parties, une où le système continue de remplir sa fonction et une autre où le système est en panne. Une fois le système en panne il peut revenir dans un état fonctionnel par réparation du composant X mais il existe une probabilité de passer dans un état où il faut entièrement réparer le système avant de le remettre en fonction.

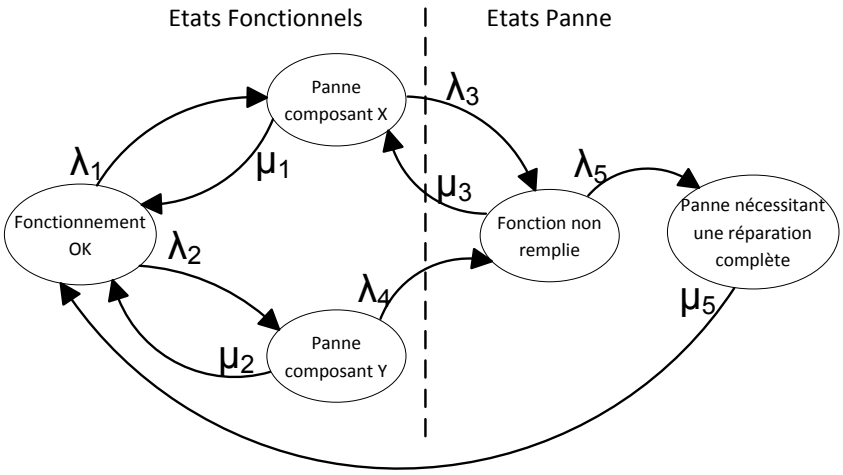


Figure 31 : Représentation d'un système sous forme de Chaînes de Markov

La Chaine de la Figure 31 correspond à la matrice de transition suivante :

$$\begin{bmatrix} 1-(\lambda_1+\lambda_2) & \lambda_1 & \lambda_2 & 0 & 0 \\ \mu_1 & 1-(\mu_1+\lambda_3) & 0 & \lambda_3 & 0 \\ \mu_2 & 0 & 1-(\mu_2+\lambda_4) & \lambda_4 & 0 \\ 0 & \mu_3 & 0 & 1-(\mu_3+\lambda_5) & \lambda_5 \\ \mu_5 & 0 & 0 & 0 & 1-\mu_5 \end{bmatrix}$$

Cette représentation s'applique très bien lorsqu'on dispose de toutes les probabilités de pannes et de réparations. Toutefois le nombre d'états élémentaires possibles dépend du nombre de constituants et de leurs relations. Dans le cas de grands systèmes la construction et la manipulation de la Chaine deviennent problématiques. De plus leur représentation probabiliste est facilement compréhensible pour un chercheur mais les industriels sont plus concernés par des représentations moins détaillées. C'est dans ce contexte que nous allons nous intéresser aux Réseaux Bayésiens pour la suite de l'étude.

3.2.Modélisation par Réseaux Bayésiens

3.2.1. Présentation

Très utilisés dans le domaine de la sûreté de fonctionnement, les Réseaux Bayésiens (RB) permettent par représentation graphique de modéliser de manière probabiliste un système complexe [39-42]. Il est possible de découper celui-ci en autant de sous-parties que nécessaire pour faciliter l'analyse et mettre en évidence les points faibles du système. Le modèle utilise des graphes acycliques orientés pour représenter le système et les logiciels utilisent un algorithme d'inférence basé sur les arbres de jonction pour effectuer les calculs [43]. En fait cette méthode trouve sa force dans une représentation graphique qui aide à comprendre un système.

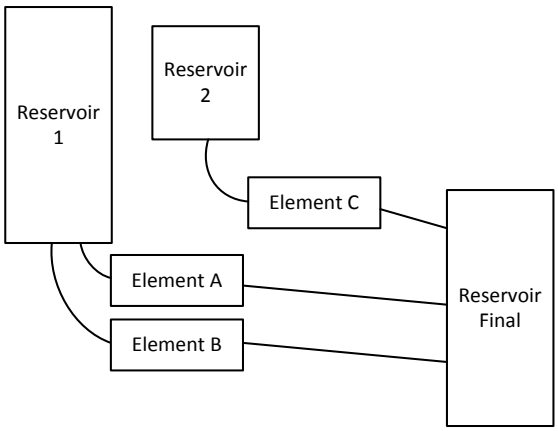


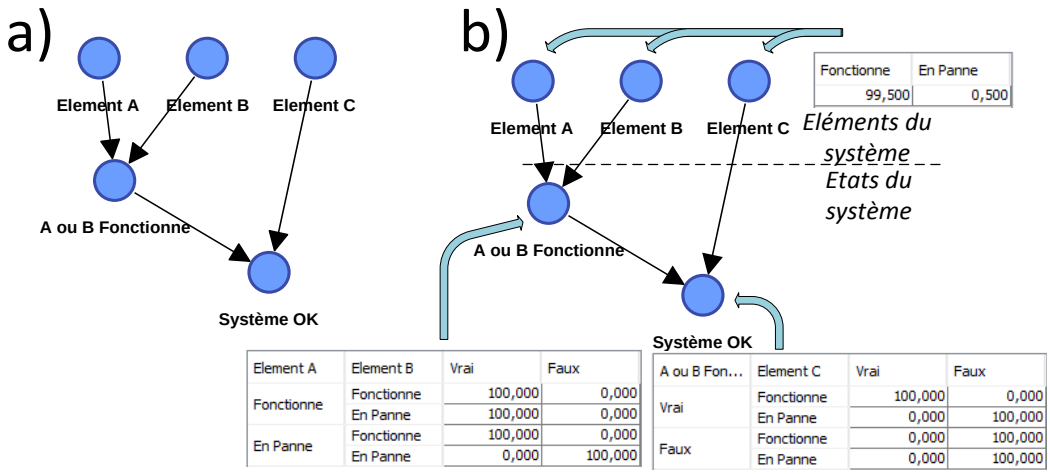
Figure 32 : Représentation d'un système de mélange avec des vannes

Pour présenter le fonctionnement des RB il est plus facile d'utiliser un exemple concret. L'exemple présenté en Figure 32 est un système de mélange utilisant des réservoirs équipés de vannes. Il a pour objectif de récolter de manière contrôlée le contenu de deux réservoirs.

Le réservoir 1 possède deux vannes A et B en parallèle qui sont chacune capable de réaliser la fonction requise. Le réservoir 2 ne possède qu'une seule vanne et ne possède donc pas de redondance. La fonction du système est assurée si A ou B fonctionne et si C fonctionne car on considère que les réservoirs sont toujours prêts à distribuer et que le réservoir final possède toujours de la place pour le mélange.

Le fonctionnement de ce système peut se représenter par le RB de la Figure 33. Le RB non documenté est fourni en a). La partie haute représente les éléments physiques du système tandis que la partie basse représente des sous-états du système. Le RB détaillé est présenté en b). A chaque élément est associée une table de probabilité définissant a priori les états de fonctionnement et de dysfonctionnement des composants. Dans la partie basse on retrouve des tables de probabilités conditionnelles (TPC) qui sont définies selon la structure fiabiliste du système. La première table présente le comportement de l'interaction entre A et B, qui est une TPC déterministe modélisant une propagation des probabilités par une logique OU. Alors que la seconde présente le comportement de l'interaction entre les deux réservoirs, un ET logique.

La terminologie suivante est utilisée : les nœuds porteurs d'une information probabiliste de fonctionnement sont appelés nœud parent et les nœuds porteurs de TPC représentant la structure fiabiliste du système sont appelés nœuds enfants. Ces derniers représentent une factorisation de la structure fiabiliste du système.



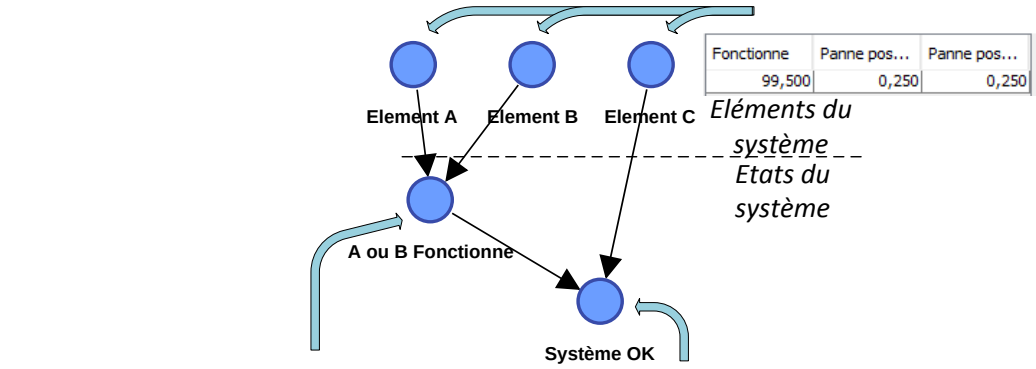
Fonctionne	En Panne
99,500	0,500

Element A	Element B	Vrai	Faux
Fonctionne	Fonctionne	100,000	0,000
	En Panne	100,000	0,000
En Panne	Fonctionne	100,000	0,000
	En Panne	0,000	100,000

A ou B Fon...	Element C	Vrai	Faux
Vrai	Fonctionne	100,000	0,000
	En Panne	0,000	100,000
Faux	Fonctionne	0,000	100,000
	En Panne	0,000	100,000

Figure 33 : a) Représentation graphique d'un système sous RB. b) Description du système représenté avec ses tables remplies

A ce stade et vu la complexité du système décrit, une analyse par arbres de défaillances aurait pu répondre au besoin. Mais les RB offrent la possibilité par inférence de réaliser le diagnostic ainsi que la possibilité de modéliser des systèmes à composants multi-états [44]. Ils peuvent donc traiter d'autres situations plus réalistes. Pour notre exemple on pourrait découper l'état « En panne » par « En panne position ouverte » et « En panne position fermée ». Le RB ne serait pas modifié graphiquement mais le contenu des nœuds parents et enfants seraient modifiés tel que présenté dans la Figure 34.



Fonctionne	Panne pos...	Panne pos...
99,500	0,250	0,250

Element A	Element B	Vrai	Faux
Fonctionne	Fonctionne	100,000	0,000
	Panne pos. Ouverte	0,000	100,000
	Panne pos. Fermée	100,000	0,000
Panne pos. Ouverte	Fonctionne	0,000	100,000
	Panne pos. Ouverte	0,000	100,000
	Panne pos. Fermée	0,000	100,000
Panne pos. Fermée	Fonctionne	100,000	0,000
	Panne pos. Ouverte	0,000	100,000
	Panne pos. Fermée	0,000	100,000

A ou B Fon...	Element C	Vrai	Faux
Vrai	Fonctionne	100,000	0,000
	Panne pos. Ouverte	0,000	100,000
	Panne pos. Fermée	0,000	100,000
Faux	Fonctionne	0,000	100,000
	Panne pos. Ouverte	0,000	100,000
	Panne pos. Fermée	0,000	100,000

Figure 34 : Représentation par RB du système de vanne en incluant deux états de pannes différents

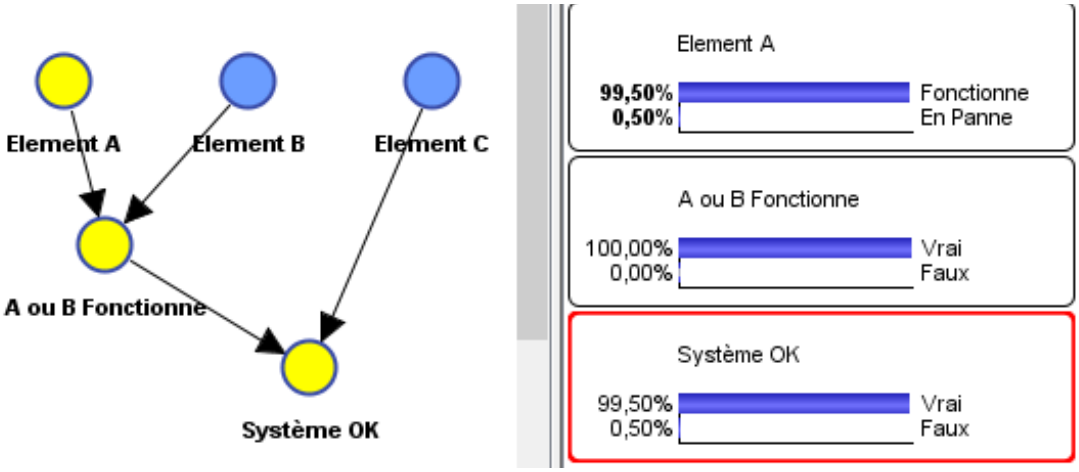


Figure 35 : Analyse par l'algorithme d'inférence du logiciel BayesiaLab

Chaque élément possède un état de panne décomposé en deux états équiprobables dans notre cas résumant le cas de panne. La TPC attachée au test de fonctionnement de A ou de B reflète une conséquence différente de la panne suivant la position ouverte ou fermée. En effet si la vanne A est bloquée en position fermée, la vanne B est capable à elle seule de faire fonctionner cette partie du système ; si la vanne A est bloquée en position ouverte, le contenu du réservoir 1 sera déversé sans retenue dans le réservoir final empêchant le système de remplir sa fonction.

Avec cette représentation, nous disposons d'un modèle qu'il est possible d'analyser par un algorithme d'inférence. Il existe plusieurs outils implémentant celui-ci. Nous avons choisi BayesiaLab car il est déjà utilisé par d'autres chercheurs du laboratoire. La Figure 35 montre comment le logiciel représente les différentes probabilités d'état du système. L'interface permet de choisir le ou les nœuds à visualiser de manière détaillée. Par exemple la Figure 35 montre que la probabilité de fonctionner du système est de 0.995 car c'est la probabilité associée à l'état Vrai du nœud « Système OK ».

Les RB offrent également des aides aux diagnostics car il est possible d'intégrer le fonctionnement ou la panne de certains équipements pour le calcul par inférence.

Cette analyse non booléenne ne pouvant être traitée par les arbres de défaillances montre bien l'apport des RB. Nous allons pouvoir l'appliquer à notre problématique sur le réseau de TDF. C'est cette propriété qui justifie ici l'utilisation de la modélisation par RB.

3.2.2. Modélisation de la disponibilité par RB

Dans cette étude nous proposons une approche originale pour modéliser la disponibilité du réseau IP/MPLS à l'aide des RB. Bien que la disponibilité de la plupart des systèmes soit modélisable par RB, aucune étude existante ne cherche à modéliser la disponibilité d'un réseau spécifique à l'audiovisuel. Cette spécificité provient du fait qu'un réseau pour le transport de l'audiovisuel doit être performant en termes de rapidité de convergence et en temps de transport. Afin de modéliser le plus fidèlement possible le réseau, nous allons d'une part intégrer la disponibilité des routeurs et des liaisons inter-routeurs et d'autre part intégrer les fonctionnalités des protocoles.

Par la suite nous allons modéliser la disponibilité d'un réseau IP/MPLS pour le transport de multiplexes nationaux et appliquer cette méthodologie pour modéliser les différences entre deux ingénieries protocolaires.

3.2.2.1. Construction du RB sans cycle

La liberté de construction du RB est telle qu'il est possible de modéliser de nombreuses façons le même système et d'avoir les mêmes résultats sous différentes formes [45]. Une difficulté supplémentaire est que notre architecture en boucle peut poser problème car les RB sont acycliques.

Le nœud cible du RB doit représenter la disponibilité du système qui est, dans notre cas, la disponibilité de tous les points de services d'un multiplexe de la TNT. Nous allons utiliser des nœuds parents pour représenter les composants et suffisamment de nœuds enfants pour modéliser la structure des protocoles de manière graphique. Nous nous intéressons particulièrement aux routeurs stratégiques qui sont chargés de récupérer le flux venant de chemins différents (Figure 36).

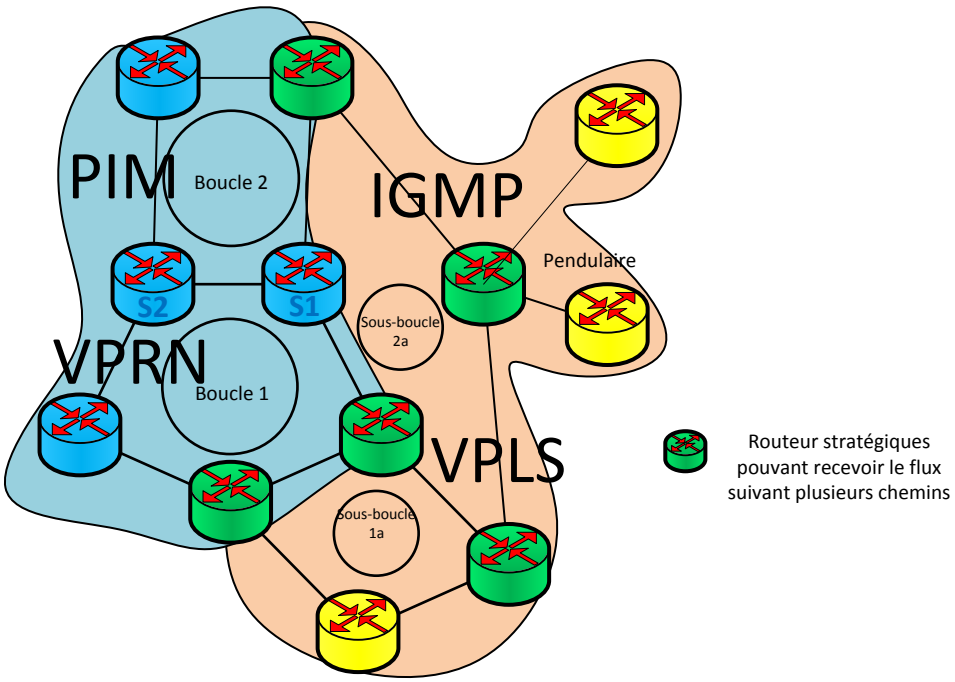


Figure 36 : Routeurs stratégiques

Nous proposons de définir un nœud de RB modélisant le fait qu'un routeur stratégique soit alimenté ou non. Un ensemble d'éléments constituant les différentes voies pourront être agrégés au sein d'un seul nœud. Ainsi sur la Figure 37, la topologie du service diffusé en A peut être représentée de deux façons. Le premier RB est une représentation de la probabilité jointe complète en une seule table tandis que le second simplifie la table du nœud "A Alimenté" en factorisant cette probabilité jointe. Ces deux représentations sont équivalentes pour le calcul de la disponibilité mais la différence réside dans la lourdeur de la TPC. La Figure 38 montre que le premier RB se focalise sur le nœud cible qui va faire l'agrégation de toutes les situations. Le résultat est que sa table est grande ; on a ici 32 cas différents à traiter et même si ce sont pour la plupart des cas où l'état est faux il ne faut pas oublier un seul cas vrai sinon le modèle n'est plus représentatif du fonctionnement du protocole. C'est une méthode de modélisation qui rend difficile la maintenance et la modélisation du modèle. Dans le second RB ces états complexes à gérer dans le premier RB sont agrégés dans les nœuds « Chemin 1 » et « Chemin 2 ». Ce second modèle est plus lisible et expressif sur la fonction rendue et évite des erreurs de modélisation.

