Comment gérer un réseau « optique » privé : l'expérience de LCG

Guillaume Cessieux
Centre de Calcul de l'IN2P3
CC-IN2P3 - 29 bd du 11 novembre 1918 – 69622 Villeurbanne Cedex
guillaume.cessieux@cc.in2p3.fr

Mathieu Goutelle
CNRS UREC
CC-IN2P3 - 29 bd du 11 novembre 1918 – 69622 Villeurbanne Cedex
mathieu.goutelle@urec.cnrs.fr

Résumé

Pour les besoins du stockage et de l'analyse des données produites par le Large Hadron Collider *(LHC) au CERN, une infrastructure de calcul de stockage, le* LHC Computing Grid *(LCG), a été construite, incluant notamment un réseau mis en place depuis 2003 et interconnectant les douze centres de ressources impliqués. Au-delà de la mise en œuvre technique d'un réseau privé haut-débit à l'échelle mondiale, l'exploitation d'un tel outil soulève des problématiques inédites, à la fois en terme de supervision et de gestion opérationnelle. Les concepts introduits, les solutions adoptées et les leçons apprises au cours de ces quatre ans peuvent sans aucun doute servir de point de départ pour les institutions ou projets confrontés à des problèmes similaires de gestion d'un tel réseau dans un contexte multi-domaines.*

Mots clefs

Opérations, supervision, perfSONAR, coordination, réseau privé optique, multi-domaines, LHCOPN.

1 Introduction

Le Grand Collisionneur de hadrons, (*Large Hadron Collider*[1], LHC) est un accélérateur de particules qui sondera la matière plus profondément que jamais. Sa mise en marche est prévue pour 2008 et il permettra à terme des collisions de faisceaux de protons à des niveaux d'énergie jamais encore atteint. Un composant critique de l'infrastructure informatique construite pour le LHC est son réseau d'interconnexion, aussi appelé *LHC Optical Private Network* (OPN) [1,5]. Ce réseau, construit pendant ces quatre dernières années, connecte le CERN (Organisation Européenne pour la Recherche Nucléaire[2], à Genève), où les données du LHC sont produites, et les onze centres de ressources (appelés Tier 1) répartis dans le monde, en Europe, en Amérique du Nord et en Asie. Les principaux objectifs sont d'abord de transférer les données produites par les expériences depuis les équipements de stockage temporaires du CERN vers les équipements de stockage permanents dans les Tiers 1, où elles seront traitées et analysées par les physiciens, et ensuite de permettre des transferts inter-sites à des fins de réplication ou d'accès aux données. À cause de l'énorme volume de données produit (de l'ordre de 15 Pétaoctets par an) et de l'espace de stockage relativement limité au CERN (de l'ordre d'une ou deux journées de données produites), ce réseau et sa fiabilité sont critiques pour le fonctionnement du *LHC Computing Grid*[3] (LCG), l'infrastructure distribuée de calcul et de stockage mise en place dans le cadre de ce projet, et, par extension, pour les résultats des quatre expériences de physique qui en dépendent.

L'OPN a été construit grâce aux dernières évolutions des architectures des réseaux nationaux de la recherche (NRN). Il utilise des liaisons dédiées basées sur l'infrastructure en fibre noire disponible dans le réseau paneuropéen GÉANT2[4] et dans la majorité des NRN d'Europe, d'Amérique du Nord et d'Asie. La construction d'un tel réseau privé, relativement complexe par le nombre de liens et d'équipements le constituant, mais surtout par le nombre de domaines administrativement distincts impliqués dans les chemins, crée un grand nombre de contraintes au niveau opérationnel. La gestion quotidienne d'un tel réseau est sans doute une tâche banale pour un opérateur ou un NRN mais elle est lourde à mettre en œuvre pour un projet scientifique. Par ailleurs, la composante multi-domaines de ce réseau ajoute une problématique nouvelle et non-triviale à résoudre.

Dans cet article, nous proposons, après une rapide description de l'OPN, de lister les besoins opérationnels identifiés pour sa bonne marche quotidienne. Ensuite, nous exposerons les solutions qui ont été apportées pour répondre à ces contraintes. En guise de conclusion, nous identifierons les leçons apprises, qui pourront sans doute aider les projets ayant des besoins similaires de réseau privé.

