La gestion des réseaux informatiques d'un site industriel classé Seveso seuil haut : proposition d'une méthode

Christophe Robin

le cnam

CONSERVATOIRE NATIONAL DES ARTS ET MÉTIERS

PARIS

Mémoire présenté en vue d'obtenir
le diplôme d'ingénieur CNAM
Spécialité : INFORMATIQUE

par

Christophe ROBIN

La gestion des réseaux informatiques d'un site industriel classé Seveso seuil haut : proposition d'une méthode

Soutenu le 04 janvier 2012

JURY
PRESIDENT : J. Akoka — Professeur CNAM
MEMBRES :
I. Wattiau — Professeur des universités — CNAM
J.-M. Lecornec — Directeur commercial — Ipsilan-Networks
S. Lefébure — Chef du service Système — Total - Raffinerie de Grandpuits
N. Lammari — Maître de conférences — CNAM

Remerciements

De nombreuses personnes ont contribué au long processus dont ce travail est l'aboutissement.

Ipsilan-Networks a encouragé et financé la formation.
Total Trading & Shipping a soutenu le début de cette démarche.
Total Raffinage & Marketing—Raffinerie de Grandpuits et établissement pétrolier de Gargenville a prolongé cet effort et a autorisé et financé la réalisation de ce projet.

I. Wattiau m'a apporté une aide très précieuse lors de la rédaction de ce document et de la préparation de la soutenance associée.

Étudier au CNAM est un projet familial. Ma famille a su me soutenir, m'encourager et me supporter sans jamais défaillir durant ces longues années. Sans l'assistance quotidienne d'Emmanuelle, ce projet n'aurait jamais pu être réalisé.

Gaëlle partagea mes efforts et supporta mes défauts. Son intelligence, sa gentillesse, sa patience et ses nombreuses autres qualités ne connaissent ni limites ni pareilles.

Fadwa, Christophe et Pierre, compagnons de CNAM, partagèrent mes difficultés. L'assistance mutuelle que nous nous portons rendit ces épreuves supportables.

Laurence, Peggy, Sandrine, Vaïana, Cédric, Jérémy et Thomas eurent la patience de relire et de commenter ce document.

Beaucoup d'anonymes m'apportèrent une aide précieuse au cours de ces cinq années, parfois de manière inconsciente.

«Merci» est loin d'exprimer toute la gratitude et la reconnaissance que je ressens à votre égard.

I keep six honest serving-men
(They taught me all I knew);
Their names are What and Why and When
And How and Where and Who.

Rudyard Kipling [14]

{J'entretiens six honnêtes serviteurs
(Ils m'enseignèrent tout ce que j'appris);
Leurs noms sont Quoi et Pourquoi et Quand
Et Comment et Où et Qui.}

TABLE DES MATIÈRES

GLOSSAIRE

Les termes soulignés dans le texte sont définis ici. Les chiffres entre crochets [x] renvoient à la bibliographie

1. Termes généraux

Terme	Définition
Directive Seveso	Directive 96/82/CE. Directive européenne imposant aux états d'identifier les sites industriels présentant des risques d'accidents majeurs. Il existe deux niveaux de classification : le « seuil bas » (543 sites en France en 2005) et le « seuil haut » (670 sites en France en 2005). Le niveau est déterminé en fonction de la quantité de matières dangereuses présentes sur le site.
DRIEE	Direction Régionale et Interdépartementale de l'Environnement et de l'Énergie. Autorité de tutelle des sites Seveso situés en Ile-de-France, placée sous la responsabilité du préfet. Elle procède régulièrement à des inspections de site et procède au classement Seveso.
Seveso	Commune d'Italie victime d'un accident industriel. Un nuage chargé de Dioxine s'est échappé d'une usine voisine le 10 juillet 1976 et a durablement contaminé les humains, les animaux et l'environnement.
SNCC	Système numérique de conduite et de contrôle. Nom complet du système de conduite
Système de conduite	Système combinant des ordinateurs et des automates. Il est utilisé pour la conduite de la production, c'est-à-dire l'action sur les éléments physiques (vannes, pompes...) en fonction de contraintes. Il comprend également la collection de valeurs depuis des capteurs (température, pression...)