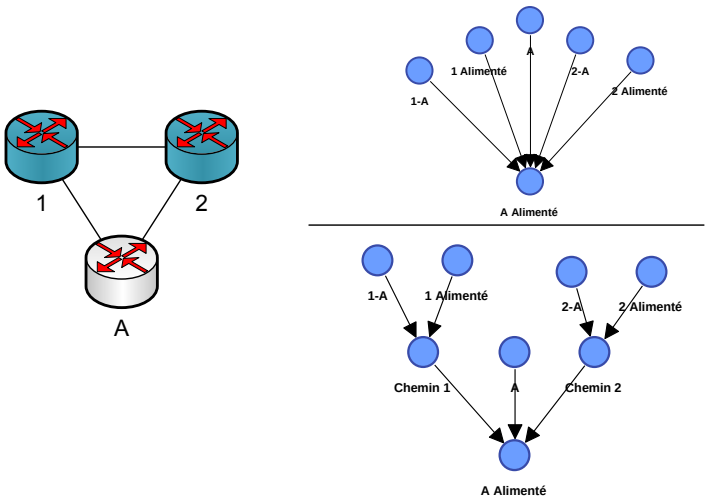
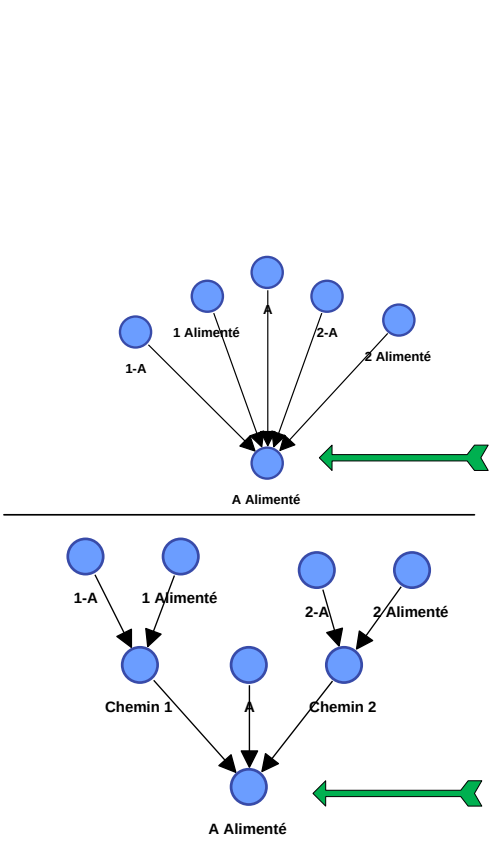


Figure 37 : Topologie simple représentée en RB



A	1 Alimenté	1-A	2 Alimenté	2-A	Vrai	Faux
Ok	Ok	Ok	Ok	Ok	100,000	0,000
				NOk	100,000	0,000
			NOk	Ok	100,000	0,000
				NOk	100,000	0,000
		NOk	Ok	Ok	100,000	0,000
				NOk	0,000	100,000
			NOk	Ok	0,000	100,000
				NOk	0,000	100,000
	NOk	Ok	Ok	Ok	100,000	0,000
				NOk	0,000	100,000
			NOk	Ok	0,000	100,000
				NOk	0,000	100,000
		NOk	Ok	Ok	100,000	0,000
				NOk	0,000	100,000
			NOk	Ok	0,000	100,000
				NOk	0,000	100,000
NOk	Ok	Ok	Ok	Ok	0,000	100,000
				NOk	0,000	100,000
			NOk	Ok	0,000	100,000
				NOk	0,000	100,000
		NOk	Ok	Ok	0,000	100,000
				NOk	0,000	100,000
			NOk	Ok	0,000	100,000
				NOk	0,000	100,000
	NOk	Ok	Ok	Ok	0,000	100,000
				NOk	0,000	100,000
			NOk	Ok	0,000	100,000
				NOk	0,000	100,000
		NOk	Ok	Ok	0,000	100,000
				NOk	0,000	100,000
			NOk	Ok	0,000	100,000
				NOk	0,000	100,000

A	Chemin 1	Chemin 2	Vrai	Faux
Ok	Vrai	Vrai	100,000	0,000
		Faux	100,000	0,000
	Faux	Vrai	100,000	0,000
		Faux	0,000	100,000
NOk	Vrai	Vrai	0,000	100,000
		Faux	0,000	100,000
	Faux	Vrai	0,000	100,000
		Faux	0,000	100,000

Figure 38 : Problème relatif à la taille de la TPC

Les topologies étudiées sont bouclée, mais les RB les représentants ne sont pas des modèles nécessairement cycliques. C'est pourquoi il est nécessaire de faire attention lors de la construction du RB afin que ce dernier ne soit pas bouclé. L'important est que la structure fiabiliste du modèle qui permet de calculer la disponibilité du système ne soit pas une projection de la topologie du réseau IP/MPLS. Aussi les scénarios de fonctionnement sont disjoints ce qui permet d'utiliser une représentation factorisée par RB sans cycle. Il faut remarquer que la méthode de modélisation utilisée fait l'hypothèse que les protocoles fonctionnent toujours correctement. Cette hypothèse est réaliste pour un réseau en production pour lequel toutes les erreurs de fonctionnement des protocoles ont été détectées et corrigées.

Cette logique de modélisation complexifie la représentation du RB et surtout la validation. Lorsque le système devient trop complexe il est impossible de le modéliser correctement sans ajouter un nombre de nœuds intermédiaires suffisants. Bien qu'il existe des algorithmes de construction des RB se basant sur l'étude des données tel que présenté dans [46], ils sont peu applicables à nos problématiques de modélisation des comportements des protocoles.

La complexité du RB est l'une des limites du modèle mais il est possible de composer avec. L'autre problème des RB est qu'ils sont acycliques ce qui demande d'être prudent lors de la représentation des boucles. Dans l'exemple de la Figure 39, il est possible de répéter cette logique pour décrire des architectures plus compliquées mais le fait de se focaliser sur les routeurs stratégiques reste important pour structurer les parties du modèle RB.

Enfin pour un système plus complet on utilise le principe tel que présenté dans le schéma de la Figure 40. Ici on imbrique deux sous-boucles et on s'intéresse au fait que le routeur B soit alimenté. B peut recevoir le flux du routeur 3 ou du routeur A mais ce dernier peut aussi recevoir le flux provenant de 3 via B. Pour cela nous utilisons deux états, « A Alimenté via G » (gauche) et « A Alimenté via D » (droite), qui seront agrégés dans le nœud « A Alimenté ». Si l'on souhaite considérer les deux états il ne faut pas faire de cycle et représenter correctement ces possibilités.

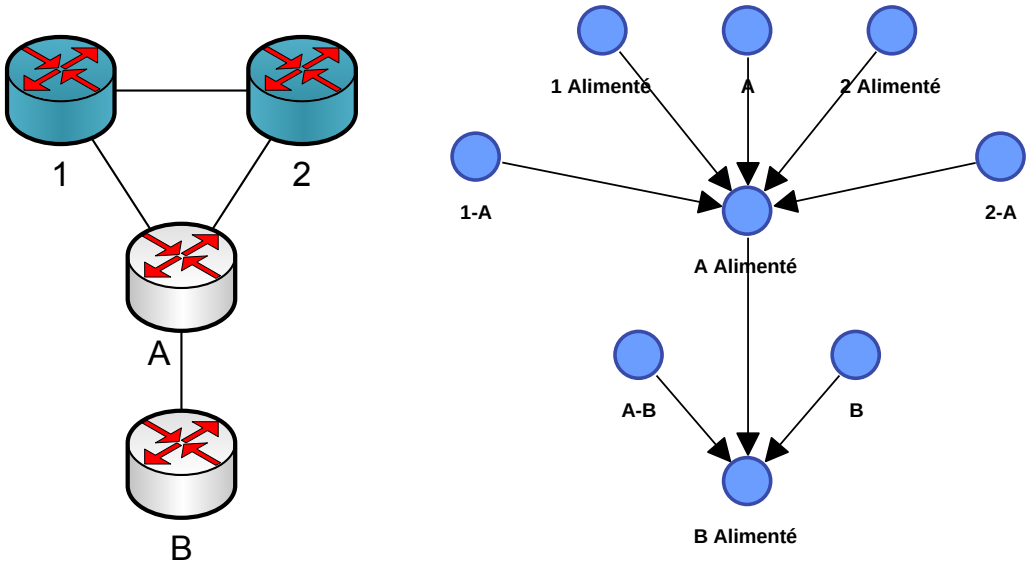


Figure 39 : Construction du RB en conservant la logique définie

Pour simplifier la conception des RB, on peut envisager une traduction de chacune des topologies basiques du réseau pour permettre de construire de manière fidèle et précise le modèle du réseau de TDF.

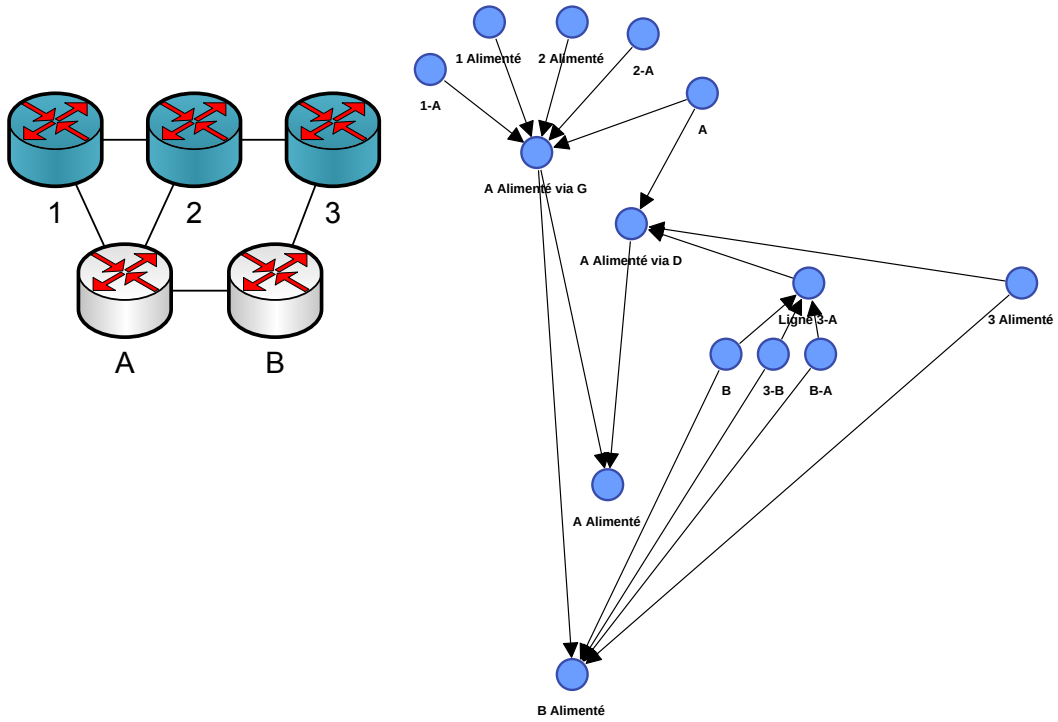


Figure 40 : Architecture proche de la réalité modélisée sous RB

3.2.2.2. Modélisation des caractéristiques des réseaux IP

Il est intéressant de profiter des caractéristiques multi-états des RB pour modéliser les situations de reroutages. Nous allons découper les états des nœuds enfants pour inclure la situation de reroutage. Pour ce faire nous allons utiliser trois états qui résument les situations présentées dans la Figure 41 :

- **a) 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.
- **b) Etat secours :** Lorsqu'une panne se produit sur le chemin principal, le système étant structuré pour résister à n'importe quelle simple 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.
- **c) 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.

Ce découpage de l'état fonctionnel en deux sous-états permet d'intégrer les situations de reroutages qui permettent au système de fonctionner le temps de la réparation.

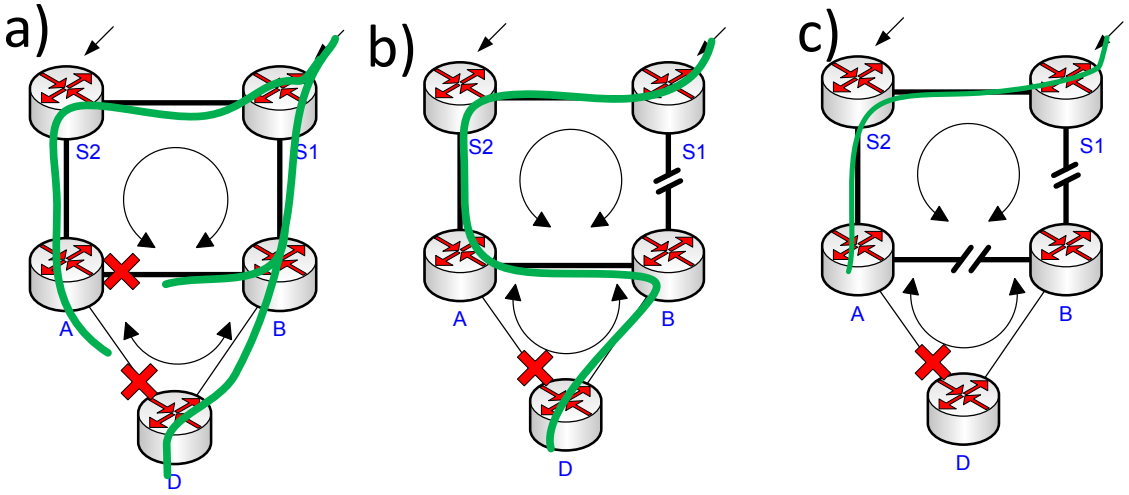


Figure 41 : Alimentation du routeur B. a) Situation nominale. b) Situation secours. c) Situation panne

3.2.3. Modélisation des ingénieries protocolaires

Un des objectifs de la modélisation du réseau TMS par RB est de comparer objectivement les deux ingénieries RSTP et MVPN. Celles-ci ont des comportements assez différents. Elles sont analysées qualitativement dans le chapitre 2 et présentent des performances différentes en disponibilité. En résumé, l'ingénierie RSTP offre des situations plus stables et moins sujettes à des reroutages car les points de coupures sont placés de la manière la plus optimale possible. Le dynamisme de l'ingénierie MVPN a pour conséquence que dans la partie VPLS, nous ne sommes jamais en situation optimale et la probabilité de reroutage est plus importante, ce que nous voulions justement éviter.

L'utilisation des RB statiques avec trois états permet la modélisation de la disponibilité sur un réseau IP/MPLS mais aussi et surtout de différencier les deux ingénieries. En fait les deux premiers états représentent des états de fonctionnement alors que le dernier est un vrai cas de panne. L'intérêt est de représenter les situations reroutées où le flux ne suit pas le chemin nominal pour quantifier la probabilité de se trouver dans une situation moins stable. La modélisation va objectiver la différence entre l'ingénierie RSTP et l'ingénierie MVPN pour savoir comment on progresse sur certains critères. Il est important de se rappeler que malgré un reroutage rapide il existe toujours des impacts à l'image le temps que la passerelle se resynchronise avec la source. Un inconvénient des RB est justement de ne pas modéliser les basculements d'états et surtout le temps nécessaire aux protocoles pour converger vers une situation stable.

Pour clarifier nous allons regarder quelques exemples qui vont permettre d'illustrer les résultats attendus. L'analyse porte sur la différence des probabilités d'état obtenues à l'aide des modèles.

Table 2 : Analyse de résultats simples pour comprendre le modèle

Diff Prob Nominal	Diff Prob Secours	Diff Prob Panne	Conclusions
0	0	0	Aucune différence fonctionnelle. La disponibilité annuelle reste identique.
+0.001	0	-0.001	Diminution de l'indisponibilité de 0.1%. Gain direct sur la disponibilité sans contrepartie car l'équilibrage se fait sur la situation nominale.
0	+0.001	-0.001	Diminution de l'indisponibilité de 0.1%. grâce à l'état secours.
+0.005	+0.005	-0.001	Diminution de l'indisponibilité de 0.1%. Les augmentations sont réparties sur les deux états.

Ces exemples permettent d'appréhender les résultats que nous allons obtenir et nous allons devoir intégrer des exemples plus concrets pour vérifier ces comportements. Dans la suite, nous allons nous intéresser à modéliser par RB certaines topologies simples et un cas réel pour avoir de premiers résultats et vérifier que les RB sont un outil utilisable pour notre problématique. L'objectif est de voir quelle solution est la plus efficace pour transporter les flux multicast à travers le réseau TMS.

3.2.3.1. Cas Simple 1

Nous commençons par les ingénieries présentés en Figure 42 et nous évaluerons la disponibilité du service sur le routeur D.

Dans la solution RSTP le flux part de la source S1 et suit la topologie définie par la protection des boucles. On identifie deux boucles dont une boucle principale en haut et une sous-boucle en bas s'appuyant sur les routeurs pères A et B. Pour l'ingénierie MVPN les routeurs de la boucle principale en haut sont capables de faire du VPRN et utilisent donc PIM pour transporter le flux entre B et S1. Le routeur père B est chargé de diffuser dans son VPLS avec ici un seul membre le routeur D et va donc envoyer le flux jusqu'au routeur A qui le bloquera.

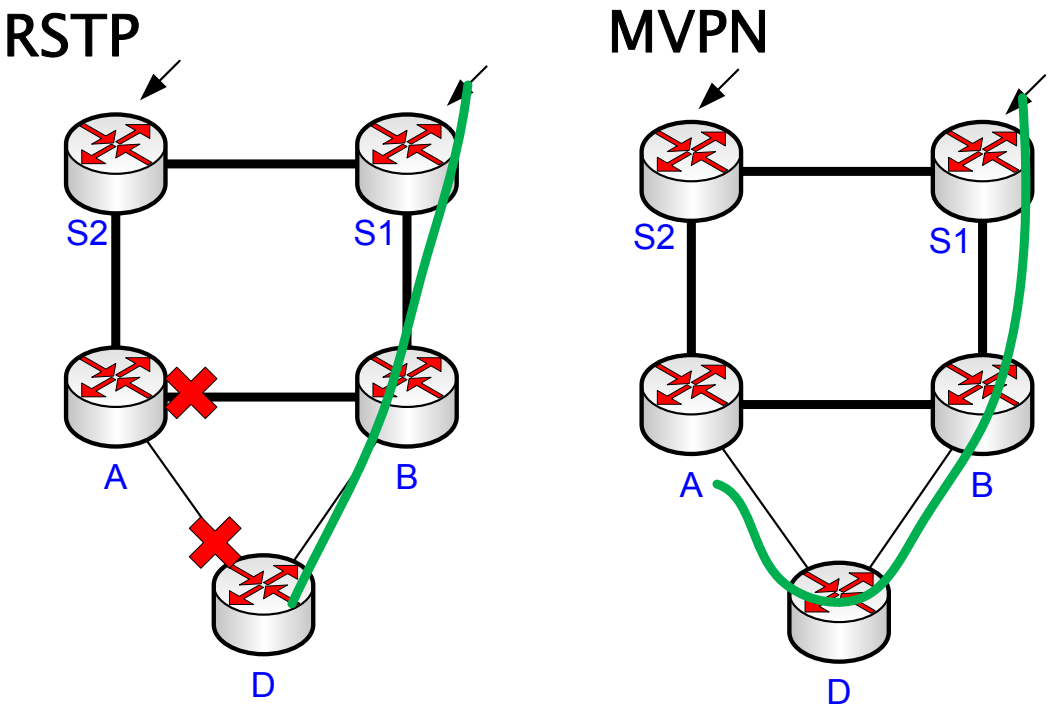


Figure 42 : Cas simple 1

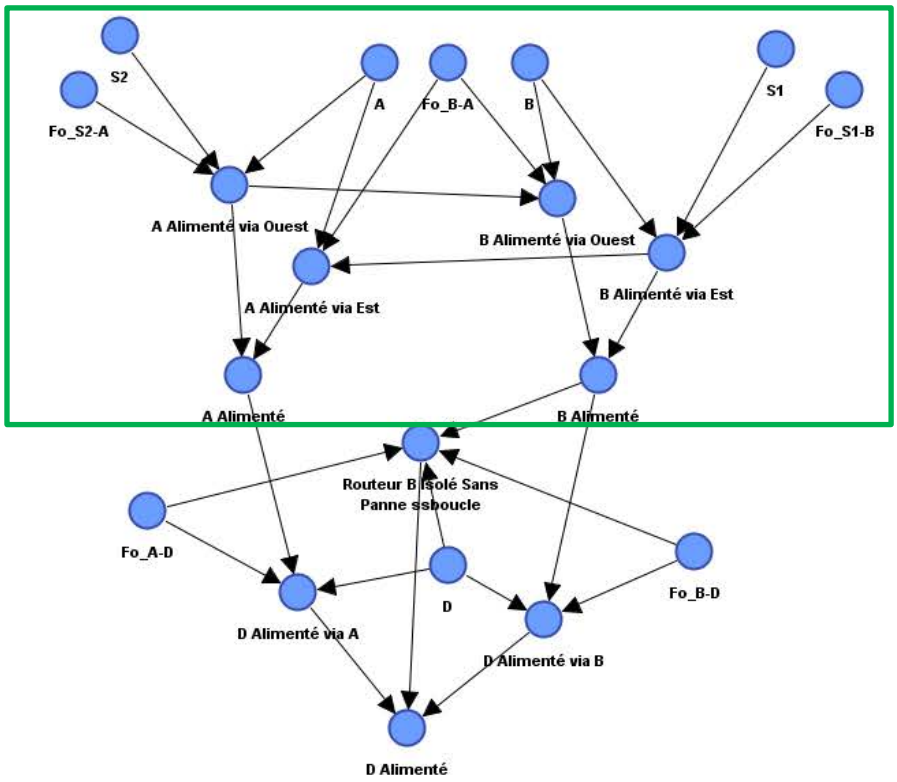


Figure 43 : Modélisation par RB du cas 1 en RSTP

Dans les deux cas le flux utilise le même chemin s'il n'y a aucune panne, cela signifie deux remarques importantes :

- Le flux est soumis aux mêmes pannes dans l'une ou l'autre des ingénieries. Plus précisément les deux ingénieries disposent de la même disponibilité sur le chemin principal car il est identique.
- L'ingénierie MVPN présente un intérêt car la situation n'est pas défavorable. Elle devrait gérer correctement certaines doubles pannes que l'ingénierie RSTP ne peut pas gérer donc l'indisponibilité du système doit baisser.

Nous allons donc modéliser en RB les deux architectures de la Figure 42 afin de mettre en œuvre et de tester notre approche de modélisation sur les deux ingénieries. Nous allons nous appuyer sur des structures très proches lors de la construction pour n'oublier aucun cas particulier de fonctionnement ou de panne.