2 Description de l'OPN

Les premières réflexions sur l'architecture de l'OPN ont commencé aux environs de 2003. À cette période, les NRN avaient massivement investi dans l'achat de fibres noires pour leurs besoins propres. Il semblait donc naturel de profiter de cette possibilité pour fournir à ce projet un

[1] http://lhc.web.cern.ch/lhc/

[2] http://cern.ch/

[3] http://lcg.web.cern.ch/LCG/

[4] http://www.geant2.net/

réseau haute-performance dédié, afin de répondre aux contraintes d'utilisation en termes de débit (de l'ordre de 4 Gbit/s inter-sites) et de disponibilité du service pendant le fonctionnement de l'accélérateur.

Ce réseau reliant le CERN aux onze autres centres de calcul est d'abord constitué de liaisons directes en étoile. Ensuite, pour assurer la fiabilité du réseau par de la redondance au niveau physique, des liens supplémentaires ont été ajoutés entre certains centres, dans la mesure des possibilités des réseaux sous-jacents. L'architecture est désormais telle que présentée à la figure 1. Les liens en trait plein figurent les liaisons actuellement opérationnelles et les liens en trait discontinu figurent les liaisons en cours de déploiement. La majorité des liens a une capacité de 10 Gbit/s ; les autres offrant une capacité moindre (mais toujours supérieure à 2 Gbit/s) sont susceptibles d'évoluer dans un très proche avenir au gré de l'amélioration des réseaux pour satisfaire les contraintes de performances.

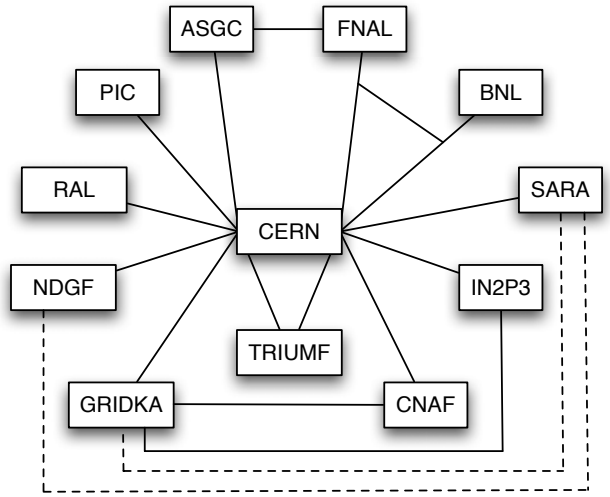

Figure 1 : Architecture logique de l'Optical Private Network.

Au-dessus de cette architecture de niveau liaison fournie par les NRN est construit un service de niveau réseau, chaque site fournissant un équipement de routage. Pour des raisons de redondance, le CERN possède deux équipements connectés. Le protocole de routage utilisé, BGP[5], permet d'utiliser au mieux la redondance mise en œuvre au niveau liaison. Ainsi, les sites interconnectés se servent mutuellement de secours en cas de problème sur les liens primaires, le changement de route étant assuré par le protocole BGP.

Une caractéristique importante de l'OPN est sa dimension multi-domaines. En effet, les liaisons inter-sites nécessitent la traversée de nombreux domaines administratifs distincts qui doivent collaborer, d'abord pour la mise en œuvre du service, puis pour son exploitation quotidienne. Les liens s'étendent, sauf cas particulier[6], sur au moins quatre domaines (pour les liaisons entre NRN limitrophes), cinq domaines pour les liaisons faisant intervenir le réseau GÉANT2 et plus pour les liaisons transatlantiques ou avec l'Asie. En tout, il y a environ 25 domaines indépendants impliqués dans l'OPN, avec par exemple, des procédures internes, des langues et des fuseaux horaires différents.

3 Les besoins opérationnels

Compte tenu du caractère critique de ce réseau dans le cadre de la bonne marche de l'infrastructure, des besoins ont été identifiés afin de définir un modèle opérationnel capable de satisfaire les utilisateurs. Ces contraintes peuvent être séparées en deux groupes, en terme d'infrastructure de supervision et en terme de support opérationnel.

Les besoins en termes de supervision sont les suivants :

- besoin d'une infrastructure capable de collecter et de présenter des informations sur le statut et le comportement (performances) du réseau au niveau physique et logique ;
- besoin d'un système capable de générer des alarmes en cas d'événements ou de suites d'événements prédéfinis observés par le système de supervision.