2. Termes informatiques

Terme français	Terme anglais	Définition
Commutateur	Switch	Équipement informatique constituant un LAN. Il sait acheminer les informations de diffusion.
Diffusion	Broadcast	Émission d'une requête à destination de l'ensemble des machines présentes sur le réseau. Cette technique permet de contacter la machine destinataire sans en connaître la localisation par avance. La diffusion induit une charge importante de la bande passante du réseau et doit être utilisée avec parcimonie
ITIL	ITIL	Information Technology Infrastructure Library. Référentiel de bonnes pratiques pour les services informatiques. Dans sa version la plus récente, il couvre les aspects de conception, de transition et d'opération des services dans le cadre d'une stratégie.
Modèle IP	IP Model	Modèle de communication entre systèmes via un réseau basé sur le protocole IP. Il a été généralisé par le modèle OSI
Modèle OSI	OSI Model	Modèle de communication (norme NF EN ISO/CEI 7498[1]) entre systèmes via un réseau, indépendant des protocoles utilisés. C'est un empilement de couches abstraites. Il est destiné à faciliter la communication entre systèmes hétérogènes par une normalisation des services rendus par chaque couche.
Pare-feu	Firewall	Équipement informatique assimilable à un routeur intelligent. Il peut filtrer le trafic selon des règles et restreindre ainsi la communication entre deux réseaux. C'est un équipement participant à la mise en place de la politique de sécurité.

Terme français	Terme anglais	Définition
Réseau local	LAN	Domaine de diffusion. Dans un réseau local, chaque machine peut dialoguer avec d'autres machines, situées sur le même réseau ou sur un autre réseau. Cependant, les informations de diffusion ne quittent pas le réseau local et permettent de définir un périmètre conceptuel.
RJ-45	RJ-45	Connecteur destiné aux câblages d'extrémité pour des transports de courants faibles. Il est utilisé dans les réseaux informatiques et téléphonique.
Routeur	Router	Équipement informatique capable d'interconnecter deux réseaux. Il est à la base du fonctionnement d'internet, par exemple. Il délimite un LAN. Il ne relaie pas les informations de diffusion.
Supervision	Supervision	Contrôle du bon fonctionnement de systèmes. Contrairement à la surveillance, il n'est pas question de mesurer des grandeurs relatives à des seuils mais de s'assurer qu'une fonction est disponible ou non. Chaque changement d'état produit une alerte.
Surveillance	Monitoring	Action de contrôler en continu et en temps réel la valeur de paramètres. Cette surveillance peut inclure un système d'alerte déclenché lors de l'atteinte d'un seuil.
Urbanisation	IT Urbanisation	Méthode de modélisation des ressources informatiques de l'entreprise. Elle permet de vérifier la cohérence (l'alignement stratégique) entre les besoins des utilisateurs et les moyens techniques mis en place pour y répondre.

Introduction

Les réseaux de télécommunication sont partout. Depuis l'invention du télégraphe de Chappe au XVIII^{e} siècle la transmission d'information sur de longues distances à constamment évolué pour satisfaire les attentes des utilisateurs. Les réseaux informatiques, apparus dans les années 1970, ont permis la « révolution Internet » et l'apparition du concept de « village planétaire ».

Cependant, l'appellation générique « réseaux informatiques » recouvre une grande diversité de technologies et de performances. Les besoins des utilisateurs, les contraintes de coût et la nature des informations à transporter ont abouti à une jungle de solutions. Alors que la confiance dans les réseaux informatiques grandit (on n'hésite plus à placer ses données sensibles dans le « nuage » Internet) le besoin de gérer au mieux cette ressource devenue stratégique s'impose.

Dans une entreprise, le « réseau » fait partie intégrante de la production. Les échanges d'information à l'intérieur et à l'extérieur des murs de l'entreprise ne sont plus possibles sans ces infrastructures. Dans une entreprise industrielle, les machines utilisées sont le plus souvent à commande numérique. Dans une raffinerie de pétrole, l'ensemble de l'usine est géré grâce à des commandes déportées. Sur une telle installation, classée Seveso seuil haut (Seveso II), la gestion du réseau est primordiale pour assurer une maîtrise efficace du risque industriel.

Que signifie gérer un réseau informatique ? Comment assurer une gestion sûre et efficiente ? À ces questions, il n'existe pas pour l'heure de réponse standard. Pourtant, alors que l'importance des réseaux informatiques dans les activités professionnelles et personnelles grandit chaque jour, répondre rapidement à ces questions est indispensable.

Ce projet, au travers de la production d'une documentation exhaustive des ressources « réseau » de la raffinerie de l'Ile de France, souhaite proposer une approche du problème de la gestion des réseaux dans des environnements à forte contrainte de sécurité. En abordant la gestion sous l'angle des objectifs, puis de la connaissance de l'existant et enfin de la stratégie pour rallier l'existant aux objectifs, il s'agit de s'appuyer sur des référentiels reconnus pour gérer des ressources clefs de l'entreprise.

1. Les entreprises participant au projet

Ce projet est réalisé par la société Ipsilan-Networks pour le compte de la raffinerie de Grandpuits, filiale du groupe Total. Ces deux entreprises entretiennent un partenariat depuis de longues années sur les aspects réseaux et téléphonie.

1.1. Ipsilan-Networks

Société spécialisée depuis plus de dix ans dans la conception et la mise en place de réseaux informatiques, Ipsilan-Networks (Ipsilan) a étendu sa gamme de services à la fourniture de systèmes d'information complets, depuis les infrastructures jusqu'à la délégation du personnel qui en assure la gestion.