Sur la Figure 43 sont placés en haut les composants relatifs aux sources et en bas les composants relatifs à la destination. La partie encadrée concerne la boucle principale dans laquelle le comportement du protocole permet de déterminer si les routeurs A et B sont alimentés par le flux. On se sert ensuite de ces états pour savoir si le routeur D est alimenté. Vu que l'on travaille dans des boucles et que les RB sont acycliques, il est important de séparer le cas où le flux

provient d'un côté de la boucle, noté Ouest, de celui où il provient de l'autre côté, noté Est. Pour cela nous utilisons deux états indépendants : « A Alimenté via Ouest » et « A Alimenté via Est » qui seront agrégés dans le nœud « A Alimenté ». La même logique est conservée pour l'alimentation du routeur D.

Ensuite il faut intégrer le chemin nominal et le chemin secours et nous utilisons les caractéristiques multi-états des RB pour cela. Ainsi B est alimenté en situation nominale si B est alimenté par l'Est en situation nominale (c'est à dire pas de panne sur S1-B). On applique la même logique à la sous-boucle en considérant le chemin nominal en passant par le routeur B.

Enfin il faut modéliser le fait que la solution RSTP possède des cas de doubles pannes non gérés par l'ingénierie. Le nœud appelé « Routeur B isolé sans panne ssboucle » a été créé dans ce but et devient vrai lorsque B n'est plus alimenté et qu'il n'existe aucune panne dans la sous boucle. S'il est vrai, le routeur D ne recevra pas le flux. Le détail de chaque TPC se trouve en annexe 1.

La représentation graphique de l'ingénierie MVPN n'est pas très différente de la précédente et est décrite par la Figure 44. Toutefois il n'y a plus de nœud « Routeur B Isolé » car l'ingénierie MVPN est capable de gérer ce cas de double panne. Les probabilités conditionnelles changent également.

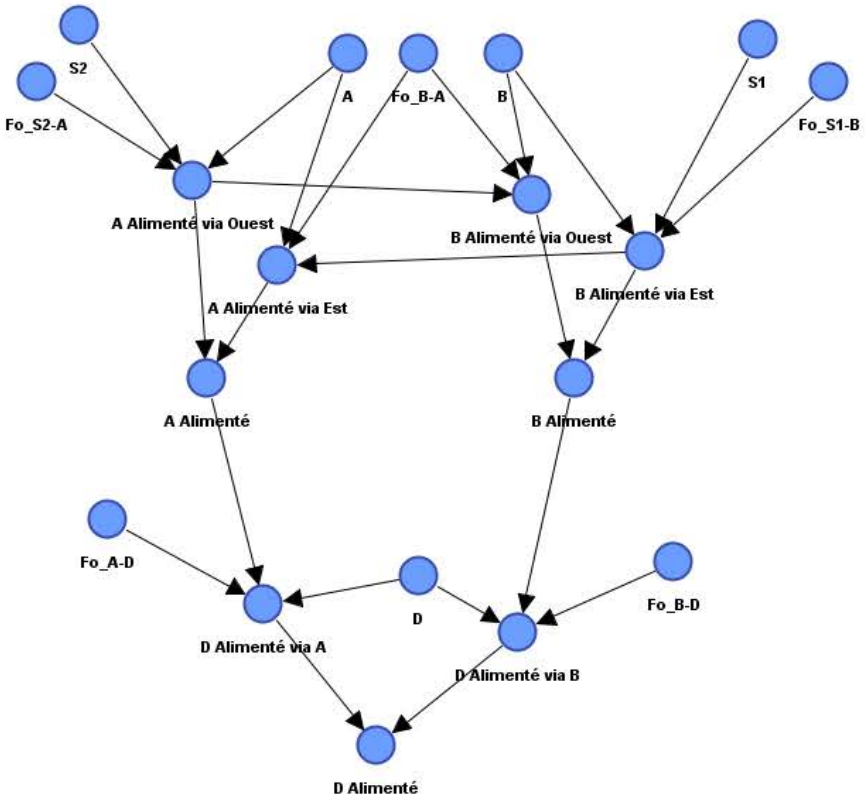


Figure 44 : Modélisation par RB du cas 1 en MVPN

Table 3 : Résultats de modélisation du cas 1 par RB

Situation	RSTP : disponibilité	MVPN : disponibilité	Delta en taux	Delta par année
Nominale	**0.99897028**	**0.99897028**	0	0
Secours	**0.00100895 (530.67 min)**	0.001019189	+0.000010239	+5.39 min (+1.0%)
Panne	0.000020770 (10.92 min)	**0.000010531**	-0.000010239	-5.39 min (-49.3%)

Les calculs réalisés sur les deux modèles donnent les résultats résumés dans la Table 3. On retrouve bien les deux remarques présentées précédemment à savoir que la probabilité de se trouver en situation nominale est identique pour les deux ingénieries et que la solution MVPN offre moins d'indisponibilité que la solution RSTP.

Les résultats montrent que le gain de disponibilité d'un peu plus de 5 minutes par an est obtenu par la seule augmentation de la durée en situation de secours. Ce résultat était prévisible d'un point de vue qualitatif car MVPN peut gérer certaines doubles pannes. En pourcentage, MVPN diminue l'indisponibilité de 50% mais augmente la durée en situation de secours de seulement 1%. Ce résultat met en évidence que le gain en disponibilité est significativement plus important que la contrepartie qui est l'augmentation de la probabilité d'être en situation de secours.

Cette première étude permet de confirmer qu'il est possible de modéliser par RB le comportement des ingénieries et d'utiliser ces modèles pour les comparer objectivement sur la base de la disponibilité tout en analysant la conséquence sur la probabilité d'être en situation de secours qui modélise la probabilité de reroutage.

3.2.3.2. Cas Simple 2

Il est facile de voir dans un cas très simple comme celui précédemment étudié quelle ingénierie est la plus performante. Cette simplicité provient du fait que le chemin nominal est identique pour les deux solutions. Ainsi la solution MVPN offre de la résilience supplémentaire sans contrepartie.

Nous allons nous intéresser à un nouveau cas simple pour mettre en évidence le cas d'un chemin nominal différent entre les deux ingénieries. La topologie et les chemins sont illustrés sur la Figure 45.

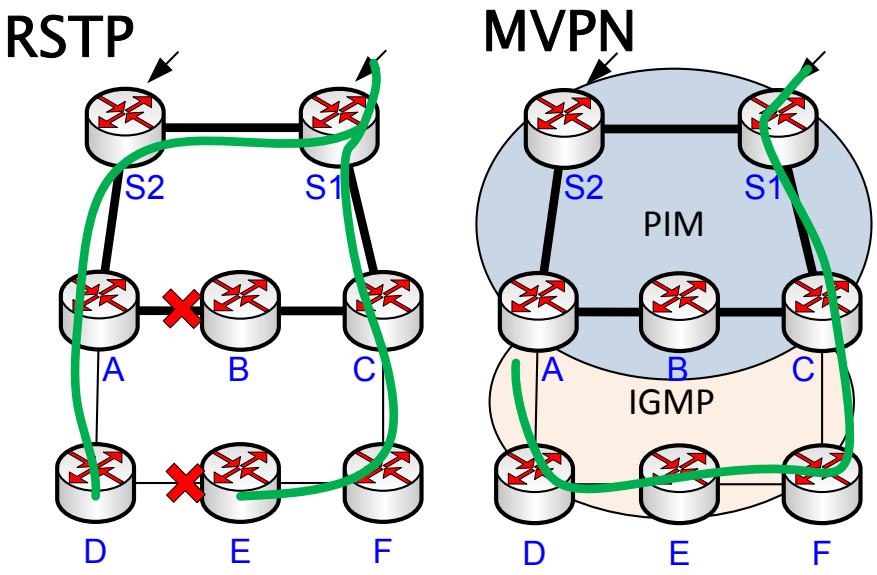


Figure 45 : Cas simple 2

Dans ce cas simple nous avons deux chemins différents pour diffuser sur RSTP et MVPN. Dans la solution RSTP les points de coupures ont été placés le plus loin possible de la source S1 si bien que le routeur D se trouve alimenté par la partie Ouest de la boucle principale et de la sous-boucle. Par contre dans l'ingénierie MVPN, les routeurs de la sous-boucle ne sont pas capables de faire du VPRN et doivent donc utiliser les techniques VPLS pour transporter le flux. Le constat direct est que soit le routeur C ou soit le routeur A doit jouer le rôle de diffuseur principal pour ce VPLS. Le routeur père C est choisi comme routeur père car il est plus proche de la source S1. Mais dans ce cas tout le VPLS se retrouve alimenté en situation nominale par le routeur C ce qui fragilise le transport en situation nominale pour le routeur D. En effet ce dernier doit utiliser quatre liaisons pour joindre la source en MVPN alors qu'il était possible de passer par la partie Ouest en RSTP avec seulement trois liaisons traversées.

Ce choix fait lors de la conception satisfait le plus grand nombre de destinations car on peut envisager que les routeurs E et F soient aussi des destinations pour ces flux multicast. Ainsi le routeur D se retrouve en situation défavorable et nous allons tout particulièrement nous concentrer sur ce routeur. La représentation graphique du RB utilisé comme modèle est présenté dans la Figure 46.

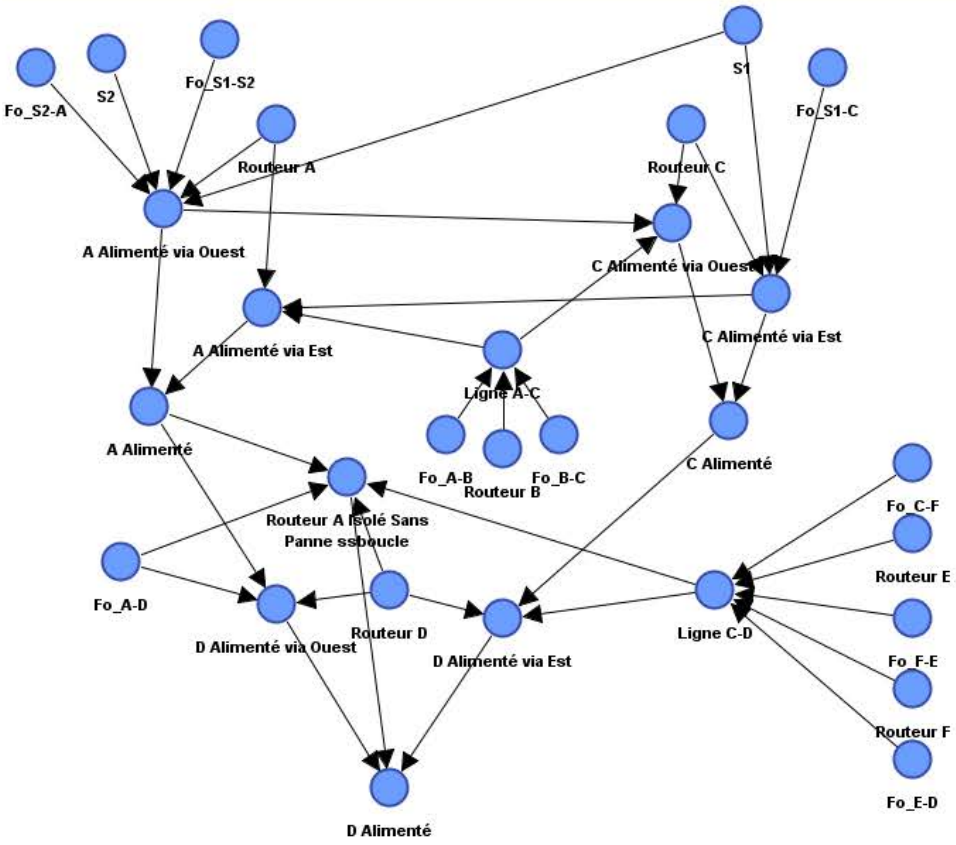


Figure 46 : Modélisation par RB du cas 2 en RSTP

Tout comme pour le cas précédent on retrouve dans la partie haute les sources et en bas la destination, en l'occurrence le routeur D. C'est la disponibilité du flux arrivant à ce routeur qui doit être calculée. On introduit dans ce schéma la notion de « ligne » qui sera utilisée dans les plus grands RB pour agréger les états des différents nœuds en un seul pour simplifier le remplissage des tables de probabilités conditionnelles. Par exemple sur la droite la « Ligne C-D » est Ok si tous ses composants sont Ok, ce qui simplifie le renseignement des nœuds « D Alimenté via Est » et « Routeur A Isolé Sans Panne ssboucle ». Pour le reste tout est identique au premier cas car la topologie ne change pas, on ajoute seulement quelques routeurs dans les boucles.

Table 4 : Résultats de modélisation du cas 2 par RB

Situation	RSTP : disponibilité	MVPN : disponibilité	Delta en taux	Delta par année
Nominal	**0.99846081**	0.9979516	-0.00050921	-267.8 min
Secours	**0.00151765 (798.2 min)**	0.002037348	+0.000519698	+273.3 min (+34.2%)
Panne	0.000021539 (11.3 min)	**0.000011051**	-0.000010488	-5.5 min (+48.7%)

La Table 4 présente les résultats des modèles RSTP et MVPN pour le cas 2. Il apparait notamment le gain en disponibilité de l'ingénierie MVPN qui est du même ordre que dans le cas 1. Mais en revanche il y a cette fois une nette baisse de la probabilité de se trouver en situation nominale. On gagne environ 5 minutes de disponibilité mais en augmentant les situations de reroutages de près de 4h35. Cela pose la question de l'apport réel de la nouvelle ingénierie compte tenu de cette augmentation de la probabilité de se retrouver en situation de secours et donc de l'accroissement du nombre de reroutages qui provoque des impacts à l'image. En pourcentage l'ingénierie MVPN apporte un gain de 48.7% sur l'indisponibilité alors qu'elle augmente les situations de reroutages de 34.2%.

Finalement, ce cas défavorable montre bien que la modélisation par RB est pertinente pour évaluer conjointement le taux de disponibilité et l'impact du reroutage. Les cas modélisés sont certes simplistes, mais ils permettent d'obtenir des résultats quantitatifs analysables et logiques. Ils confortent le choix des RB comme outil de modélisation de la disponibilité d'un service sur un réseau de diffusion audiovisuel. Il faut maintenant modéliser un cas concret pour vérifier que le modèle s'adapte au réseau de TDF et obtenir de premiers résultats pour aider à la décision.

3.2.3.3. Cas réel avec une seule destination

Le cas réel est naturellement extrait du réseau TMS et en particulier de la distribution du multiplexe R5 dans la boucle Sud-Ouest. Bien que la diffusion soit liée à la topologie nationale nous allons simplifier en se focalisant uniquement sur une boucle jugée suffisamment représentative.

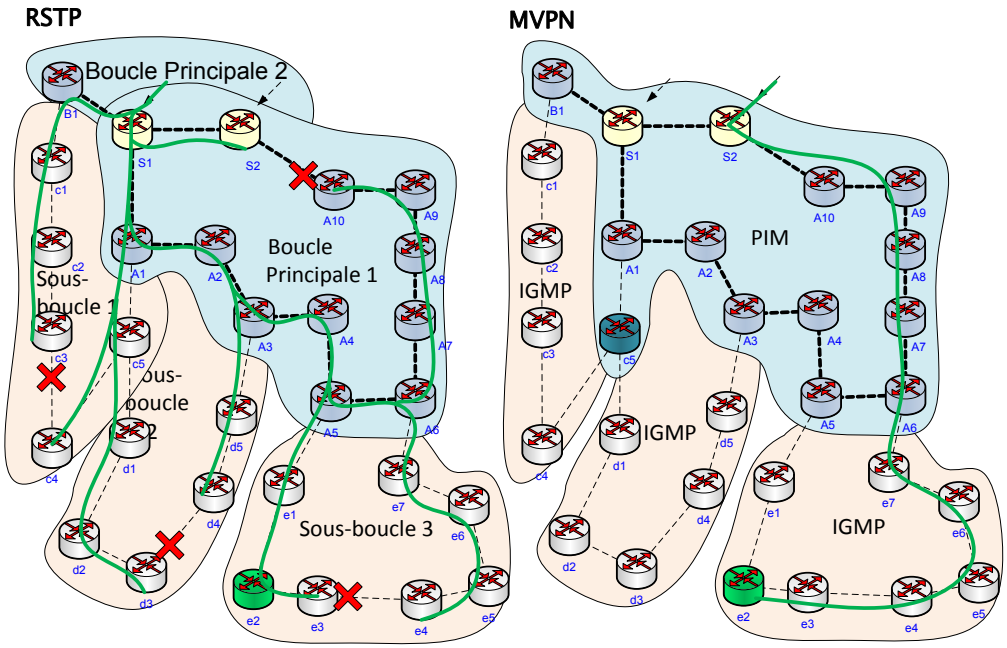


Figure 47 : Topologie étudiée pour le cas réel, pour les deux solutions

La topologie et les chemins des flux pour chacune des ingénieries sont présentés sur la Figure 47. On retrouve les deux têtes de réseau S1 et S2 en haut de la boucle principale 1 et trois sous-boucles dont une indépendante contenant la destination e2. C'est la disponibilité du service à e2 que la modélisation par RB va permettre de calculer. Les sous-boucles 1 et 2 sont dépendantes car le routeur c5 de la sous-boucle 1 est l'un des routeurs pères de la sous-boucle 2. La sous-boucle 1 dépend d'une autre boucle principale c'est pourquoi la boucle principale 2 est partiellement représentée dans les deux ingénieries.

Dans l'ingénierie RSTP on note quatre coupures spanning tree à travers les quatre boucles. Celle de la boucle principale se trouve entre le routeur S2 et A10 car il s'agit d'une liaison à grande distance fréquemment en panne et historiquement il a été choisi de localiser la coupure RSTP à cet endroit. Pour les autres boucles la coupure RSTP est placée au milieu de la topologie afin que la moitié des routeurs soient alimentés par l'Ouest et l'autre par l'Est. Le flux est ensuite diffusé dans toute la topologie en provenant de S1.

Au niveau de la solution MVPN on note un changement de routeur par rapport à la solution RSTP. En effet le routeur c5 qui se trouvait à la frontière des deux sous-boucles 1 et 2 a été changé pour permettre d'utiliser la technologie VPRN. Ainsi ce routeur sera un routeur père pour la sous-boucle 1 et la sous-boucle 2. Vu que la diffusion ne concerne que le routeur e2, l'arbre multicast créé emprunte uniquement un chemin qui passe par l'Est contrairement à l'ingénierie RSTP qui passe par l'Ouest. De plus pour la sous-boucle contenant le routeur destination on change de diffuseur par rapport à RSTP et l'on passe dans une situation défavorable car e2 est plus éloigné d'A6 que d'A5. On se retrouve alors dans une situation proche du cas simple 2 mais avec beaucoup plus de constituants pour le réseau. La topologie du RB utilisé est présentée en Figure 48 et détaillée en annexe 2.

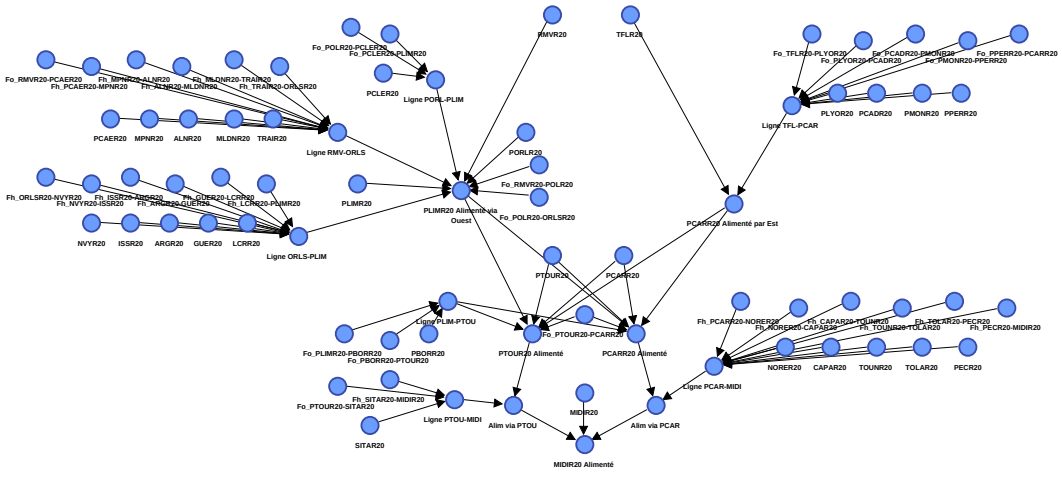


Figure 48 : Représentation par RB du cas réel pour la solution MVPN

Table 5 : Résultats de modélisation du cas réel par RB

Situation	RSTP : disponibilité	MVPN : disponibilité	Delta en taux	Delta par année
Nominal	**0.996824298**	0.996784525	-0.000039773	-20.9 min
Secours	**0.003157427 (27.7h)**	0.003202403	+0.000044976	+23.7 min (+1.4%)
Panne	0.000018276 (9.6 min)	**0.000013072**	-0.000005204	-2.7 min (-28.5%)

Structurellement on retrouve en haut les sources et la destination en bas. Les « grappes » de nœuds représentent des lignes pour agréger les états de plusieurs nœuds. Sinon la même logique que précédemment est appliquée : on cherche à savoir si un routeur père est alimenté ou non et on effectue ce résonnement dans la sous-boucle concernée.