Ces besoins en terme d'outils sont des pré-requis indispensables à la bonne exploitation du réseau. En terme d'exploitation et de support, en plus des critères de qualité opérationnelle (comme les temps de réponse minimaux aux événements [2]), les besoins identifiés sont les suivants :

- besoin d'une entité opérationnelle qui « surveille » l'OPN (en utilisant les données collectées par l'infrastructure de supervision) et reçoit les alarmes ;
- besoin d'une entité opérationnelle qui réagit, selon les procédures établies, à la réception d'alarmes ou à la détection de comportements inattendus ;
- besoin d'une entité opérationnelle qui coordonne la résolution d'un problème entre les différents domaines impliqués ;
- besoin d'un moyen pour les entités opérationnelles et les « utilisateurs » de l'OPN de contacter une entité opérationnelle lorsqu'ils ont détecté un comportement inattendu ou inhabituel.

Le troisième point est rendu nécessaire par la composante multi-domaines du réseau : il est en effet primordial, lorsque de nombreux domaines sont impliqués dans un problème, qu'une entité soit « responsable » du suivi des actions entreprises jusqu'à la résolution et éviter qu'un problème reste non-résolu pour cause d'une mauvaise identification des responsables. Quant au quatrième point, il est important de noter que les « utilisateurs » de l'OPN sont en nombre limité et uniquement constitués de personnes responsables des transferts de données pour les expériences.

En plus de ces besoins principaux, notons aussi un certain nombre de besoins annexes, mais non-triviaux à satisfaire. D'abord, il est important que tous les interlocuteurs partagent un ensemble de termes afin d'éviter les incompréhensions : il est par exemple indispensable que les sites et des liens soient nommés de façon identique entre

[5] *Border Gateway Protocol*

[6] La liaison IN2P3-CERN est entièrement dans le domaine de Renater.

Domain	IN2P3		RENATER					CERN	
Link Structure	EP	◄·····	·····►	DP	◄———►	DP	◄·····	·····►	EP
Type	EndPoint	ID Part.Info	ID Part.Info	Demarc	Domain Link	Demarc	ID Part.Info	ID Part.Info	EndPoint
Local Name	**IN2P3-LHCOPN1**	IN2P3-CERN_LYON	RENATER-LYO-CERN-IN2P3	**RENATER-LYO**	RENATER-GEN-LYO	**RENATER-GEN**	RENATER-GEN-CERN	S513-C-BE7	**CERN-T0**
State Oper.	-	Up	Up	-	Up	-	Up	Up	-
State Admin.	-	Normal Oper.	Normal Oper.	-	Normal Oper.	-	Normal Oper.	Normal Oper.	-

Figure 2 : Visualisation du statut d'un lien et de ses segments

toutes les entités impliquées. Ensuite, un système commun de suivi des incidents et des requêtes peut être mis en place. La communication entre les différents systèmes de suivi utilisés peut se révéler être un point d'achoppement important : la normalisation, par exemple des modèles de données de tickets d'incident est encore balbutiante voire inexistante.

4 Les fonctions

Les fonctions clés ont été dérivées des besoins précédemment cités, toujours séparés en deux groupes. Nous ne traiterons pas ici des problèmes annexes de système de suivi d'incident ni de la mise en œuvre d'un système d'information global pour représenter la topologie du réseau, qui ne sont que des conséquences de la mise en place des fonctions suivantes. Nous ne détaillerons pas non plus les critères de qualité de l'exploitation qui ont principalement un impact sur les procédures et moins sur les fonctions.

4.1 Supervision

Deux outils principaux sont actuellement utilisés pour la supervision, l'un donnant une vision de l'état des liens jusqu'au niveau liaison, l'autre permettant d'évaluer l'état du réseau en terme de routage et de service.

L'OPN est actuellement composé de plus d'une vingtaine de liens, chacun composé en moyenne d'une dizaine de segments. Pour superviser ces liens, la solution retenue est celle de perfSONAR [3, 6], résultat d'une activité conjointe du projet GÉANT2, ESnet[7], Internet2[8] et RNP[9] pour fournir un outil de *monitoring* multi-domaines qui abstrait les différentes technologies employées dans chaque domaine. Chaque site ou domaine traversé installe des sondes ou utilisent des sondes déjà existantes qui vont collecter et agréger des métriques dans une base de données comme montré dans la figure 3.