Les résultats des calculs effectués grâce à cette modélisation sont résumés dans la Table 5. On observe des résultats intéressants comme le fait que l'ingénierie MVPN ne fait baisser l'indisponibilité que de 2,7 minutes par an et qu'elle fait augmenter la durée des situations reroutées de 23,7 minutes par an. Pour apprécier le gain de la solution MVPN par rapport à RSTP, il ne faut pas analyser les valeurs en absolu mais en relatif. Ainsi on gagne bien 28,5% de disponibilité pour une augmentation en situation reroutée de seulement 1,4%.

Maintenant que l'on a prouvé le bon fonctionnement du raisonnement sur une topologie réelle il faut s'intéresser à modéliser plusieurs points de service pour montrer que les RB supportent le passage à l'échelle. Pour cela nous allons appliquer cette modélisation à un cas réel basé sur la même topologie mais en examinant simultanément la disponibilité à plusieurs points de service.

3.2.3.4. Cas réel multi-destinations

Pour la suite de l'étude, on s'intéresse à la livraison de six destinations placées dans différentes boucles (cf routeurs verts de la Figure 49). Ce choix de six destinations est arbitraire pour montrer la faisabilité de la modélisation. Le fonctionnement est le même que présenté précédemment mais il faut préciser ici que pour l'ingénierie MVPN on utilise un routeur père principal de la sous-boucle 2 : le routeur c5.

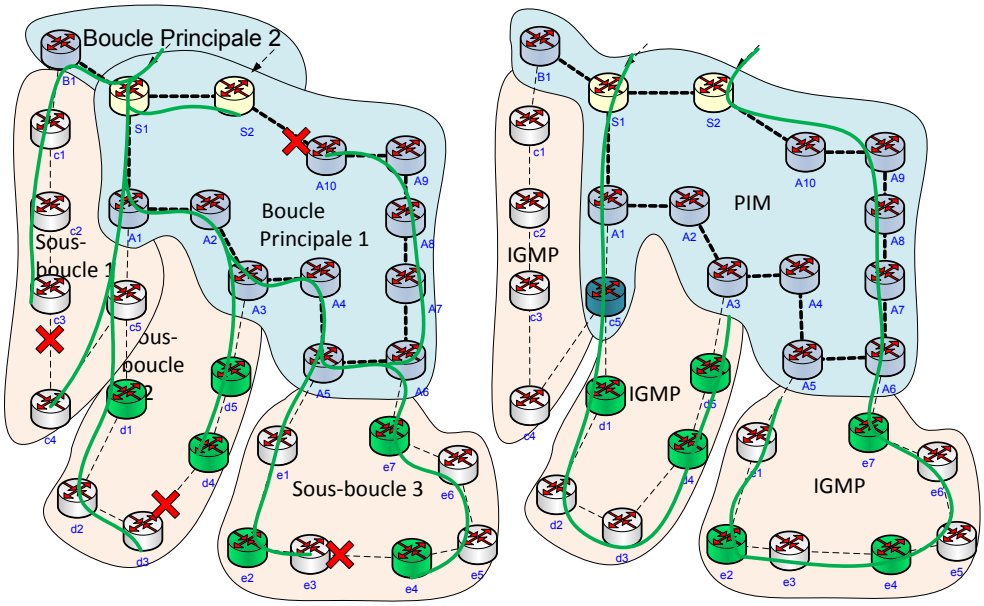


Figure 49 : Topologie du cas réel qui délivre le flux en plusieurs points

Dans la solution MVPN, les destinations étant placées dans différentes boucles, il est possible que les sources soient différentes pour chacune des destinations. On s'intéresse à plusieurs destinations, notre modèle est construit sur un nœud appelé « Système Ok » agrégeant l'état de fonctionnement des six nœuds destination et présenté en annexe 3. Ici le système est en fonctionnement nominal si toutes les destinations sont alimentées en chemin nominal. Si une ou plusieurs destinations obtiennent le flux en situation de secours alors le système est en état secours s'il n'y a aucune panne. Enfin si un ou plusieurs points de service ne reçoivent pas le flux alors le système est en état de panne. La Table 6 résume les résultats de modélisation.

On constate à nouveau le gain apporté par l'ingénierie MVPN cependant ces résultats diffèrent de l'attendu. Dans la situation de secours nous nous attendions à avoir une dégradation modérée et pour la situation de panne nous espérions une amélioration plus significative. Cette situation s'explique aisément par le fait que la coupure spanning tree n'a pas été placée de manière optimale pour le nœud d4 et on est donc en situation défavorable pour l'ingénierie RSTP lorsqu'il n'y a pas de panne.

Table 6 : Résultats de modélisation du cas réel par RB sur plusieurs points de service

Situation	RSTP : disponibilité	MVPN : disponibilité	Delta en taux	Delta par année
Nominal	0.995651019	**0.99785806**	0.002207042	+19.3h
Secours	0.004281791	**0.00207604**	-0.002205751	-19.3h (-51.5%)
Panne	0.000067191	**0.0000659**	0.000001291	-41s (-1.9%)

On rappelle que la logique de placement consiste à positionner la coupure spanning tree au milieu de la sous-boucle afin que la moitié des destinations de la sous-boucle soient alimentées par un routeur père et l'autre moitié par un autre routeur père. Cette logique découpe la sous-boucle en deux sous-ensembles équilibrés afin que seule la moitié d'une sous-boucle soit impactée par une panne en amont. Néanmoins cela ne permet pas un fonctionnement optimal par rapport à la distribution de la source à travers le réseau. En effet pour rejoindre la source, le routeur d4 utilise le chemin d4-d5-A3-A2-A1-S1 qui est un chemin avec moins de disponibilité que le chemin d4-d3-d2-d1-c5-A1-S1. Cette différence provient du fait que la disponibilité des faisceaux hertziens utilisés dans la sous-boucle soit meilleure que la disponibilité de la fibre optique louée sur la boucle principale. Il aurait ainsi été plus efficace de placer la coupure RSTP entre d4 et d5 pour améliorer la disponibilité globale du système étudié.

Cette analyse du cas réel multi-destinations permet avant tout de montrer qu'il est possible d'estimer simultanément la disponibilité de plusieurs points de service. Par la modélisation de ce cas réel et l'obtention de résultats cohérents, on démontre la pertinence de l'utilisation des RB pour la modélisation d'un service audiovisuel à distribution nationale.

Ces modèles permettent de conforter le choix d'évolution du réseau vers cette nouvelle ingénierie en montrant des résultats satisfaisants. Mais cette modélisation est une vue probabiliste qui n'intègre pas la dynamique de fonctionnement des protocoles et donc les temps de détection de panne et de convergence ne sont pas pris en compte. Ainsi nous allons utiliser une autre approche d'analyse de la disponibilité en utilisant un simulateur.

3.3.Simulation sous Modeler

3.3.1. Introduction à l'utilisation de Modeler

Avant d'entrer dans le détail de nos modèles représentés sous Modeler, il est important de se rappeler que toute simulation possède ses limites. Malgré un comportement proche de la réalité, les simulations peuvent ne pas retranscrire exactement le fonctionnement d'un réseau [47]. De plus notre étude concerne des réseaux très fiables ce qui complique l'analyse des résultats obtenus par simulation et nécessiterait des approches particulières comme l'utilisation de méthodes de Monte-Carlo. Cependant, d'après des travaux sur les réseaux hautement fiables [48], l'utilisation de cette méthode n'est pas indispensable pour notre étude et nous ferons cette approximation pour simplifier toutes les simulations sous Modeler.

Modeler est un logiciel issu du commerce qui permet la simulation de réseaux en intégrant de nombreuses bibliothèques mises à disposition par les équipementiers et des entreprises spécialisées. Ce logiciel intègre des profils de simulations complets qui permettent selon le besoin d'intégrer toutes les

problématiques réseau [49-52]. On peut ainsi vérifier le comportement de protocoles dans certaines situations et recopier entièrement le comportement d'un réseau.

Modeler est très répandu et bénéficie d'un important retour d'expériences. Il présente donc des garanties de fiabilité des résultats de simulation que n'offrent pas toujours les autres simulateurs. Pour mener à bien ces travaux de simulation, j'ai encadré le stage de recherche d'un étudiant en Master 2, Benoit Hingray [53].

Pour simuler le fonctionnement du réseau dans notre cas nous allons faire deux simplifications importantes mais sans impact significatif sur le comportement du réseau réel :

- Afin de simplifier au maximum et ne pas monopoliser de la ressource inutilement, nous n'allons pas modéliser une pile protocolaire IP/MPLS pour nos modèles mais simplement reproduire un comportement niveau 2 approchant le fonctionnement des services techniques. Cela signifie que nous n'utiliserons pas des services MPLS et donc que notre flux simulé ne sera pas cloisonné. Cette approximation impacte peu la réalité dans la mesure où, d'un point de vue temporel, le traitement par MPLS d'un routeur est de l'ordre de la dizaine de microsecondes.
- La seconde proposition concerne les profils de pannes. Pour cela nous allons utiliser les notions de MTBF (Mean Time Between Failure), MTTR (Mean Time To Repair) et MTTF (Mean Time To Failure) utilisées en sûreté de fonctionnement pour définir la disponibilité. Un module intégré à Modeler permet d'interpréter ces données pour aléatoirement provoquer des pannes représentatives de la disponibilité prévue, suivant une loi et une moyenne à choisir.

En sûreté de fonctionnement le MTBF et la disponibilité sont définis par :

$$MTBF = MTTF + MTTR$$

$$Disponibilité = \frac{MTTF}{MTBF} = \frac{MTBF - MTTR}{MTBF}$$

Ces définitions vont nous permettre de définir les paramètres de simulation que nous allons utiliser. Nous allons limiter notre simulation sur une durée de 60 jours. Afin de calculer correctement les valeurs ci-dessus, il faut fixer le MTBF pour qu'il soit représentatif. Dans cette étude nous proposons une moyenne de deux pannes par équipement sur la durée du test, c'est-à-dire un MTBF de 2592000 secondes (30 jours). Le MTTR peut être calculé en fonction de la disponibilité définie, selon le MTBF. Choisir un MTBF identique pour différents taux de disponibilité est discutable, mais ce choix est réalisé faute d'avoir un critère de répartition réaliste.

$$MTTR = MTBF\ (1 - Disponibilité)$$

Table 7 : Définition des MTFB et MTTR pour nos simulations sous Modeler

Equipement	Disponibilité	MTBF (en s)	MTTR (en s)
Routeur	10^{-5}	2592000	26
Fibre Optique	$5.\ 10^{-5}$	2592000	1296
Faisceau Hertzien	10^{-4}	2592000	259

La Table 7 montre pour 60 jours les MTBF et MTTR utilisés dans le cadre de nos simulations sur Modeler. A noter une difficulté importante pour l'exploitation des résultats qui sont restitués sous la forme de courbes telles que présentées Figure 50. Modeler ne dispose pas d'un outil d'analyse restituant directement le temps de panne. Pour obtenir les disponibilités associées, nous devons exploiter un fichier csv contenant ces résultats et l'analyser.

L'approche par simulation apporte aussi la possibilité de mesurer les phénomènes de bascules qu'il n'était pas possible de représenter avec les RB. Ces mécanismes propres à la convergence des protocoles ajoutent au temps de panne le temps de détection de la panne et le temps de cicatrisation du réseau. Les simulations sous Modeler nous permettent de mesurer directement le temps où le flux n'arrive plus à la destination tel que présenté dans la Figure 50.

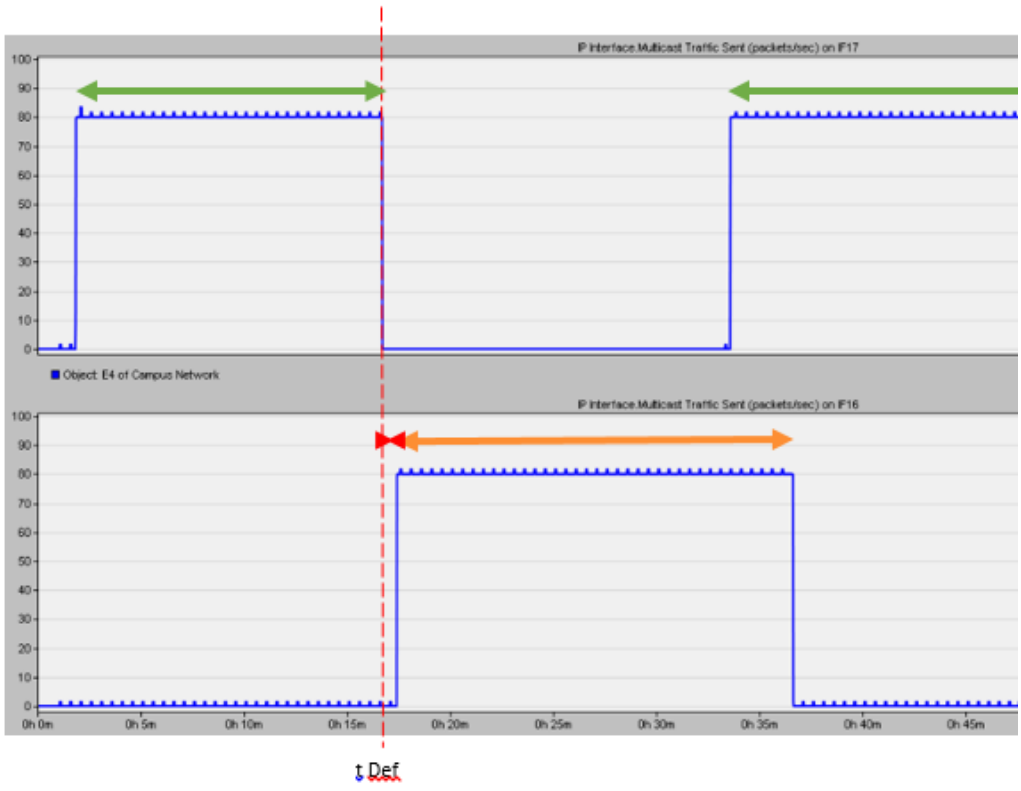


Figure 50 : Illustration de la mesure graphique du phénomène de bascule sur Modeler

Il y a deux objectifs majeurs pour notre approche par simulation :

- Simuler le comportement du réseau pour conforter l'approche utilisée dans les RB : il s'agit de valider la démarche utilisée en RB.
- Analyser le comportement des basculements qui ont été ignorés dans les RB et voir leur influence sur les performances annoncées par le RB : nous souhaitons mesurer les temps de basculements.

Dans les parties suivantes nous allons revenir au cas simple présenté pour la modélisation par RB pour comparer les résultats obtenus par simulation aux résultats observés en RB. Nous modéliserons ensuite le cas réel.

3.3.2. Cas simple

Dans un premier temps nous allons étudier le cas simple 1 présenté précédemment et analysé en RB. La Figure 51 montre la représentation graphique du réseau par l'outil pour la solution RSTP. Le PC nommé « Envoyeur » est paramétré pour envoyer un flux multicast à travers le réseau, le PC nommé « Receveur » est chargé de le récupérer. Ces équipements sont directement connectés à des hubs pour à la fois répartir le flux sur les deux têtes de réseau et servir d'outils de métrologie. On retrouve ensuite sur la gauche trois contraintes de simulation qui vont venir modifier la simulation pour envoyer un flux multicast et provoquer des pannes ou les réparer en suivant les MTBF et MTTR que l'on va renseigner.

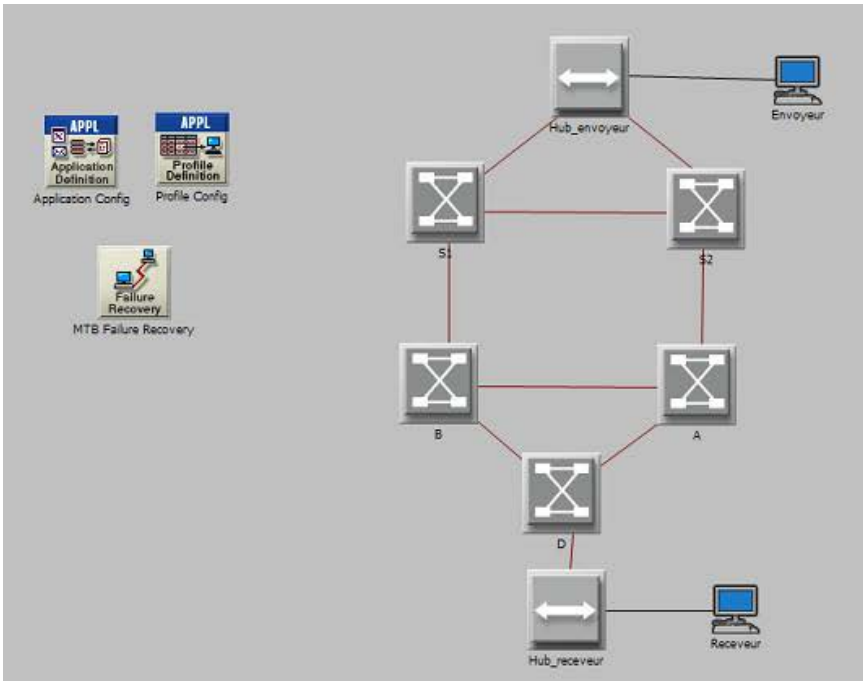


Figure 51 : Représentation sous Modeler du cas simple 1 en RSTP

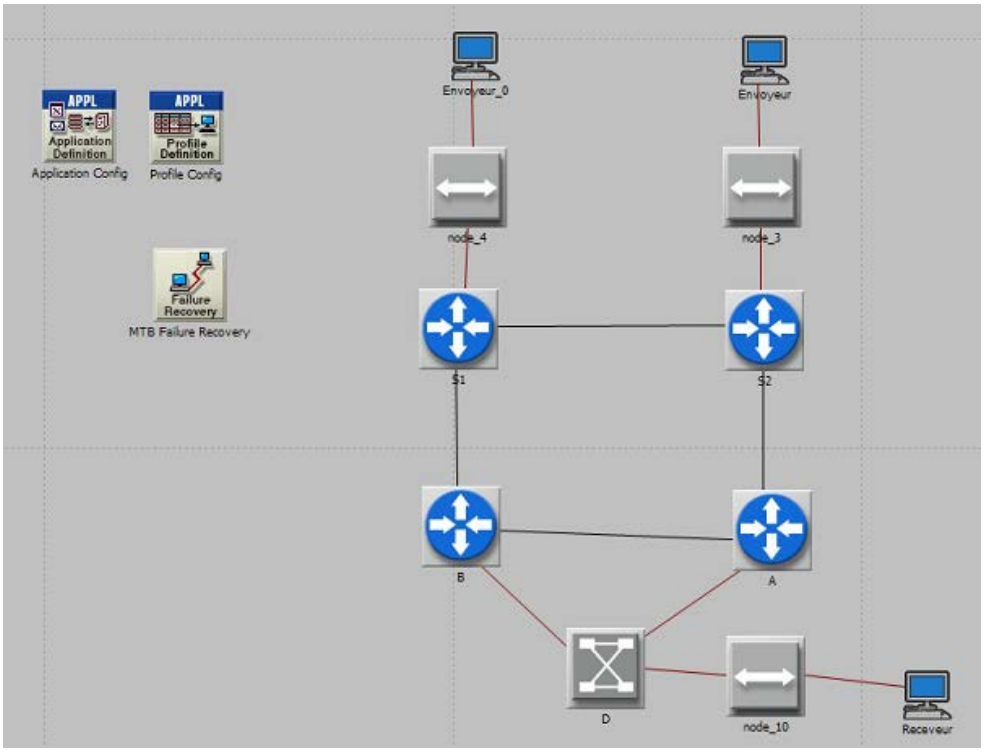


Figure 52 : Représentation sous Modeler du cas simple 1 en MVPN

Pour la solution MVPN il s'agit de la même base mais on remplace les quatre switchs en haut du schéma par des routeurs qui utilisent le protocole PIM tel que présenté dans la Figure 52. Nous faisons aussi une duplication de sources afin de mieux gérer les sources et d'éviter un traitement de priorités en amont de la diffusion dans le réseau.

Au niveau des résultats de simulation on obtient les données rassemblées dans la Table 8. Ces mesures sont des conversions des temps passés dans chaque état. Ces données sont cohérentes pour RSTP par le fait qu'elles retranscrivent les mêmes ordres de grandeur entre les deux modèles RB et Modeler. Par contre pour MVPN, le modèle ne passe jamais en situation de secours. Nous sommes confrontés à un problème d'implémentation dans lequel les durées des pannes restent toujours petites par rapport à la moyenne des MTTR programmés et restent systématiquement inférieures aux durées de détection par les protocoles. Cela explique pourquoi les protocoles n'ont pas le temps de converger et donc pourquoi le modèle ne passe jamais en situation de secours.

Table 8 : Comparaison des résultats du cas simple entre RB et Modeler

Solution	RSTP (RB) : disponibilité	MVPN (RB) : disponibilité	RSTP (Modeler) : disponibilité	MVPN (Modeler) : disponibilité
Nominal	0.99897028	0.99897028	0.998100	0.99833
Secours	**0.00100895**	0.001019189	0.001520 **(+50.7%)**	0
Panne	0.000020770	**0.000010531**	0.0000463 **(+123%)**	0.00167

Il aurait été intéressant de pouvoir modéliser sous Modeler RSTP et MVPN tout comme dans les modèles RB. Le problème d'implémentation de MVPN rend impossible cette comparaison et nous oblige à changer de démarche d'étude. Cela signifie aussi qu'il va être impossible de mesurer de manière directe le temps de basculement en situation de secours de la manière présentée en 3.3.1. Néanmoins nous allons continuer à modéliser sous Modeler les modèles en RSTP pour permettre de valider l'utilisation des RB comme outil de mesure de la disponibilité.

3.3.3. Cas réel

La modélisation du cas réel permet aussi de comparer les performances avec les résultats obtenus par RB.

Malheureusement cette représentation en Figure 53 est trop complexe par rapport aux recommandations des équipementiers. En effet la norme RSTP demande d'éviter d'utiliser plus de 20 nœuds dans une même topologie. Dans la vraie topologie de TMS, on s'appuie sur MPLS pour utiliser différentes instances de RSTP ce qui ne pose pas de problème d'implémentation. Ici du fait de l'approximation on dépasse la recommandation et on va devoir utiliser une autre topologie physique telle que présentée en Figure 54.

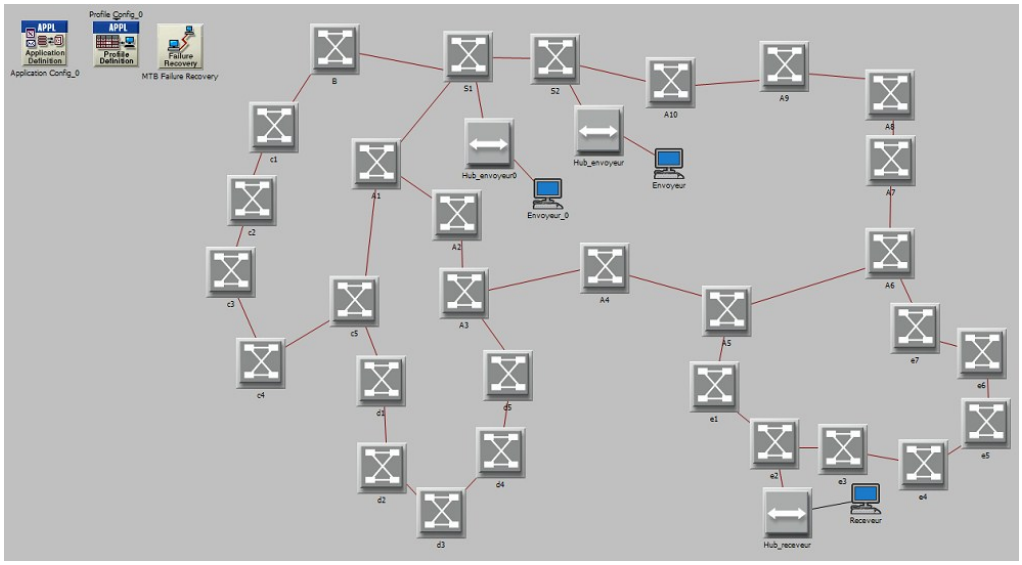


Figure 53 : Représentation du cas réel sous Modeler en RSTP

Le principe est de supprimer des éléments lorsqu'ils sont placés en série pour simplifier la topologie. On va ensuite agir sur les disponibilités des liaisons et des équipements pour tenir compte des switchs supprimés suivant la formule suivante :

$$Dispo_{x\ FH+(x-1)\ routeurs} = (Dispo_{\ FH})^{x} * (Dispo_{\ Routeur})^{x-1}$$

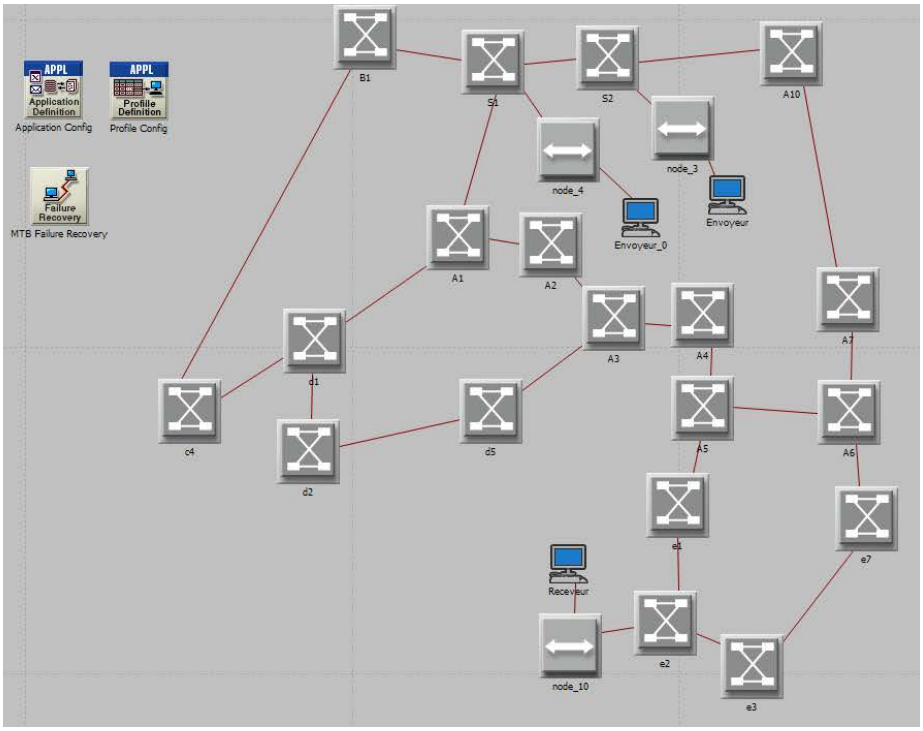


Figure 54 : Simplification sous Modeler du cas réel

Table 9 : Comparaison des résultats du cas réel entre RB et Modeler

Solution	RSTP (RB) : disponibilité	RSTP (Modeler) : disponibilité	Delta
Nominal	0.996824298	0.9993171	+0.002492802
Secours	0.003157427 (27.7h)	0.0002469 (2.16h)	-0.002910527 (-92.2%)
Panne	0.000018276 (9.6 min)	0.0004360 (3.82h)	+0.000417724 (+2186%)

Cela nous permet d'obtenir les résultats de la Table 9. On observe des résultats dans des ordres de grandeurs différents, ne favorisant pas la situation de secours telle que présentée dans les RB. Le résultat le plus important est la nette augmentation de l'indisponibilité mesurée par simulation qui augmente de près de 22 fois. Cette différence de mesure avec les RB provient vraisemblablement des phénomènes de basculement entre la situation nominale et la situation de secours.

Ce cas réel montre la difficulté de modélisation pour un passage à l'échelle de la simulation et nous avons été contraints d'utiliser des approximations pour simuler le comportement du réseau. Nous observons alors des résultats dans des proportions différentes des RB dû aux phénomènes de basculements qui ne sont pas instantanés.

Les modèles étudiés sous Modeler mettent en avant les problèmes des simulateurs et des approximations nécessaires à leur fonctionnement. Parmi les deux objectifs initiaux qui étaient de valider les études RB et pouvoir mesurer les basculements, seul le premier a pu être mis en évidence. Cela provient notamment du fait de l'impossibilité de simuler sous Modeler l'ingénierie MVPN et de permettre une comparaison équivalente des deux solutions tout comme en RB. Nous obtenons néanmoins une confirmation de notre analyse de la disponibilité par RB tout en prenant en considération le phénomène de basculement existant.

Ce phénomène de basculement influençant beaucoup les services étudiés, nous avons souhaité trouver une solution offrant une situation plus optimale. Une nouvelle ingénierie est donc proposée dans ces travaux, constituant une seconde contribution qui est détaillée dans le chapitre suivant.

Chapitre 4

Proposition d'une nouvelle ingénierie

Chapitre 4 Proposition d'une nouvelle ingénierie 85

4.1. Limitations connues de la solution MVPN 86

4.2. Ingénierie MVPN+ 88

4.2.1. Présentation de la nouvelle ingénierie 88

4.2.2. Modélisation par RB 92

4.2.3. Emulation de la solution MVPN+ par MVPN+e 95

4.2.4. Simulation sous Modeler 96

4.2.5. Maquettage en laboratoire 97

4.2.6. Conclusion 101

4.1.Limitations connues de la solution MVPN

Aujourd'hui la solution MVPN apporte suffisamment de mécanismes de sécurisations au sens sûreté de fonctionnement et ce de manière autonome pour le réseau. Toutefois la solution est complexe à implémenter, et toutes les situations ne sont pas optimisées.

Pour plus de simplicité, nous représenterons dans la suite le service rendu au client et non la topologie physique utilisée. Pour rappel le flux est diffusé sur l'ensemble du réseau pour l'ingénierie RSTP alors que dans la solution MVPN un arbre est construit jusqu'au routeur père qui diffuse uniquement le flux dans son VPLS. Cela signifie qu'un seul routeur diffuse pour tout le VPLS et que certains membres peuvent se retrouver en situation moins favorable du point de vue sûreté de fonctionnement par rapport au RSTP.

Il n'existe pas aujourd'hui de solution d'ingénierie protocolaire sur l'infrastructure déployée qui permette d'optimiser la distribution du flux dans la partie VPLS. Le protocole PIM prolongé sur l'infrastructure VPLS permettrait cette optimisation. Par exemple sur la topologie présentée en Figure 55 l'utilisation de PIM provoquerait la diffusion des flux définis sur la Figure 56.

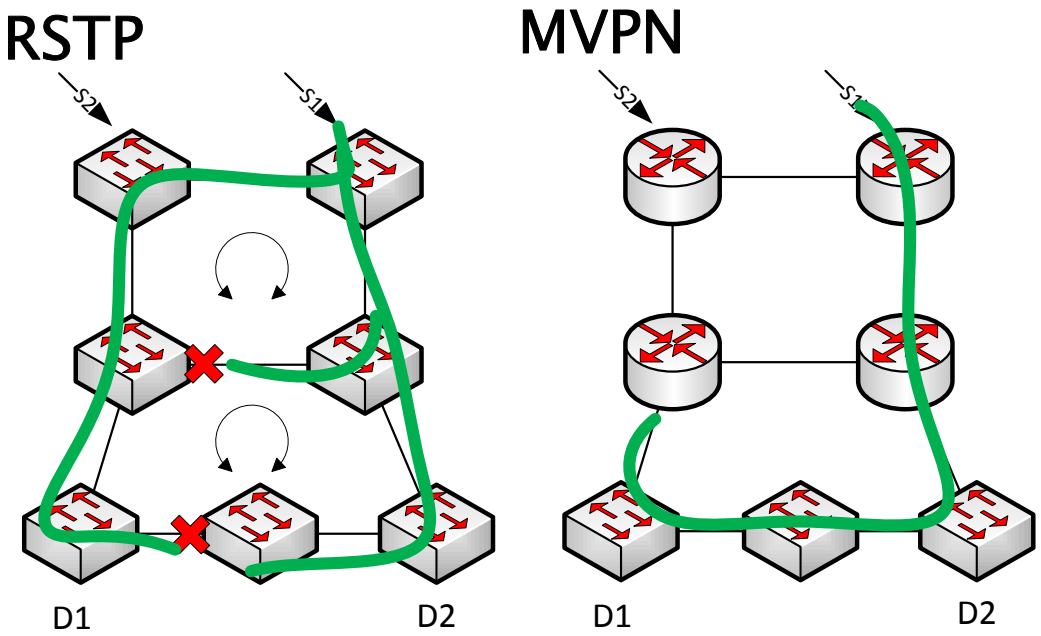


Figure 55 : Différence de diffusion vers D1 entre RSTP et MVPN

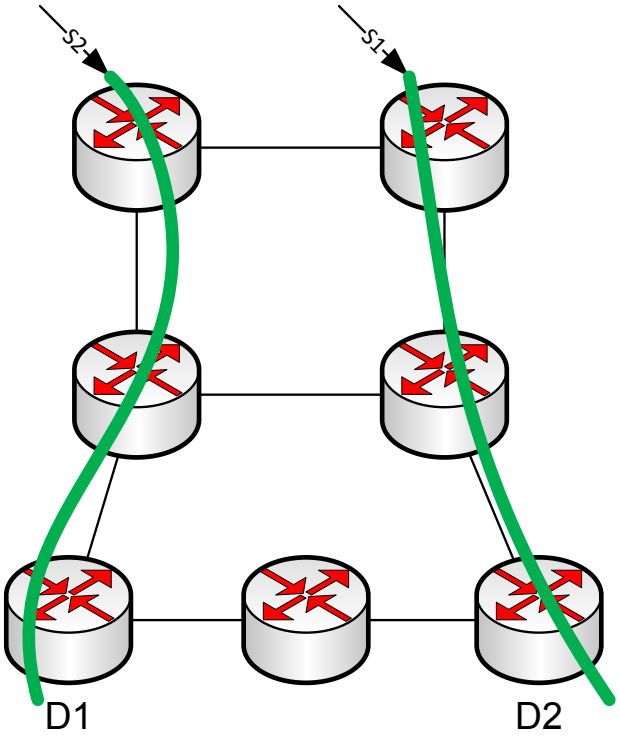


Figure 56 : Transport sur l'infrastructure en utilisant uniquement PIM

Cette logique serait la plus optimisée possible étant donné que l'algorithme de diffusion de PIM envoie le flux selon le chemin le plus court uniquement aux destinations qui demandent le flux (ici D1 et D2). Mais l'utilisation de PIM dans les VPRN contraindrait TDF à changer plus de 200 routeurs par des routeurs plus performants et significativement plus chers. Cet investissement ne pourrait pas être justifié par le seul gain en réduction d'impact qu'amène cette distribution suivant le chemin le plus court aux récipiendaires des multiplexes de la TNT.

Les équipementiers font constamment évoluer leurs produits de manière à ce que des « bugs » soient corrigés, mais aussi pour implémenter les dernières évolutions des protocoles. Dans ces évolutions il n'est pas rare de voir apparaitre des protocoles « propriétaires » qui par la suite peuvent suivre ou non le cycle de standardisation de l'IETF (Internet Engineering Task Force) et du MEF (Metro Ethernet Forum). Nous visons cette approche qui consiste à proposer une évolution de protocole en l'occurrence le protocole IGMP-Snooping pour approcher le comportement du protocole PIM. Ainsi on pourrait bénéficier de ses vertus mais sur la base des équipements de niveau 2 existants.

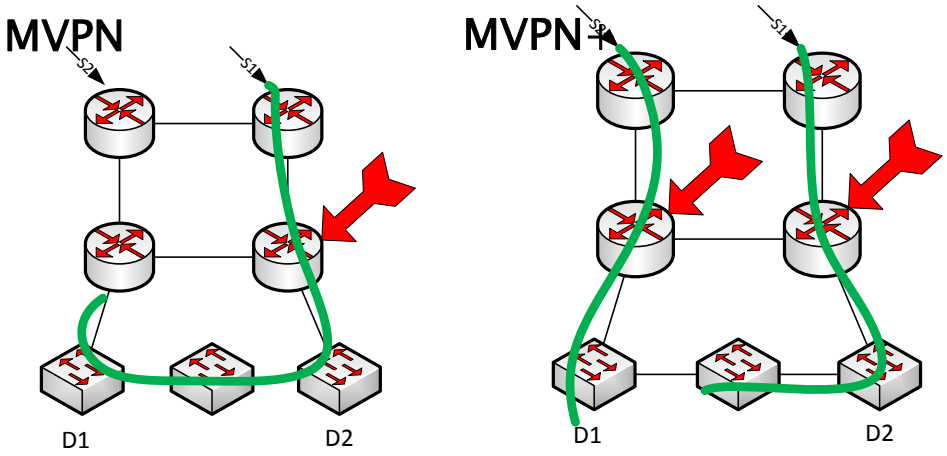


Figure 57 : Différence de diffusion dans le VPLS entre MVPN et MVPN+

4.2.Ingénierie MVPN+

4.2.1. Présentation de la nouvelle ingénierie

La démarche utilisée est de trouver une solution dans laquelle notre ingénierie de niveau 2 adopte un comportement similaire au protocole PIM. Comme le présente la Figure 57, le principal problème réside dans le fait que seul un routeur père diffuse le flux dans le VPLS alors qu'il existe plusieurs routeurs pères. Cette situation provient de la technologie PIM utilisée qui, pour éviter une double diffusion dans un même réseau local, possède un mécanisme d'élection de diffuseur principal. Tant que les deux VPRN peuvent s'échanger des informations à travers le VPLS pour savoir qui est diffuseur et qui est en attente, il ne peut y avoir qu'un seul diffuseur dans le VPLS. Trouver un moyen d'isoler les échanges PIM ne serait pas une solution viable, car deux flux seraient diffusés à travers le réseau ce qui doublerait la bande passante consommée mais surtout ce qui corromprait les flux multicast transportés.

Utilisée dans la solution MVPN, la technologie IGMP-Snooping autorise un switch à scruter les échanges IGMP entre les clients et les routeurs. Egalement embarquée dans les VPLS, elle est utilisée pour la construction de l'arbre multicast. Aujourd'hui ce protocole permet de suivre les échanges IGMP au sein d'un réseau local et offre au switch la possibilité de prendre des décisions d'aiguillage relatives aux messages surveillés. Le comportement sur un réseau local en multicast revient à ce que le client demande un flux multicast particulier avec un message en broadcast et que le routeur connecté au reste du réseau diffuse en broadcast le flux si un client le demande. Ainsi comme le montre la Figure 58 sans fonctionnalité IGMP-Snooping les demandes et flux sont diffusées dans tout le domaine alors qu'avec IGMP-Snooping les demandes et les flux sont uniquement envoyés aux clients concernés. Pour simplifier, sans IGMP-Snooping le client c1 reçoit le flux du client c2 et vice-versa.

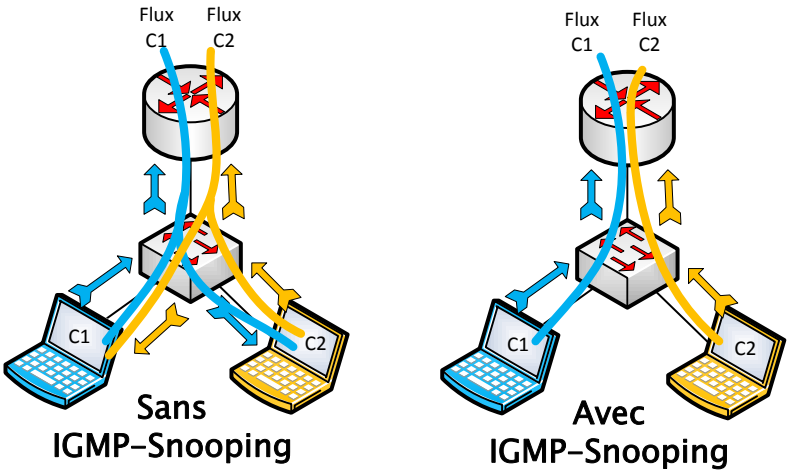


Figure 58 : Fonctionnement d'IGMP-Snooping dans un réseau local

En fait le switch IGMP-Snooping tient à jour en plus de sa table des adresses MAC une table propre à IGMP qu'il remplit en fonction des messages échangés. Par exemple lorsqu'il reçoit un message « General Query » qui est généré automatiquement par le routeur, le switch le note et indique dans sa table que le port 1, par exemple, est connecté au routeur. Cela signifie que toutes les demandes d'abonnement seront uniquement envoyées à ce port lorsqu'elles arrivent depuis un autre port. Lorsqu'un client envoie une demande d'abonnement, le switch note qu'un client sur le port 2, par exemple, demande tel ou tel multicast et lorsque le routeur enverra ce flux, le switch prendra la décision de le diffuser uniquement sur ce port.

Ce mécanisme offre sur de grands réseaux la possibilité d'éviter un gaspillage inutile de bande passante. Elle permet aussi d'éviter à un client de surveiller à quel contenu est abonné un autre client. Dans la solution MVPN on utilise IGMP-Snooping pour gérer les abonnements multicast. Ce ne sont pas les passerelles IP/ASI qui gèrent les abonnements mais les routeurs auxquels elles sont connectées. C'est un choix d'implémentation qui a été fait suite à des dysfonctionnements rencontrés sur les équipements d'extrémité.

Dans cette étude nous proposons une évolution d'IGMP-Snooping pour lui permettre de prendre des décisions différentes en fonction de paramètres additionnels transmis sur le réseau. Nous appellerons cette solution MVPN+.