On peut ensuite déterminer le statut des liens en interrogeant successivement les bases de données au sein des domaines traversés. Une centralisation des résultats est faite permettant de parcourir rapidement l'état des différents liens de manière transparente : les domaines impliqués dans la fourniture d'un lien sont initialement répertoriés avec les segments utilisés. Le statut de bout-en-bout peut ainsi être obtenu, sans se préoccuper des domaines traversés. En cas d'erreur, les segments et domaines concernés peuvent être aisément identifiés en analysant les métriques relatives aux différents segments composant le lien. Les résultats sont agrégés au sein d'une interface présentant les résultats par lien et par segment. Un exemple de statut obtenu est fourni à la figure 2. Des alarmes peuvent être positionnées sur certaines métriques afin de détecter automatiquement des anomalies.

L'OPN reposant sur de nombreux liens, la connaissance de leurs états n'est pas suffisante pour évaluer le service disponible. Il faut en effet pouvoir, à partir de leurs statuts, déterminer si le réseau est dans un état normal, par exemple en cas d'incidents sur des liens de secours ou ceux pour lesquels le trafic peut être rerouté. Sinon, l'impact sur le service délivré sera défini. Mais perfSONAR fournit l'état des liens sans se préoccuper de savoir si le lien est utilisé

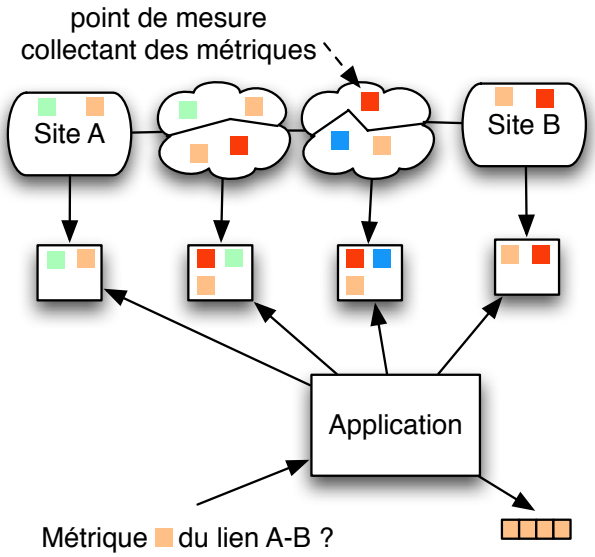

Figure 3 : Architecture de perfSONAR

ou non. Un lien de secours non utilisé mais en incident déclenchera quand même une alarme bien que ceci soit sans impact sur le service tant que le lien primaire reste fonctionnel. Il faut donc pouvoir différencier les fautes impactant le service ou non.

Pour cela, l'*EGEE Network Operation Centre*[10] (ENOC), a développé un outil permettant d'évaluer l'état de l'OPN au niveau IP, en particulier l'état de convergence du protocole de routage et quels sont les liens réellement utilisés à un instant donné pour acheminer le trafic IP.

Cet outil se base sur les tables de routage BGP des routeurs de chaque centre de ressources : elles sont régulièrement récupérées par SNMP[11], stockées, puis analysées afin de déterminer pour chaque site si les réseaux des sites distants peuvent être atteints et si oui par quels chemins. La table de

[7] http://www.es.net/

[8] http://www.internet2.edu/

[9] http://www.rnp.br/en/

[10] http://egee-sa2.web.cern.ch/egee-sa2/ENOC.html

[11] *Simple Network Management Protocol*

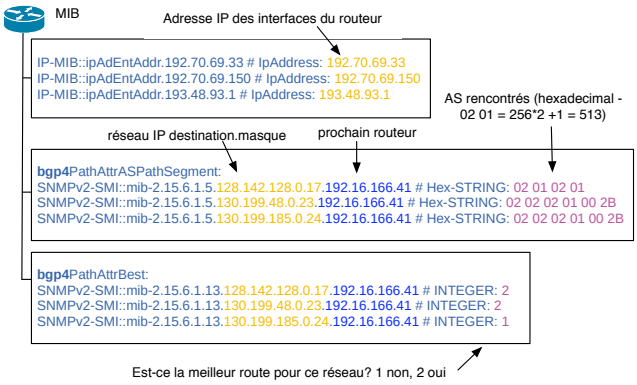

Figure 4 : Détail de l'analyse des routes BGP

routage indique en effet le prochain routeur sur le trajet et, en croisant successivement les informations des différents équipements interrogés, le chemin complet utilisé pour atteindre une destination est reconstitué. Les informations utilisées sont détaillées sur la figure 4.

Certains routeurs d'extrémité utilisés ne sont pas dédiés à l'OPN et leur table de routage BGP peut être assez volumineuse. Dans ce cas, les requêtes SNMP sont limitées aux routes concernant des réseaux de l'OPN. En moyenne par routeur est récupérée une soixantaine de ligne de la MIB[12] SNMP, ce qui garantit une requête rapide et peu consommatrice de ressource pour des équipements potentiellement fortement sollicités.

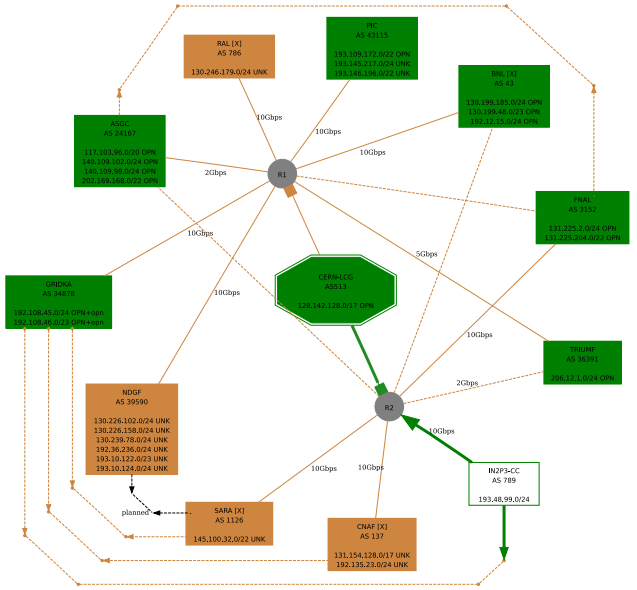

Figure 5 : Carte générée pour le site IN2P3-CC

Une carte par routeur (cf. figure 5) est ensuite générée, indiquant quels sont les autres sites accessibles. Les cartes sont stockées dans un format de description de graphes[13] au format texte permettant une analyse automatique, par exemple pour pouvoir déclencher des alarmes ou avoir un historique des problèmes. Il est ainsi possible de juger automatiquement ou non de l'impact de la perte de certains liens sur le routage et ainsi sur le service fourni.

Ces informations étant assez techniques et leur nombre ne permettant pas forcément une compréhension rapide, une vue synthétique est construite (cf. figure 6), permettant de juger instantanément quels sites sont atteints ou non au niveau IP. Par exemple, un site pourra être considéré joignable par un autre même si le lien principal entre ces deux sites est en incident dès lors qu'une solution alternative existe et est utilisée, par exemple en utilisant un lien de secours ou par rebond au travers de liens d'autres sites.

Cet outil se révèle être complémentaire des services fournis par perfSONAR, en particulier lorsque de nombreux liens et chemins de résilience sont disponibles. Ainsi, il permet d'abstraire la couche liaison et de mesurer uniquement le service fourni au niveau IP.

Finalement, ces deux outils combinés donnent, de manière automatisée, une évaluation précise de l'état du réseau et de ses éléments constitutifs tout en masquant l'hétérogénéité des domaines et des technologies utilisées. La supervision BGP permet de rapidement détecter des problèmes impactant le service et perfSONAR permet de déterminer précisément les incidents et leurs localisations. Ces informations indispensables servent de socle à une bonne exploitation du réseau.