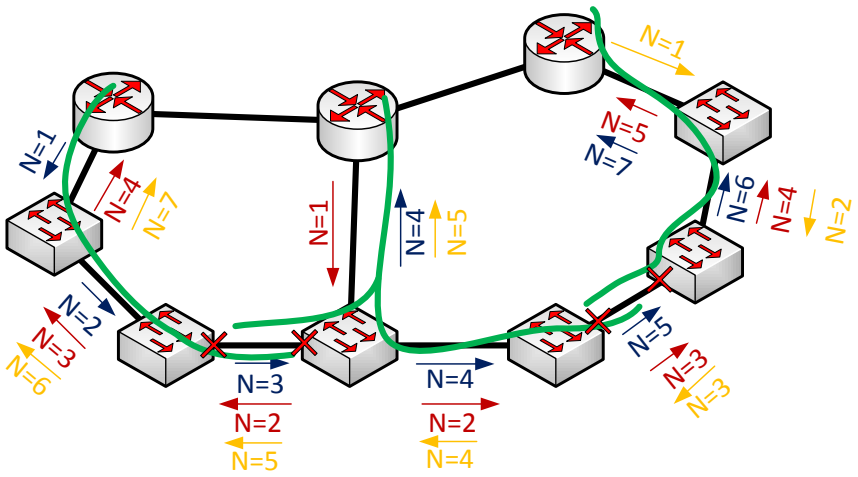


Figure 59 : Fonctionnement de MPVN+

Prenons pour illustration la Figure 59. Chaque routeur père va générer un paquet IGMP avec un champ optionnel appelé « Compteur » et qui aura pour valeur 1. A chaque passage dans un switch IGMP-Snooping, ce champ va être incrémenté de 1. Une fois tous les messages passés, après une temporisation adéquate, chaque switch regarde sur quelle interface il a reçu le message avec le champ « Compteur » le plus bas ; en cas d'égalité il choisit le port avec l'ID le plus bas. Le switch prendra alors la décision de bloquer tout multicast provenant des autres ports tant qu'il recevra du trafic multicast sur ce port. Dans cet exemple, les trois routeurs pères génèrent leur propre paquet IGMP avec le champ « Compteur » valant 1. Tous les messages transitent alors sur le réseau local en s'incrémentant dans chaque switch et permettant à chaque switch de prendre la décision optimale. On retrouve alors une diffusion impliquant les trois routeurs pères et des membres du VPLS allant chercher le routeur père le plus proche.

Il existe néanmoins deux principales limitations à cette nouvelle solution :

- La construction de l'arbre de diffusion est légèrement différente de PIM ce qui ne rend pas optimale cette nouvelle solution mais améliore l'existant.
- Pour que le mécanisme fonctionne il faut modifier le paquet au niveau IP et les switchs ne sont pas capables d'analyser un paquet avec une telle profondeur d'analyse, seules les adresses MAC sont traitées à leur niveau. Cela signifie que cette solution ne peut être directement implémentée.

Ce qui diffère légèrement sur la construction de l'arbre provient de la construction locale et non globale au réseau. En effet dans une solution globale PIM, chaque routeur cherche le chemin le plus court jusqu'à la source principale la plus proche alors que dans cette proposition la décision est uniquement locale, cloisonnée au sein du VPLS. Ainsi avec cette solution on n'aboutit pas à la situation idéale, mais on s'en rapproche par rapport à l'ingénierie MVPN.

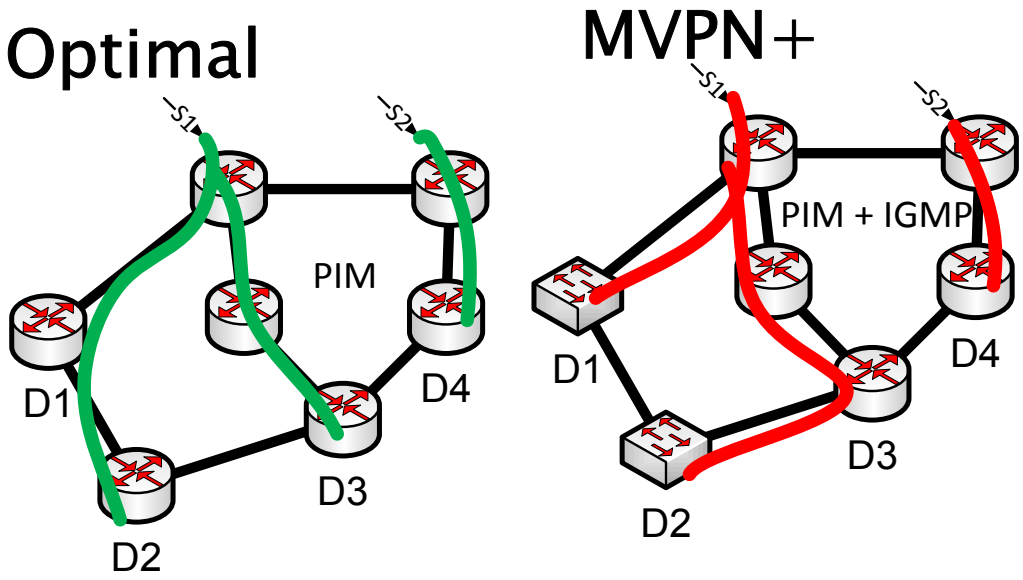


Figure 60 : Différence de diffusion entre solution optimale entièrement en PIM et MVPN+

L'exemple de la Figure 60 met en évidence la différence entre les chemins des flux crées par PIM et MVPN+. PIM construit un arbre optimal par rapport aux sources disponibles. Chaque destination construit le chemin le plus court jusqu'à l'une des deux sources principales. Avec MVPN+, chaque switch fait son choix localement et ainsi la destination D2 se retrouve alimentée par D3 ce qui finalement n'est pas le chemin le plus proche.

Le fonctionnement des switchs pour renseigner leurs tables IGMP-Snooping reste cantonné à l'analyse des trames Ethernet et cela pose problème pour l'implémentation de cette nouvelle solution. En effet il faudrait que le switch MVPN+ analyse la trame Ethernet jusqu'au niveau IGMP pour pouvoir prendre des décisions d'aiguillage.

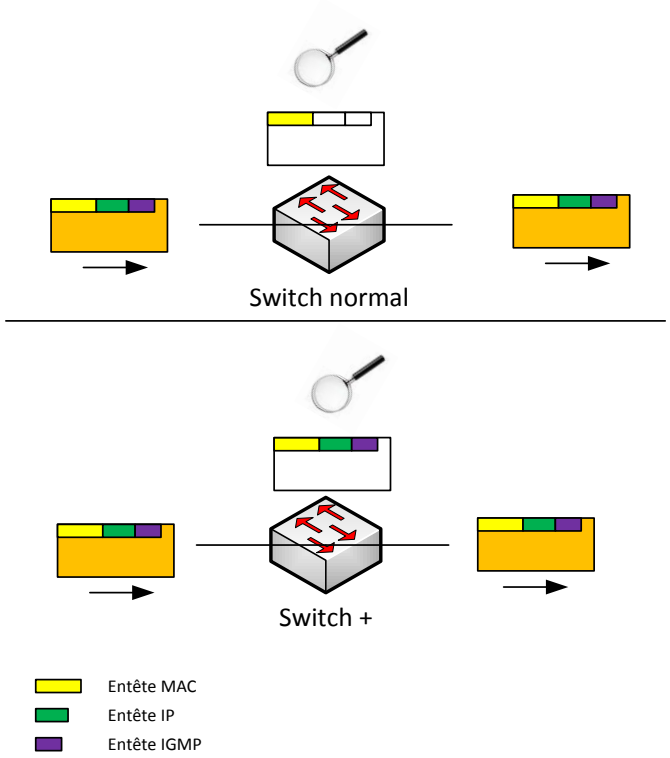


Figure 61 : Différences d'analyse des trames Ethernet par les switchs

Aussi lors de nos simulations et du maquettage nous ne pourrons reproduire exactement le comportement de MVPN+. Nous nous limiterons à un cas approchant cette solution pour modéliser et réaliser la maquette en laboratoire. Les paragraphes suivants concernent justement l'expérimentation de cette nouvelle ingénierie.

4.2.2. Modélisation par RB

Nous allons d'abord nous focaliser sur un cas extrêmement simple décrit sur la Figure 62 afin de constater de manière évidente l'apport de cette solution MVPN+.

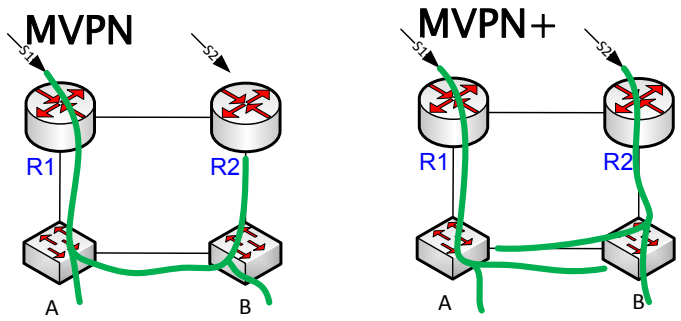


Figure 62 : Cas simple pour prouver l'intérêt de MVPN+

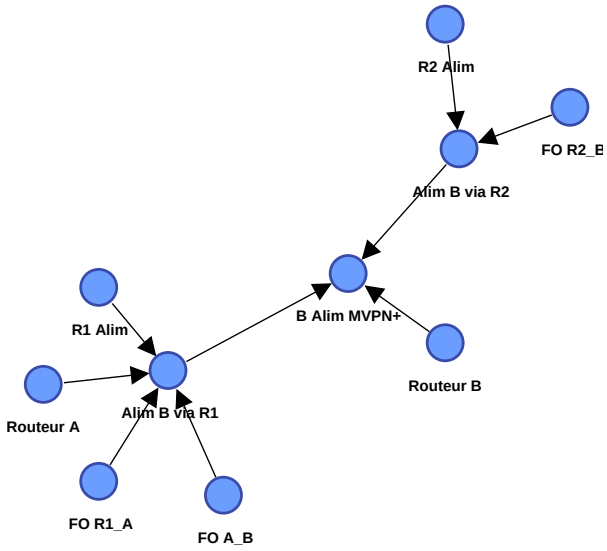


Figure 63 : Représentation par RB du cas simple en MVPN+

Ici nous avons deux sources identiques directement connectées à un VPLS porteur de deux routeurs qui seront deux destinations distinctes. Les deux routeurs R1 et R2 portent des VPRN pour gérer via PIM la redondance de sources. Les routeurs-switchs A et B sont connectés par VPLS aux routeurs pères pour former une sous-boucle R1-A-B-R2.

Dans l'ingénierie MVPN le routeur R1 diffuse à travers tout le VPLS. Ainsi la destination B se retrouve en situation défavorable car elle pourrait directement obtenir son flux depuis la source R2. Avec la nouvelle solution MVPN+, les deux routeurs pères diffusent simultanément dans le VPLS et les routeurs A et B prennent la décision de supprimer le flux transitant entre les deux routeurs. Ainsi la destination B n'est plus en situation défavorable.

La représentation graphique en RB du cas étudié est présentée en Figure 63.

Les résultats des calculs de disponibilité sont rassemblés dans la Table 10. Il apparait que la probabilité de se trouver en situation reroutée diminue et que ce gain augmente la probabilité d'être en fonctionnement nominal. Le temps passé en situation de reroutage est divisé par deux avec la nouvelle solution MVPN+.

Table 10 : Résultats de modélisation du cas simple en RB pour MVPN+

Solution	MVPN : disponibilité	MPVN+ : disponibilité	Delta	Delta par année
Nominal	0.999900003	**0.99995**	+0.000049997	+26.3 min
Secours	0.000099993 (52.6 min)	**0.000049995 (26.3 min)**	-0.000049998	-26.3 min (-50.0%)
Panne	**0.000000005**	**0.000000005**	0	0

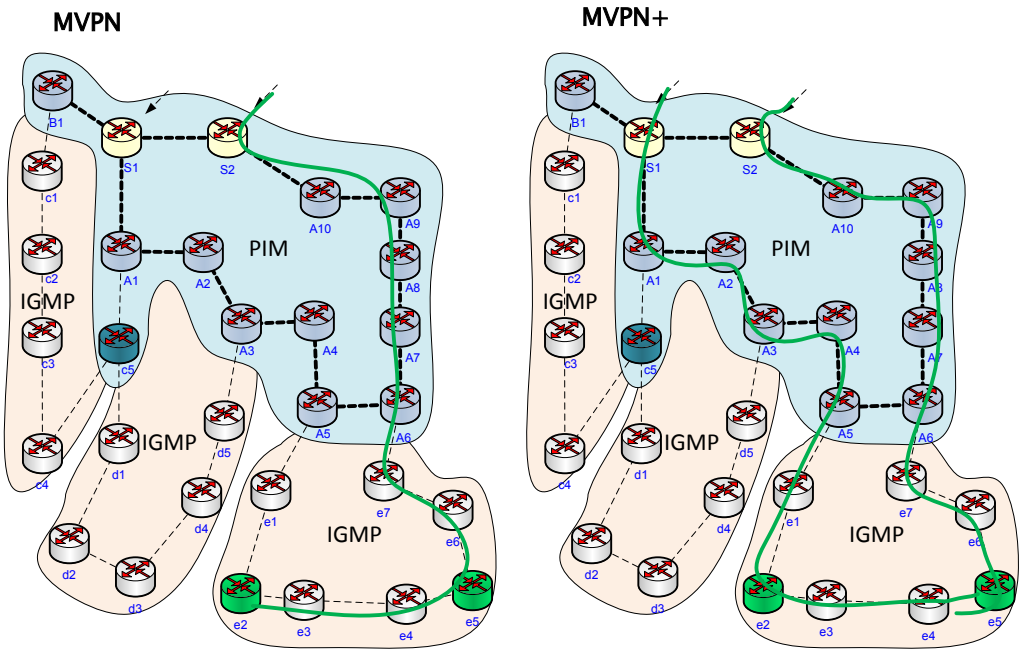


Figure 64 : Fonctionnement sur le cas réel de MVPN et MVPN+

L'étude va maintenant chercher à vérifier sur un cas réel ce que donne la modélisation par RB de la nouvelle solution.

Intéressons-nous à la Figure 64. Avec MVPN seul un des routeurs pères diffuse dans son VPLS. Ici le VPLS contient deux destinations e2 et e5 ; MVPN diffuse de manière optimale pour e5 mais pas pour e2. Dans la solution MVPN+ les deux routeurs pères diffusent pour un comportement optimal que ce soit pour e5 ou pour e2.

Pour le cas réel on obtient la Table 11. On constate que cette nouvelle ingénierie fait gagner 21 minutes de situations de secours ce qui correspond à un gain direct de 1,5%. Comme attendu, il n'y a aucun gain sur la disponibilité et le faible gain en secours n'est pas surprenant dans la mesure où il reflète la situation réelle.

Table 11 : Résultats de modélisation du cas réel en RB pour MVPN+

Solution	MVPN : disponibilité	MPVN+ : disponibilité	Delta	Delta par année
Nominal	0.996784525	**0.996824298**	+0.000039773	+20.92 min
Secours	0.003202403 (28.1h)	**0.00316263 (27.7h)**	-0.000039773	-20.92 min (-1.5%)
Panne	**0.000013072**	**0.000013072**	0	0

Nous avons pu prouver grâce aux RB que cette solution possède des avantages par rapport au MVPN conventionnel. Nous allons dans la suite consolider ces résultats par simulation et maquettage pour tenir compte du comportement dynamique de l'ingénierie MVPN+.

Nous avons vu dans le paragraphe 4.2.1 que la solution MVPN+ nécessite l'analyse de la part des équipements de niveau 2 de la trame Ethernet de manière approfondie. Cette fonction n'est ni remplie par les routeurs-switchs disponibles ni par les modèles de simulation disponibles sous Modeler. Pour tester MVPN+ nous allons émuler son fonctionnement au travers de la solution MVPN+e.

4.2.3. Emulation de la solution MVPN+ par MVPN+e

MVPN+ propose un nouvel algorithme non implémenté dans les équipements et demande des capacités de traitement pour les switchs qui ne sont pas disponibles. Dans le schéma de la Figure 65 la solution implémentable que l'on va appeler MVPN+e utilise la possibilité offerte par un routeur de dernière génération d'intégrer directement un switch sur son interface. On connecte ces switchs entre eux de manière à former une topologie VPLS bouclée, autorisant une protection telle que RSTP à gérer cette boucle. Ainsi une coupure RSTP va se mettre en place et on peut la forcer pour qu'elle soit au point le plus optimal. On obtient alors en amont du VPLS une construction optimale et automatique conditionnée par PIM et dans le VPLS un comportement optimal imposé de manière statique mais suffisamment souple pour résister à des pannes.

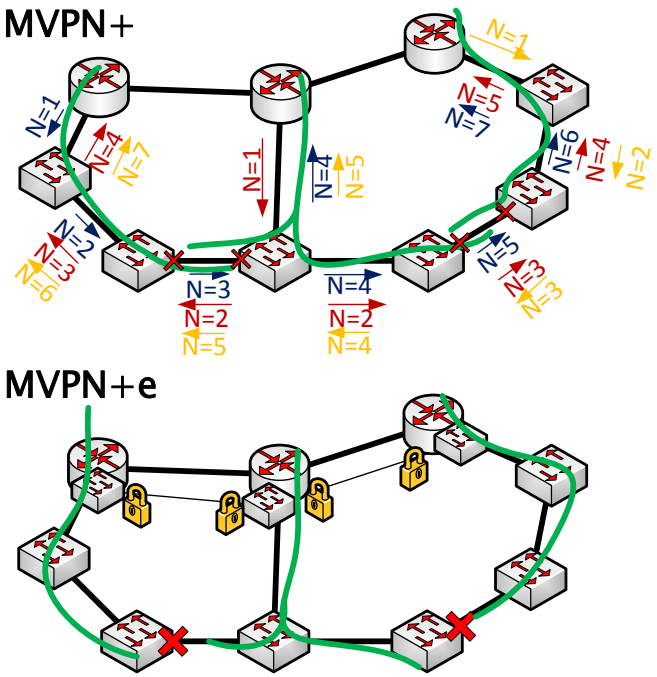


Figure 65 : Solution implémentable de MVPN+ en simulation et en maquette

Une autre particularité de cette proposition est l'utilisation de tunnels de signalisation entre les switchs placés sur les routeurs pères et symbolisés par des cadenas sur le schéma. Ces tunnels bloquent tout trafic multicast et n'autorisent que le protocole RSTP à circuler. Ils produisent un double effet, d'une part de former des topologies bouclées et d'autre part d'empêcher une double consommation de bande passante sur ces liaisons qui sont aussi utilisées pour transporter le multicast via PIM.

Avec cette implémentation MVPN+e nous nous rapprochons beaucoup de la solution cible qui est MVPN+. En effet il est possible de placer les coupures RSTP sur des liaisons choisies, émulant ainsi le comportement de MVPN+ car le switch prend une décision de coupure par boucle tout comme RSTP.

4.2.4. Simulation sous Modeler

Sur Modeler il n'existe pas de modèle de routeur de dernière génération intégrant un switch directement rattaché à une interface du routeur. Ceci dit, cet équipement peut être simulé par un binôme routeur et switch tel que présenté dans la Figure 66 (S1-S1_VPLS et S2-S2_VPLS).

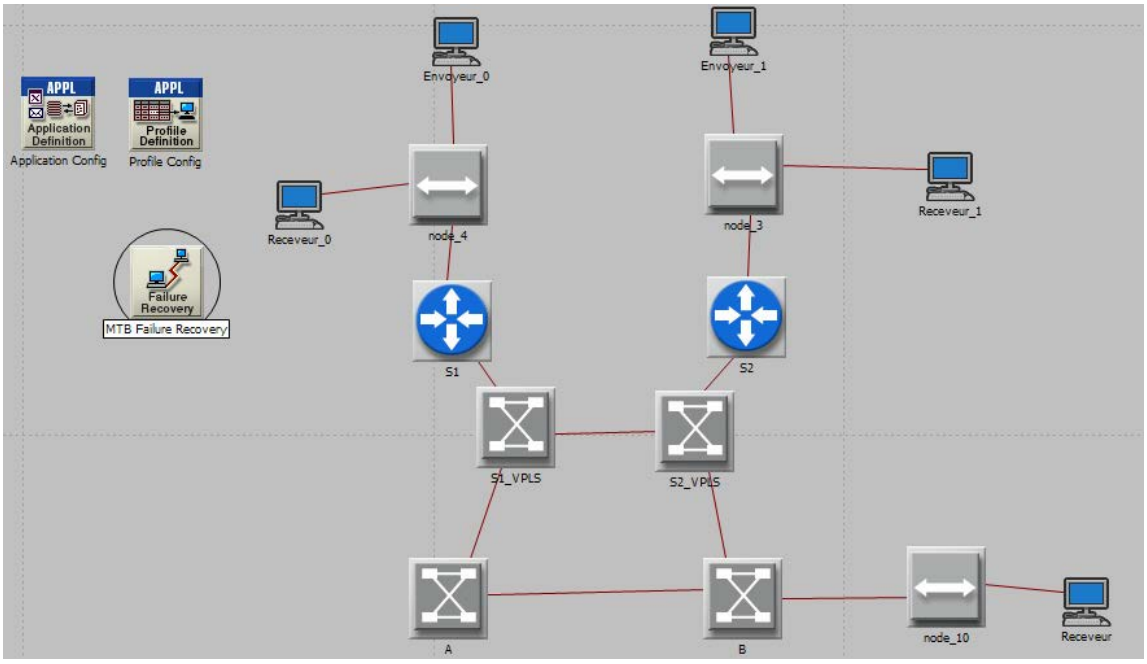


Figure 66 : Représentation sous Modeler de la solution MVPN+e

Table 12 : Résultats de modélisation du cas simple sous Modeler

Solution	MVPN+ (RB) : disponibilité	MPVN+e (Modeler) : disponibilité	Delta	Delta par année
Nominal	0.996824298	0.99376931	+0.00305499	+26.78 h
Secours	0.00316263 (27.7h)	0.00004525 (23.8 min)	-0.00311738	-27.33 h (-98.5%)
Panne	0.000013072 (6.9 min)	0.00007562 (39.8 min)	+0.000062548	+32.9 min (+378%)

Les résultats sont résumés dans la Table 12. Comme il est impossible de modéliser correctement MVPN sous Modeler, nous allons comparer les résultats obtenus pour MVPN+e avec ceux obtenus en RB pour MVPN+. Tout comme MVPN, l'ingénierie simulée par MVPN+e passe beaucoup moins de temps en situation de secours que prévue par le RB. Les phénomènes de basculements ajoutent 32,9 minutes d'indisponibilité ce qui représente une augmentation de 378% de l'indisponibilité par rapport à celle obtenue par RB.