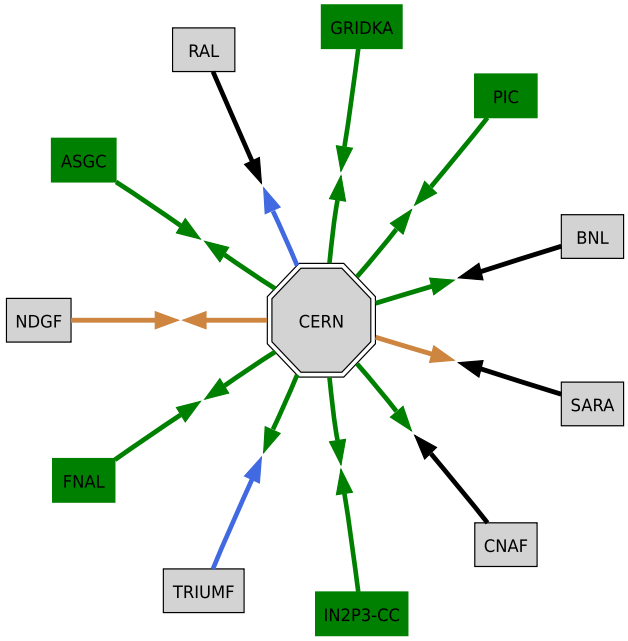

Figure 6: Vue synthétique de l'OPN

4.2 Coordination opérationnelle

En raison des nombreux acteurs impliqués dans la fourniture, la gestion et l'utilisation des liens, des entités de coordination sont apparues indispensables pour simplifier les flux d'information concernant la gestion des problèmes réseaux, par exemple en proposant des points de contact uniques et une centralisation des informations comme le présente la figure 7. En revanche, ces entités n'ont pas la responsabilité d'intervenir sur les équipements, ce rôle étant dévolu aux entités administrativement responsables dans les domaines concernés.

[12] *Management Information Base*

[13] *The DOT language, http://www.graphviz.org/doc/info/lang.html*

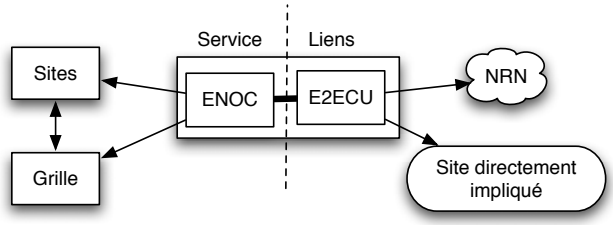

Figure 7 :Relations entre les différents acteurs

L'*End to End Coordination Unit* (E2ECU) [4] est une entité de coordination mise en place et opérée par Dante. Elle est responsable du bon fonctionnement des liens composant l'OPN. Sa proximité avec les fournisseurs de réseaux et son implication dans la mise en place des segments favorisent un suivi efficace des problèmes. Les informations concernant les éléments du réseau recueillies par le système perfSONAR déployé dans de nombreux domaines ainsi que dans certains sites sont centralisées et analysées. En cas d'alarme, l'E2ECU identifie et coordonne les entités impliquées pour restaurer l'état des liens en erreur dans les meilleurs délais. Un système de tickets est utilisé pour traiter automatiquement et suivre les alarmes remontées par perfSONAR ainsi que les requêtes des administrateurs de site.

L'*EGEE Network Operating Centre* (ENOC) est l'unité de support réseau du projet de grille de calcul EGEE[14] qui va être l'utilisateur majeur des données fournies par le LHC. En cas de problème impactant le service fourni par le réseau dédié, les conséquences seront importantes : les solutions de stockage temporaire fournies par le CERN pourraient devenir rapidement insuffisantes et l'accès à des données réparties dans différent sites deviendrait impossible. Il faut donc être capable d'évaluer précisément l'état du service fourni, et en cas de dégradation assurer un suivi rigoureux de l'incident afin d'avertir les utilisateurs des ressources à leur disposition.

Dans le cadre de l'OPN, l'ENOC est responsable de la connectivité au niveau IP entre les sites et d'aviser les utilisateurs des interruptions de service en cas d'incident ou de maintenance sur des segments, liens ou chemins qui impacteront les services fournis. Tous les événements affectant des éléments du réseau mais sans impact sur le service pourront être masqués aux utilisateurs et gérés de manière « silencieuse ». De cette façon, les utilisateurs ne sont pas noyés sous un flot d'information concernant des événements ne les affectant finalement pas. Cette réduction importante de la quantité d'information à destination des usagers permet d'améliorer sensiblement la gestion opérationnelle : tout message devient important.

Comme le souligne la figure 8, la détection des problèmes est faite par deux entités distinctes. Cette séparation est rendue nécessaire car des segments sont parfois utilisés par différents liens eux-mêmes utilisés par différents projets. L'E2ECU permet une mutualisation de leur résolution : les domaines impliqués auront un interlocuteur unique et ne seront pas contactés de multiple fois pour un même problème impactant de nombreux projets. Pour ces domaines, la communication du suivi d'incident s'en trouve

[14] *Enabling Grid for E-sciencE*, http://www.eu-egee.org/

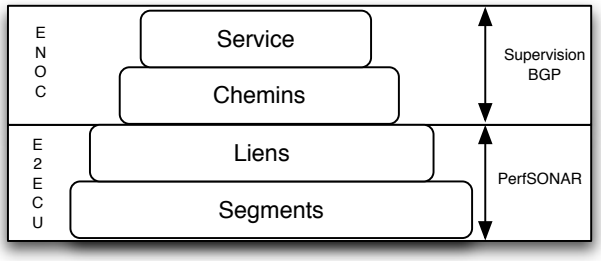

Figure 8 : Répartition de la détection des problèmes réseaux

grandement simplifiée, ainsi que pour les projets pour lesquels l'E2ECU est l'interlocuteur unique. La complexité du réseau devient cachée sans perdre en réactivité.

Les relations entre l'E2ECU et l'ENOC sont primordiales et se font principalement via le système de tickets mis en place par l'E2ECU. Ainsi les liens non opérationnels sont connus ainsi que l'état d'avancement de la résolution de leur problème. Si la supervision IP remonte un impact sur le service, l'ENOC va pouvoir vérifier que l'incident est géré par l'E2ECU, en connaître les causes et parfois obtenir une date de résolution prévue. L'ENOC communique alors ces informations via le système de support d'EGEE afin d'avertir tous les utilisateurs. Un système de hiérarchie de tickets a été mis en place afin que la clôture d'un ticket de l'E2ECU puisse fermer automatiquement les tickets qui en dépendent, en particulier les tickets EGEE relatifs à l'OPN. Le flux d'information en cas d'incident est présenté sur la figure 9.

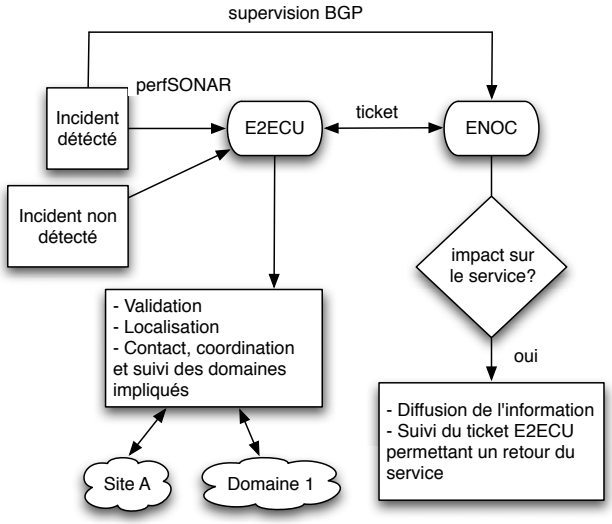

Figure 9 : Gestion des incidents

Dans le cas des maintenances, il faut être capable de prévoir le service qui perdurera pour savoir s'il faut avertir et qui. Dans tous les cas, un ticket E2ECU sera ouvert et en cas d'impact supposé sur le service, l'ENOC diffusera plus largement l'information. Les alarmes déclenchées durant une maintenance pourront ainsi être marquées comme déjà reliées à un événement existant. Le flux d'information en cas de maintenance est présenté sur la figure 10.

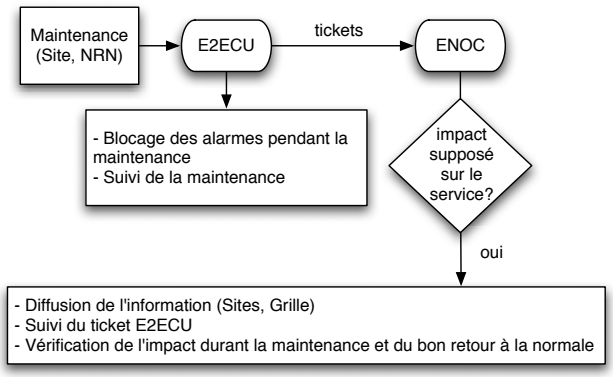

Figure 10 : Gestion des maintenances

Ainsi, les problématiques opérationnelles soulevées par la complexité et l'hétérogénéité des nombreux domaines et technologies utilisées pour ce réseau ont pu être résolues grâce à une répartition et une définition des tâches rigoureuse. La séparation de la gestion opérationnelle du réseau entre deux entités distinctes leur permet de se focaliser sur des tâches bien définies tout en assurant un cloisonnement des domaines de responsabilité et de compétence. Mais pour cela, les procédures et les échanges ont dû être précisément définis et optimisés afin de s'assurer que tout problème réseau déclenche une suite d'actions cohérente et que tous les acteurs en sont correctement et rapidement tenus informés. Pendant que l'E2ECU se focalise sur le bon fonctionnement des éléments constitutifs du réseau, l'ENOC s'assure que ces éléments sont utilisés au mieux pour fournir un service fiable et performant. Il servira aussi d'interface avec les utilisateurs de l'OPN, pour les problèmes de performances par exemple.