Les résultats obtenus par simulation confirment ceux modélisés par RB. Mais ces approches théoriques méritent une représentation plus qualitative, sur une maquette représentative, que nous proposons dans la dernière partie.

4.2.5. Maquettage en laboratoire

TDF dispose d'une maquette utilisant les mêmes équipements que le réseau TMS. Ce laboratoire constitue un centre de tests pour les différentes évolutions du réseau comme les mises à jour des routeurs ou l'intégration de nouveaux équipements. Dans ce contexte l'équipe de conception du réseau TMS s'est récemment doté de nouveaux routeurs Alcatel qui sont arrivés dans une version logicielle très récente intégrant des fonctions encore plus évoluées que ce que nous permet le réseau actuel.

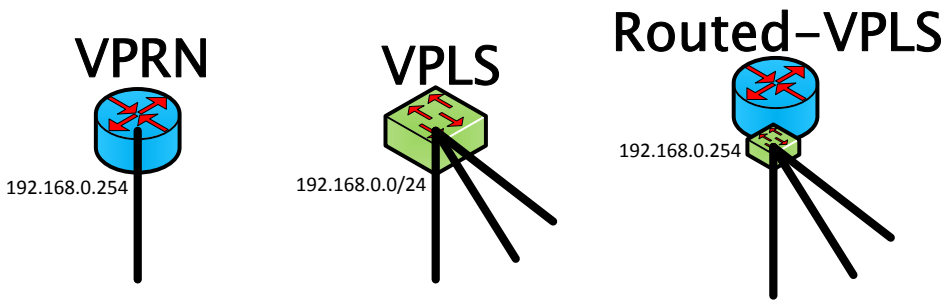


Figure 67 : Différences entre VPRN, VPLS et Routed-VPLS

Ces équipements sont en cours de qualification et de référencement par TDF ce qui fait qu'aujourd'hui ils ne sont pas encore intégrables au réseau TMS. Bien que MVPN+ ne soit pas directement implémentable nous allons encore une fois nous rapprocher du comportement en utilisant MVPN+e et les fonctionnalités de Routed-VPLS disponibles uniquement sur ces équipements de nouvelle génération. Cette technologie permet d'allouer plusieurs tunnels MPLS à une seule interface dans un VPRN. Classiquement dans un VPRN on ne peut allouer qu'un seul tunnel MPLS ou un seul port vers un client par interface. Un VPLS ne permet pas de faire de routage ou d'accéder à ces fonctions sur le même routeur. Le Routed-VPLS autorise le lien entre un VPLS et un VPRN au sein du même routeur pour qu'une interface soit propagée à travers plusieurs tunnels MPLS (Figure 67). C'est une fonction équivalente à celle qui permet à une box Internet de posséder plusieurs ports dans le même réseau local.

L'objectif est de quantifier les impacts à l'image lors de pannes sur le réseau. On se place dans la configuration présentée Figure 68. On va chercher à mesurer qualitativement le rendu à l'image suite à des pannes sur les liaisons numérotées. L'outil de mesure est placé sur le routeur C, qui est en situation défavorable dans la solution MVPN. Pour des raisons d'optimisation nous allons également placer une destination sur le routeur A mais qui ne sera pas monitorée.

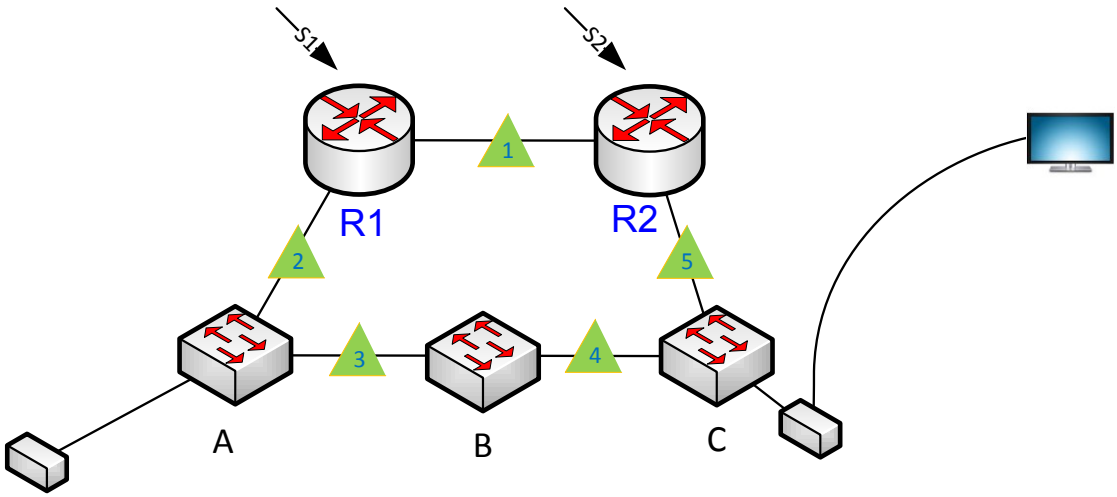


Figure 68 : Topologie utilisée pour l'analyse d'impacts à l'image

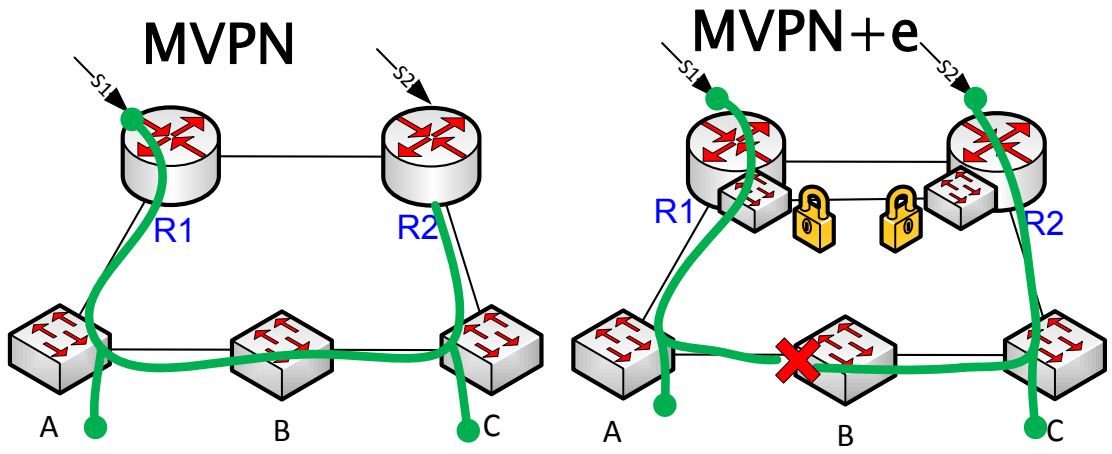


Figure 69 : Utilisation de MVPN et MVPN+e sur la maquette

Sur cette topologie nous allons implémenter MVPN et MVPN+e tel que résumé dans la Figure 69. Pour MVPN c'est le routeur R1 qui va diffuser pour tout le VPLS alors que pour MVPN+e les deux routeurs R1 et R2 diffuseront dans le VPLS. On met en place un filtre dans le tunnel entre R1 et R2 pour empêcher tout trafic autre que le RSTP et en particulier le multicast à diffuser.

La Table 13 résume les tests effectués pour les deux solutions du point de vue des impacts à l'image sur le routeur C. Les localisations des pannes sont présentées Figure 68.

Table 13 : Résultats de mesure qualitative sur le labo entre les deux solutions MVPN

	MVPN	MPVN+e
Panne 1	Aucun impact	Aller : Petit blocage sur le moniteur, 32 paquets IP perdus et 11285 RTP sequence errors Retour : 3s bloqué sur l'image, 2 secondes d'erreurs sur le moniteur et 1 resynchronisation sur la passerelle
Panne 2	Aller : 3s bloqué sur l'image, 2 secondes d'erreurs sur le moniteur et 1 resynchronisation sur la passerelle Retour : Aucun impact détecté, aucune erreur sur le moniteur mais 4958 RTP sequence errors dans la passerelle	Aucun impact
Panne 3	Aller : 3s bloqué sur l'image, 2 secondes d'erreurs sur le moniteur et 1 resynchronisation sur la passerelle Retour : Aucun impact détecté, aucune erreur sur le moniteur mais 13489 RTP sequence errors dans la passerelle	Aucun impact
Panne 4	Aller : 2s bloqué sur l'image, 1 secondes d'erreurs sur le moniteur et 1 resynchronisation sur la passerelle Retour : Aucun impact détecté, aucune erreur sur le moniteur mais 57945 RTP sequence errors dans la passerelle	Aucun impact
Panne 5	Aucun impact	Aller : 3s bloqué sur l'image, 2 secondes d'erreurs sur le moniteur et 1 resynchronisation sur la passerelle Retour : Aucun impact détecté, aucune erreur sur le moniteur mais 1 RTP sequence errors dans la passerelle et 7 RTP jumps

Sur cette topologie, l'ingénierie MVPN+e est moins sensible aux pannes que l'ingénierie MVPN, 2 pannes sur 5 versus 3 pannes sur 5. Autre constatation importante, au retour de panne il y a un impact conséquent dans la solution MVPN+e alors que l'ingénierie classique n'induit aucun impact au retour de panne. Ce phénomène d'impact au retour de panne pour MVPN+e provient

vraisemblablement de l'interaction entre les protocoles RSTP et PIM qui ralentit la convergence de chacun d'eux.

Ceci dit, nous considérons que la solution MVPN+e reste préférable du fait de sa plus faible sensibilité aux pannes. La solution MVPN+e est donc globalement plus avantageuse que MVPN.

4.2.6. Conclusion

Ces modèles nous permettent de vérifier que le comportement de l'ingénierie MVPN+ apporte une amélioration théorique de la disponibilité du système en minimisant les reroutages ce que montrent les RB. L'émulation de MVPN+ par MVPN+e permet de conforter les résultats obtenus par RB grâce à la simulation de l'ingénierie dans Modeler. Finalement l'approche qualitative effectuée sur la maquette avec des éléments réels confirment l'apport pressenti de la solution MVPN+ sur le nombre d'impacts à l'image.

Conclusion et Perspectives

Les services de communication à usage professionnel ou usage grand public sont très répandus, fonctionnant sur des réseaux de communication à couverture nationale ils doivent naturellement présenter un taux de disponibilité très élevé. Les pannes ont des causes diverses et sont inéluctables. C'est donc la durée de chaque défaillance qu'il faut minimiser en utilisant de la redondance d'infrastructure et des mécanismes de basculement rapide entre le mode initial et le mode de secours. Ces mécanismes sont développés depuis longtemps sur des réseaux homogènes comme SDH. Ils ne sont pas applicables sur des réseaux utilisant des liaisons hétérogènes comme le réseau TMS de TDF. Cette thèse avait pour objectif d'établir une méthode scientifique d'analyse de la disponibilité des services réseau en y intégrant les impacts induits par les reroutages.

La première contribution de cette thèse est une méthode de modélisation par Réseaux Bayésiens de la disponibilité d'un service sur un ensemble de points du réseau. La construction du Réseau Bayésien s'appuie sur le fonctionnement des protocoles assurant l'acheminement du flux audiovisuel jusqu'au point de service. C'est la partie délicate de la modélisation car elle demande une bonne connaissance de ces protocoles et de leurs interactions. Les tables de probabilités conditionnelles sont remplies à l'aide de cette connaissance tandis que les tables de probabilités de fonctionnement des systèmes physiques, liaisons et routeurs/switchs, sont remplies à l'aide des données de disponibilité mesurées ou fournies par le constructeur.

Les modèles obtenus pour des services implémentés sur des réseaux de complexité variable ont été exploités sur l'outil d'inférence BayesiaLab. Les résultats obtenus sont conformes et ont permis une comparaison efficace et pertinente de deux ingénieries protocolaires différentes mais qui avait une même finalité de distribution de flux multicast.

Ces résultats montrent que la méthode utilisée et les modèles construits sont corrects même si cela ne constitue pas une preuve formelle de validité. Cette contribution est importante pour l'entreprise TDF car elle acquiert un outil d'évaluation a priori de la disponibilité d'un service sur toute infrastructure et pour tout type d'ingénierie protocolaire. Elle devrait en faire usage dans l'avenir pour l'évaluation de son réseau, pour le choix de nouvelles ingénieries protocolaires et pour la conception de nouveaux réseaux et systèmes complexes à haute disponibilité.

Une deuxième contribution de cette thèse est la proposition de l'ingénierie protocolaire MVPN+. Elle a été conçue dans le but de combler les faiblesses de l'ingénierie protocolaire MVPN mises en évidence par la première contribution. Cette proposition offre une nouvelle alternative à la solution MVPN originale basée sur les caractéristiques uniques du réseau TMS.

Après la conception du fonctionnement de cette ingénierie, notre étude s'est focalisée sur la mesure de la disponibilité et la vérification de l'apport réel de la solution. A l'aide des approches de modélisation par RB et par simulation sous Modeler, nous avons pu mettre en avant le gain apporté par cette solution. Néanmoins la proposition étant une innovation dans le fonctionnement des protocoles, cette solution n'a pu être réellement implémentée et nous avons dû émuler le comportement de cette ingénierie pour la simuler et la maquetter. Cette émulation appelée MVPN+e a permis de prouver que la proposition MVPN+ apportait les espérances d'amélioration de la solution MVPN.

Dans cette thèse deux approches ont été utilisées pour modéliser la disponibilité d'un service audiovisuel : une approche par modélisation probabiliste et une approche par modélisation sous simulateur. Lors des simulations, il a été envisagé d'utiliser des modèles de type simulations de Monte-Carlo car le réseau est un système très fiable. L'étude d'évènements rares a mis en évidence des contraintes fortes sur les paramètres de simulation comme la durée de simulation.

Les principales difficultés sont donc apparues dans la partie simulation notamment avec le logiciel Modeler. Nous nous sommes aperçus que les modèles représentant le comportement de MVPN n'étaient pas compatibles avec les modules ajoutés à Modeler pour dégrader les équipements réseau. Il a donc été impossible d'effectuer une analyse proche de celle effectuée en RB et nous avons donc dû nous contenter d'une validation des modèles RB à l'aide de la simulation. De plus l'approche par simulation devait nous permettre de modéliser les durées de basculements qui ne sont pas représentées sous RB. Mais comme il a été impossible de simuler correctement le comportement de MVPN, les simulations ne nous ont pas permis de conclure quant à l'impact des durées de basculement sur la disponibilité globale.

La suite de ces travaux consiste à tester sur d'autres ingénieries protocolaires l'utilisation des RB à des fins d'analyse et d'aide à la décision. Il va être également possible d'utiliser les données du réseau réel pour faire de nouvelles analyses de disponibilité une fois la solution entièrement mise en place. Une autre perspective est d'implémenter le protocole MVPN+ sur d'autres simulateurs que Modeler pour tester de façon plus approfondie le comportement et les performances de cette évolution dans le transport des flux multicasts.

Annexes

Annexes..... 105

Annexe 1 : Détail du modèle en RB du cas simple 1 en RSTP..... 106

Annexe 2 : Représentation par RB du cas réel pour la solution MVPN. 110

Annexe 3 : Représentation par RB du cas réel pour la solution MVPN et plusieurs destinations. 111

Annexe 1 : Détail du modèle en RB du cas simple 1 en RSTP.

S2	Fo_S2-A	A	Nominal	Secours	Panne
Ok	Ok	Ok	100,000	0,000	0,000
		NOk	0,000	0,000	100,000
	NOk	Ok	0,000	0,000	100,000
		NOk	0,000	0,000	100,000
NOk	Ok	Ok	0,000	0,000	100,000
		NOk	0,000	0,000	100,000
	NOk	Ok	0,000	0,000	100,000
		NOk	0,000	0,000	100,000

Annexe 1. 1 : Nœud « A Alimenté via Ouest »

Fo_B-A	A	B Alimenté ...	Nominal	Secours	Panne
Ok	Ok	Nominal	0,000	100,000	0,000
		Secours	0,000	100,000	0,000
		Panne	0,000	0,000	100,000
	NOk	Nominal	0,000	0,000	100,000
		Secours	0,000	0,000	100,000
		Panne	0,000	0,000	100,000
NOk	Ok	Nominal	0,000	0,000	100,000
		Secours	0,000	0,000	100,000
		Panne	0,000	0,000	100,000
	NOk	Nominal	0,000	0,000	100,000
		Secours	0,000	0,000	100,000
		Panne	0,000	0,000	100,000

Annexe 1. 2 : Nœud « A Alimenté via Est »

A Alimenté...	A Alimenté...	Nominal	Secours	Panne
Nominal	Nominal	100,000	0,000	0,000
	Secours	100,000	0,000	0,000
	Panne	100,000	0,000	0,000
Secours	Nominal	0,000	100,000	0,000
	Secours	0,000	100,000	0,000
	Panne	0,000	100,000	0,000
Panne	Nominal	0,000	100,000	0,000
	Secours	0,000	100,000	0,000
	Panne	0,000	0,000	100,000

Annexe 1. 3 : Nœud « A Alimenté »

A Alimenté...	Fo_B-A	B	Nominal	Secours	Panne
Nominal	Ok	Ok	0,000	100,000	0,000
		NOk	0,000	0,000	100,000
	NOk	Ok	0,000	0,000	100,000
		NOk	0,000	0,000	100,000
Secours	Ok	Ok	0,000	100,000	0,000
		NOk	0,000	0,000	100,000
	NOk	Ok	0,000	0,000	100,000
		NOk	0,000	0,000	100,000
Panne	Ok	Ok	0,000	0,000	100,000
		NOk	0,000	0,000	100,000
	NOk	Ok	0,000	0,000	100,000
		NOk	0,000	0,000	100,000

Annexe 1. 4 : Nœud « B Alimenté via Ouest »

B	S1	Fo_S1-B	Nominal	Secours	Panne
Ok	Ok	Ok	100,000	0,000	0,000
		NOk	0,000	0,000	100,000
	NOk	Ok	0,000	0,000	100,000
		NOk	0,000	0,000	100,000
NOk	Ok	Ok	0,000	0,000	100,000
		NOk	0,000	0,000	100,000
	NOk	Ok	0,000	0,000	100,000
		NOk	0,000	0,000	100,000

Annexe 1. 5 : Nœud « B Alimenté via Est »

B Alimenté ...	B Alimenté ...	Nominal	Secours	Panne
Nominal	Nominal	100,000	0,000	0,000
	Secours	100,000	0,000	0,000
	Panne	100,000	0,000	0,000
Secours	Nominal	0,000	100,000	0,000
	Secours	0,000	100,000	0,000
	Panne	0,000	100,000	0,000
Panne	Nominal	0,000	100,000	0,000
	Secours	0,000	100,000	0,000
	Panne	0,000	0,000	100,000

Annexe 1. 6: Nœud « B Alimenté »

Fo_A-D	D	A Alimenté	Nominal	Secours	Panne
Ok	Ok	Nominal	0,000	100,000	0,000
		Secours	0,000	100,000	0,000
		Panne	0,000	0,000	100,000
	NOk	Nominal	0,000	0,000	100,000
		Secours	0,000	0,000	100,000
		Panne	0,000	0,000	100,000
NOk	Ok	Nominal	0,000	0,000	100,000
		Secours	0,000	0,000	100,000
		Panne	0,000	0,000	100,000
	NOk	Nominal	0,000	0,000	100,000
		Secours	0,000	0,000	100,000
		Panne	0,000	0,000	100,000