5 Conclusion

En plus des défis techniques que présente l'OPN, sa gestion opérationnelle est rendue très difficile en raison des nombreuses entités y jouant un rôle ainsi que par le nombre d'équipements hétérogènes utilisés. Si ce travail coordonné entre les différents acteurs a permis de bâtir un réseau privé mondial d'une telle envergure, sa force en fait sa faiblesse : les problèmes opérationnels doivent s'accommoder du grand nombre d'entités sollicitées. De plus, la criticité du réseau nécessite une gestion opérationnelle sans faille qui permette de tirer le meilleur parti de l'infrastructure.

Les besoins opérationnels en terme d'infrastructure ont été résolus par le déploiement de perfSONAR et l'utilisation de supervision BGP. En termes de support opérationnel, la création de l'E2ECU a permis la supervision et le suivi des problèmes réseau multi-domaines tandis que l'ENOC est capable d'évaluer le service disponible et d'assurer un suivi des problèmes l'impactant, tout en servant d'interface avec les « utilisateurs ». Cette séparation des responsabilités et des rôles a autorisé la réduction au strict minimum des flux échangés. Les relations entre l'ENOC et l'E2ECU sont un élément crucial et la mise au point de procédures détaillées définissant leur étroite coopération permet d'assurer la bonne gestion opérationnelle du réseau.

La complexité du réseau est largement cachée aux utilisateurs et seuls les impacts majeurs sur le service seront communiqués : le flux d'information à leur destination est réduit aux éléments importants, chose indispensable lorsque un réseau repose sur les services fournis conjointement par plus de 25 domaines et que le volume d'information échangé devient rapidement très important.

Les problématiques rencontrées et les solutions qui furent apportées ont montré que la gestion quotidienne d'un tel réseau ne doit pas être sous-estimée. Au delà de la fiabilité technique, les tâches opérationnelles contribuent grandement à la bonne marche du réseau et doivent garantir un suivi optimal des problèmes dans le but de minimiser leur durée.

Néanmoins la formalisation et la rationalisation des procédures doivent sans cesse être améliorées. Au delà de l'implémentation actuelle, il faut dégager les objectifs, les rôles, les comportements et responsabilités de chacun lors de chaque événement possible (incident, maintenance et évolution du réseau). Il faut également penser aux métriques, aux indicateurs, à leurs mesures et aux comptes-rendus périodiques. Cette tâche lourde, actuellement conduite, reste indispensable pour parvenir à un modèle opérationnel fiable, au delà de la technique pure, sur lesquels les utilisateurs pourront compter en cas d'incident qui, inévitablement, ne manquera pas de mettre à mal la bonne marche du réseau et donc de l'infrastructure.

Finalement, si la solution des liaisons dédiées est très attirante pour un projet ou une communauté, elle induit un certain nombre de conséquences à ne pas négliger, notamment au niveau opérationnel. Evidemment, s'il s'agit d'un ou deux liens, fournis par le même NRN, des solutions simples sont envisageables. En revanche, dès que les liens se multiplient, traversant de nombreux domaines administratifs, il est important de mettre en place dès le départ, des structures adéquates, tant au niveau supervision qu'au niveau support opérationnel. Il est intéressant de noter que, désormais, l'existence de l'E2ECU au niveau de GÉANT2 facilite le travail des futurs projets qui pourront s'appuyer sur cette interface pour construire leur propre modèle.

Bibliographie

[1] Edoardo Martelli et al., LHC Optical Private Network. https://twiki.cern.ch/twiki/bin/view/LHCOPN.

[2] David Jacobs, WLCG Memorandum of Understanding. http://lcg.web.cern.ch/LCG/C-RRB/MoU/WLCGMoU.pdf, août 2007.

[3] *PerfSONAR – PERFormance Service-Oriented Network monitoring Architecture*, http://www.perfsonar.net/.

[4] Emma Apted, E2ECU support for the LHCOPN, http://www.dante.net/upload/pdf/E2ECU_LHC_OPN_Presentation.pdf

[5] Jérôme Bernier, Utilisation haut débit des nouvelles infrastructures réseaux de la recherche, *JRES2007*, novembre 2007

[6] Nicolas Simar, Frédéric Loui, Perfsonar – Supervision réseau Multi-domaines, *JRES2007*, novembre 2007