Annexe 1. 7 : Nœud « D Alimenté via A »

Fo_B-D	D	B Alimenté	Nominal	Secours	Panne
Ok	Ok	Nominal	100,000	0,000	0,000
		Secours	0,000	100,000	0,000
		Panne	0,000	0,000	100,000
	NOk	Nominal	0,000	0,000	100,000
		Secours	0,000	0,000	100,000
		Panne	0,000	0,000	100,000
NOk	Ok	Nominal	0,000	0,000	100,000
		Secours	0,000	0,000	100,000
		Panne	0,000	0,000	100,000
	NOk	Nominal	0,000	0,000	100,000
		Secours	0,000	0,000	100,000
		Panne	0,000	0,000	100,000

Annexe 1. 8 : Nœud « D Alimenté via B »

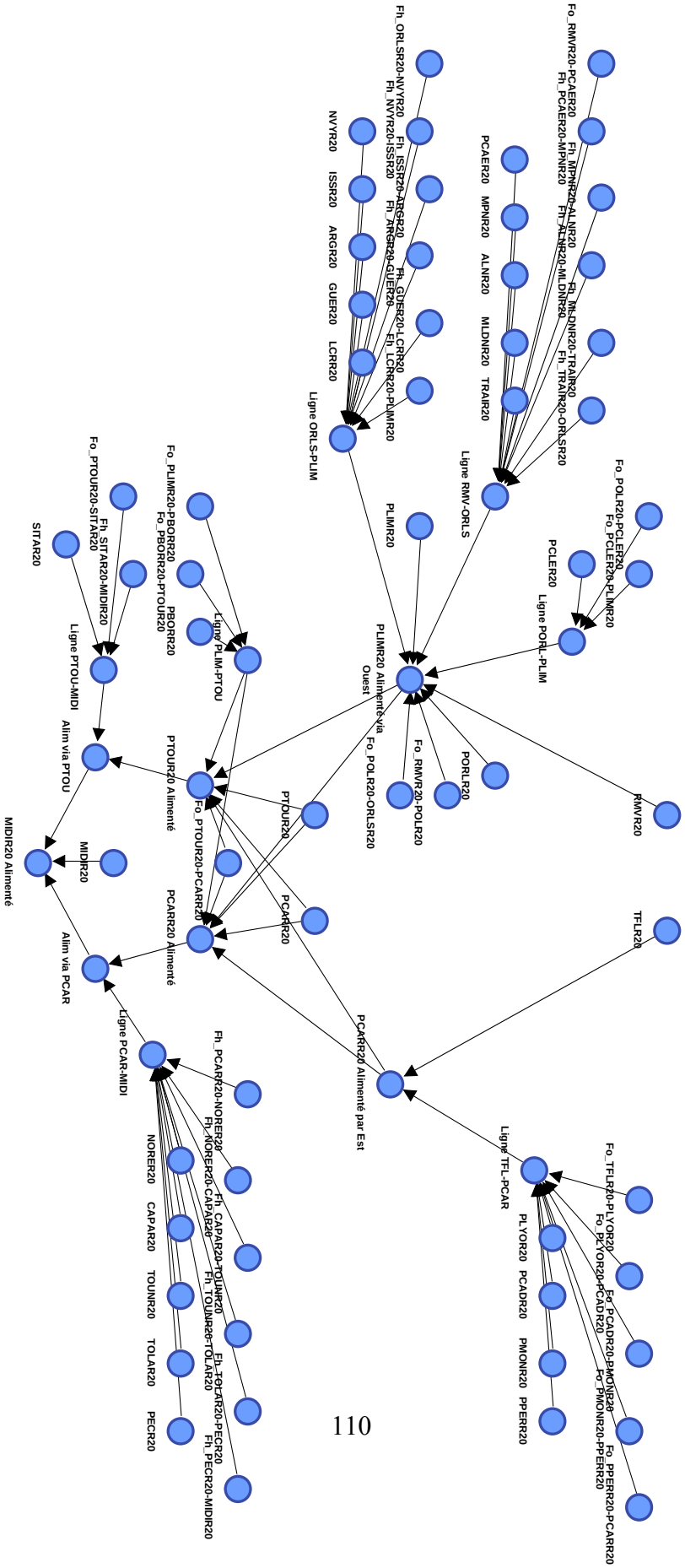
Routeur B ...	D Alimenté...	D Alimenté...	Nominal	Secours	Panne
Vrai	Nominal	Nominal	0,000	0,000	100,000
		Secours	0,000	0,000	100,000
		Panne	0,000	0,000	100,000
	Secours	Nominal	0,000	0,000	100,000
		Secours	0,000	0,000	100,000
		Panne	0,000	0,000	100,000
	Panne	Nominal	0,000	0,000	100,000
		Secours	0,000	0,000	100,000
		Panne	0,000	0,000	100,000
Faux	Nominal	Nominal	100,000	0,000	0,000
		Secours	100,000	0,000	0,000
		Panne	100,000	0,000	0,000
	Secours	Nominal	0,000	100,000	0,000
		Secours	0,000	100,000	0,000
		Panne	0,000	100,000	0,000
	Panne	Nominal	0,000	100,000	0,000
		Secours	0,000	100,000	0,000
		Panne	0,000	0,000	100,000

Annexe 1. 9 : Nœud « D Alimenté »

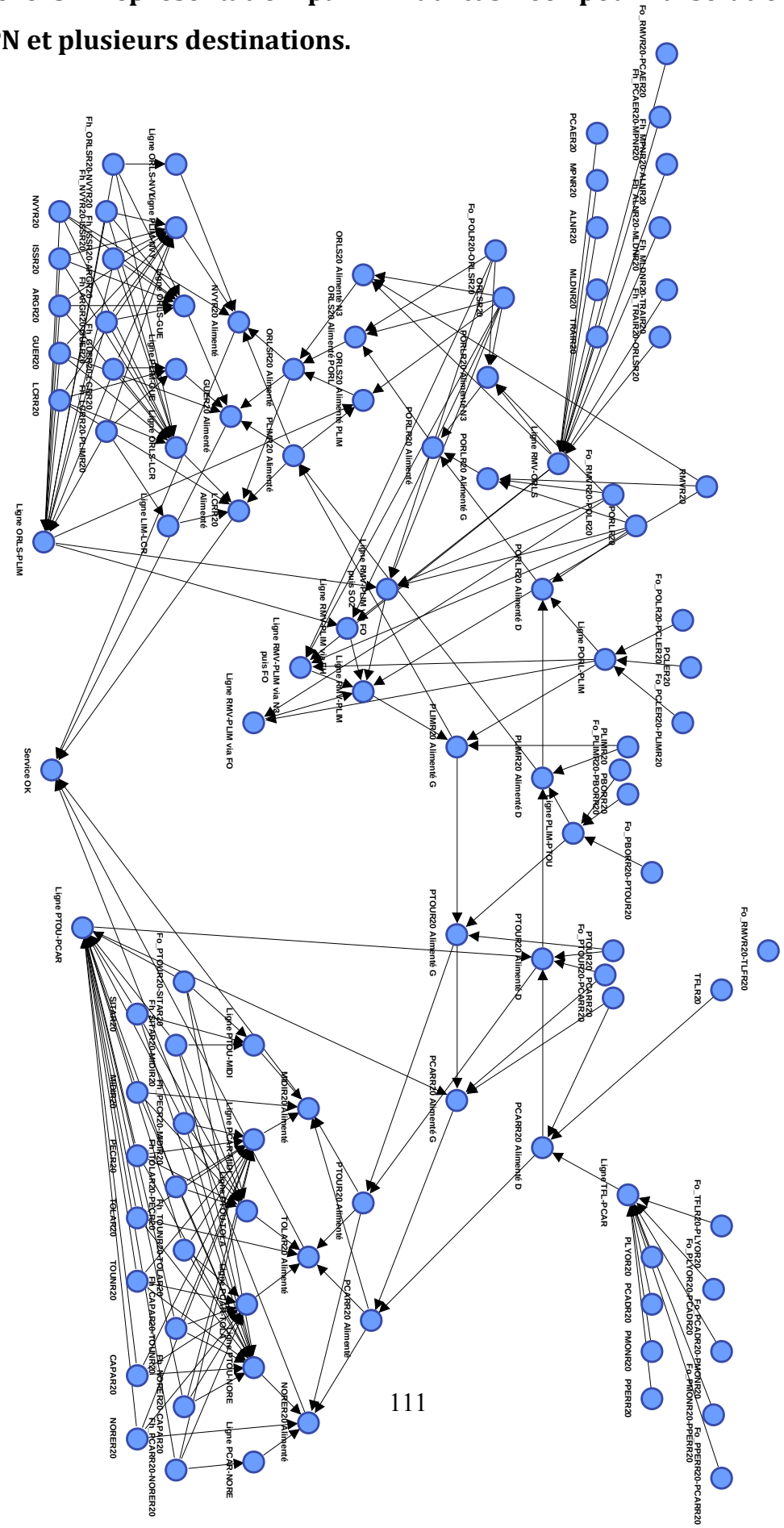
B Alimenté	Fo_A-D	D	Fo_B-D	Vrai	Faux
Nominal	Ok	Ok	Ok	0,000	100,000
			NOk	0,000	100,000
		NOk	Ok	0,000	100,000
			NOk	0,000	100,000
	NOk	Ok	Ok	0,000	100,000
			NOk	0,000	100,000
		NOk	Ok	0,000	100,000
			NOk	0,000	100,000
Secours	Ok	Ok	Ok	0,000	100,000
			NOk	0,000	100,000
		NOk	Ok	0,000	100,000
			NOk	0,000	100,000
	NOk	Ok	Ok	0,000	100,000
			NOk	0,000	100,000
		NOk	Ok	0,000	100,000
			NOk	0,000	100,000
Panne	Ok	Ok	Ok	100,000	0,000
			NOk	0,000	100,000
		NOk	Ok	0,000	100,000
			NOk	0,000	100,000
	NOk	Ok	Ok	0,000	100,000
			NOk	0,000	100,000
		NOk	Ok	0,000	100,000
			NOk	0,000	100,000

Annexe 1. 10 : Nœud « Routeur B Isolé Sans Panne ssboucle»

Annexe 2 : Représentation par RB du cas réel pour la solution MVPN.



Annexe 3 : Représentation par RB du cas réel pour la solution MVPN et plusieurs destinations.



Bibliographie

[1] Poul E. Heegaard, Kishor S. Trivedi. Network survivability modeling. *Computer Networks*. Volume 53, Issue 8, Pages 1215–1234, 2009.

[2] James P.G. Sterbenz, David Hutchison, Egemen K. Çetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Schöller, Paul Smith. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*. Volume 54, Issue 8, Pages 1245–1265, 2010.

[3] Chunlei Wang, Lan Fang, Yiqi Dai, Liang Ming, Qing Miao, Dongxia Wang. Network Survivability Evaluation Model Based on Immune Evolution and Multiple Criteria Decision Making. CyberC 2012. Sanya, Chine. 2012.

[4] Chunlei Wang, Dongxia Wang, Yiqi Dai. Towards a Unified Framework for Network Survivability Measurement. IEEE NSWCTC 2010. Wuhan, Chine. 2010.

[5] H. Derbel, N. Agoulmine, M. Salaün. ANEMA : Autonomic network management architecture to support self-configuration and self-optimization in IP networks. *Computer Networks*. Volume 53, Issue 3, Pages 418-430, 2009.

[6] W. Itani, C. Ghali, R. Bassil, A. Kayssi, A. Chehab. ServBGP : BGP-inspired autonomic service routing for multi-provide collaborative architectures in the cloud. *Future Generation Computer Systems*. Volume 32, Pages 99-117, 2014.

[7] Iftakharul Islam, Javed I Khan. Video Splicing Techniques for P2P Video Streaming. ICDCSW'15. Columbus. Ohio. 2015.

[8] Yan Jinyao, W Muhlbauer. Analytical Framework for Improving the Quality of Streaming Over TCP. *IEEE Transactions on Multimedia*. Volume 14, Issue 6, Pages 1579 – 1590, 2012.

[9] Marcus Laumer, Peter Amon, Andreas Hutter, Andre Kaup. A Compressed Domain Change Detection Algorithm for RTP Streams in Video Surveillance Applications. MMSP'11. Hangzhou. Chine. 2011.

[10] Z Begic, H Bajric, M Kos. Rapid synchronization of RTP multicast sessions using the retransmission server. SoftCOM'10. Split. Croatie. 2010.

[11] Jochen Gruen, Manuel Gorius, Thorsten Herfet. Interactive RTP services with Predictable Reliability. ICCE-Berlin'13. Berlin. Allemagne. 2013.

[12] M Nuhbegovic, A Colakovic, A Haskovic. Validating IPTV service quality under realistic triple play network conditions. BIHTEL'14. Sarajevo. Bosnie-Herzégovine. 2014.

[13] Joonho Choi, Myungsik Yoo, Biswanath Mukherjee. Efficient Video-on-Demand Streaming for Broadband Access Networks. *Journal of Optical Communications and Networking*. Volume 2, Issue 1. Pages 38-50. 2010.

[14] R Rabbat, Siu Kai-Yeung. QoS support for integrated services over CATV. *Communications Magazine, IEEE* . Volume 37 , Issue 1. Pages 64-68. 1999.

[15] X.D Yang, Y.H Song, T.J Owens, J Cosmas. Performance analysis of time slicing in DVB-H. SympoTIC '04. Bratislava, Slovaquie. 2004.

[16] P.S Pandey, N Purohit. Improving multicasting approach in UMTS network. ICGCCEE'14. Coimbatore. Inde. 2014.

[17] J Ott, C Borgmann. Multicasting the ITU MCS: integrating point-to-point and multicast transport. ICCS '94. Singapour. 1994.

[18] Stephen F Bush, Orhan Imer. Enhancing reliable multicast transport to mitigate the impact of blockage. CAMAD'06. Trente. Italie. 2006.

[19] Joseph P. Macker. Reliable Multicast Transport and Integrated Erasure-Based Forward Error Correction. MILCOM'97. Monterey. Californie. 1997.

[20] M Solera-Delgado, S Sallent. A Cost-Based Approach to a Reliable Multicast Transport Protocol. ICCT '06. Guilin. Chine. 2006.

[21] Sarah Ruepp, Henrik Wessing, and Michael Berger. Protection Switching for Carrier Ethernet Multicast. GLOBECOM'10. Miami. Floride. 2010.

[22] T Shome, S Gupta. Performance enhancement of pragmatic general multicast (PGM) protocol using a local loss recovery strategy. ICCC'13. Xi'an. Chine. 2013.

[23] T. Bartczak, P. Zwierzykowski. Performance evaluation of Source-Specific Multicast routing protocols for IP networks. CSNDSP'12. Poznan. Pologne. 2012.

[24] T Gayraud, P Berthou, P Owezarski, M Diaz. M3POC : a multimedia multicast transport protocol for cooperative applications. ICME'2000. New York, New York. 2000.

[25] M.P.F Dos Santos, W.A Clarke, A.L Nel. Enhancing telecommunications business operations and service level agreements by

incorporating operational risk management. AFRICON 2007. Windhoek. Afrique du Sud. 2007.

[26] Y Diao, L Lam, L Shwartz, D Northcutt. Modeling the Impact of Service Level Agreements During Service Engagement. *IEEE Transactions on network and service*, Volume 11, No. 4, Pages: 431-440, 2014.

[27] Houda Ghamlouch, Mitra Fouladirad, Antoine Grall. On the use of Jump-Diffusion process for Maintenance decisionmaking: A first step. RAMS'15. Palm Harbor, Floride. 2015.

[28] Kailbach Walter, Ilchmann Frank. Multi Service OTN Design and Optimization of a Germany Wide Scale Example Network. ITG'10. Leipzig. Allemagne. 2010.

[29] D. Katz, D. Ward. Bidirectional Forwarding Detection (BFD). *RFC 5880*. 2010.

[30] M. Lasserre, V. Kompella. Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling. *RFC 4762*. 2007.

[31] B. Gleeson, A. Lin, J. Heinanen, G. Armitage, A. Malis. A Framework for IP Based Virtual Private Networks. *RFC 2764*. 2000.

[32] D. Levi, D. Harrington. Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol. *RFC 4318*. 2005.

[33] B. Fenner, M. Handley, H. Holbrook, I. Kouvelas. Protocol Independent Multicast - Sparse Mode (PIM-SM) : Protocol Specification (Revised). *RFC 4601*. 2006.

[34] B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan. Internet Group Management Protocol, Version 3. *RFC 3376*. 2002.

[35] Eric C. Rosen, Yiqun Ca. Multicast in MPLS/BGP IP VPNs. *Internet Draft*. 2004.

[36] 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.

[37] Alain Villemeur. *Sûreté de fonctionnement des systèmes industriels*. Eyrolles. 1988.

[38] Jianwen Xiang, Yanoo K., Maeno Y., Tadano K. Automatic Synthesis of Static Fault Trees from System Models. SSIRI 2011. Jeju. Islande. 2011.

[39] A. Bobbio, L. Portinale, M. Minichino, E. Ciancamerla. 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.

[40] P. Weber, G. Medina-Oliva, C. Simon, B. Iung. 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.

[41] 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.

[42] 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.

[43] Jensen F, Jensen F.V, Dittmer S.L. From Influence Diagrams to Junction Trees. UAI'94. Seattle, Washington. USA. 1994.

[44] Weber P, Simon C, Theilliol D, Puig V. Control allocation of k-out-of-n systems based on Bayesian Network Reliability model : Application to a drinking water network. ESREL'11. Troyes. France. 2011.

[45] Weber P, Simon C. Réseaux bayésiens : methodologies de modélisation en sûreté de fonctionnement. *Dans BIVI AFNOR Maitrise des risques*, pp 1-29. 2013.

[46] Xiao-Li Gao, Bing-Han Li, San-Yang Liu. New algorithm for constructing Bayesian network structures from data. ISKE'10. Hangzhou. Chine. 2010.

[47] Fishman G.S. *Principles of discrete Event Digital Simulation*. John Wiley and Sons. New York. 1978.

[48] Saggadi Samira. *Simulation d'événements rare par Monte Carlo dans les réseaux hautement fiable. Modélisation et simulation*. Thèse Université Rennes 1. 2013.

[49] Jie Cai, Bo Jia. Network Simulation Based on OPNTE[4] and Application. ETCS '09. Wuhan. Hubei. 2009.

[4] Erreur dans le titre de la part de l'auteur. Il faut lire OPNET.

[50] Lee Junghoon, R Life, G Elmasry, C Phillips. Using opnet with satcom planning. MILCOM 2010. San Jose. CA. 2010.

[51] Jing-bo XIA, Ming-hui LI, Lu-jun WAN. Research on MPLS VPN Networking Application Based on OPNET. ISISE '08. Shanghai. Chine. 2008.

[52] A Bashar, G Parr, S McClean, B Scotney. Performance analysis of Bayesian Networks-based distributed Call Admission Control for NGN. NOMS'12. Maui. Hawai. 2012.

[53] Hingray B. Evaluation de la disponibilité d'un service d'un réseau de communication multicast par simulation et estimation de son impact environnemental. Rapport Master 2. 2015.

Liste des publications

S.Pirlot, E. Gnaedinger, F. Lepage, R. Kopp. Modélisation d'un réseau IP/MPLS par réseaux Bayésiens pour améliorer le recouvrement d'une double défaillance. JD/JNMACS'15, Bourges, France, 2015.

S.Pirlot, E. Gnaedinger, F. Lepage, R. Kopp. IP/MPLS network modeling using Bayesian networks to improve double failure recovery. IEEE IESM'15, Séville, Espagne, 2015.

S.Pirlot, E. Gnaedinger, F. Lepage, R. Kopp. Modeling an IP network for audiovisual streaming to improve double failure recovery. IEEE ANTS'15, Calcutta, Inde, 2015.

Acronymes

BGP : Border Gateway Protocol
Epipe : Ethernet Pipe
GRE : Generic Routing Encapsulation
IETF : Internet Engineering Task Force
IGMP : Internet Group Management Protocol
IS-IS : Intermediate System to Intermediate System
LDP : Label Distribution Protocol
MEF : Metro Ethernet Forum
MPLS : MultiProtocol Label Switching
MTBF : Mean Time Between Failure
MTTR : Mean Time To Repaire
MVPN : Multicast VPN (Virtual Private Network)
OSPF : Open Shortest Path First
OTN : Optical Transport Network
PIM : Protocol Independent Multicast
POP : Point Of Presence
QdS : Qualité de Service
RB : Réseaux Bayésiens
RSTP : Rapid Spanning Tree Protocol
RSVP : Ressource reSerVation Protocol
RUHD : Réseau Ultra-Heut Débit (TDF)
SFN : Single Frequency Network
SLA : Service Level Agreement
TMS : Transport Multi-Services (TDF)
TNT : Télévision Numérique Terrestre
TPC : Table de Probabilités Conditionnelles
VLL : Virtual Leased Line
VPLS : Virtual Private Lan Service
VPRN : Virtual Private Routed Network
VRF : VPN Routing and Forwarding