Ipsilan compte environ cinquante personnes et maintient un rythme de croissance en personnels de 10 à 15 % par an depuis plus de cinq ans. La société met l'accent sur la qualité des prestations au travers de nombreuses actions de tutorat d'apprentis, de formation continue des salariés et d'accompagnement sur les nouvelles technologies. C'est dans cette politique d'évolution continue que s'inscrit le soutien humain, technique et financier qu'Ipsilan fournit à ses salariés ayant choisi de suivre une formation au CNAM.

L'expertise développée depuis sa création associée à la faible rotation du personnel a permis à cette toute petite structure de se tailler une place de choix auprès de grand comptes soucieux de la qualité des ressources informatiques qu'ils achètent.

1.2. Total

1.2.1. Le groupe Total

Total est le cinquième groupe pétrolier intégré au monde par sa capitalisation boursière. Il est dit « intégré » car ses activités portent sur l'ensemble de la chaîne de production de produits pétroliers, depuis l'exploration jusqu'à la distribution de produits finis. Le Groupe produit également de l'énergie électrique d'origine éolienne ou photovoltaïque. Son siège est situé à Paris mais ses activités s'étendent sur tous les continents. Le groupe Total a segmenté ses activités en cinq branches : l'exploration et la production, le trading et le shipping, le raffinage et le marketing (R&M) et la chimie, le tout supervisé par une holding. La division R&M a elle-même des activités dans le

monde entier au travers de raffineries (notamment une des plus grande au monde à Jubail en Arabie Saoudite) et de réseaux de distribution sous de multiples marques (par exemple en France : Total, Elf, Elan, AS24...).

1.2.2. La raffinerie de l'Ile de France

Inaugurée par le premier ministre Pompidou en 1967, la raffinerie de Grandpuits (Seine et Marne) s'est toujours distinguée par sa culture d'innovation. Ainsi elle s'adapte régulièrement à son environnement en modifiant l'outil de production : les installations ou modifications d'unités de production permettent de satisfaire les besoins des clients et de limiter l'empreinte environnementale de l'usine.

La raffinerie fait également figure de précurseur dans le domaine informatique : en 1977, elle a été la première raffinerie en France à adopter un système de pilotage couplant informatique et automatique. Elle a également été la première installation industrielle du groupe Total à disposer d'un système de téléphonie sur IP et elle est actuellement pilote sur un projet d'infogérance des infrastructures bureautiques pour l'ensemble de la branche R&M.

Cette ouverture aux nouvelles technologies se fait cependant avec beaucoup de prudence. Pour qu'une nouveauté soit mise en production sur le site, il faut en démontrer la fiabilité afin de ne pas mettre en péril le fonctionnement de l'usine par un changement. Cette culture a conduit les informaticiens à fonctionner en mode « projet », c'est-à-dire à aborder les changements de manière construite, en anticipant les risques et en préparant les opérations de manière minutieuse selon une méthode rigoureuse. Cependant, cette méthode manque de formalisation car les équipes sont très restreintes, ce qui incite à avoir « tout dans la tête » et pénalise l'aspect documentation des projets.

2. Le contexte

2.1. L'historique des réseaux du site

La raffinerie de l'Ile de France a certes toujours été un précurseur dans l'adoption des nouvelles technologies mais les réseaux de communication ont été déployés au fur et à mesure des besoins, sans réelle stratégie. Cela a conduit à des installations hétérogènes, partielles et parfois incompatibles. Ainsi il existe une séparation politique entre les réseaux dédiés aux automates et ceux d'un usage plus général. Cependant, cette situation n'a plus réellement de sens aujourd'hui : les automates sont maintenant

des ordinateurs et la distinction entre un réseau d'automates et un réseau d'ordinateurs est factice.

Les réseaux furent sous la responsabilité d'équipes différentes, en fonction de leurs finalités. Le réseau téléphonique, le premier mis en place sur le site, était du ressort des électriciens. Le réseau des automates, installé parallèlement au système de conduite, fut géré par les automaticiens. Le réseau informatique bureautique, à sa création dans les années 1990, fut confié à des informaticiens.

Lors de l'installation du système de téléphonie sur IP au milieu des années 2000, les informaticiens héritèrent la gestion des lignes téléphoniques du réseau analogique dont les électriciens furent alors débarrassés. Cependant, la gestion des ressources entre les automaticiens et les informaticiens restait séparée.

Avec le temps, il devint de plus en plus évident que séparer les réseaux conduisait à des problèmes de gestion : les capacités installées étaient sous-évaluées, les ressources n'étaient pas partagées et la documentation associée disparaissait ou devenait inexploitable par manque de mise à jour.

Le service Systèmes de la raffinerie de Grandpuits a donc décidé d'unifier la gestion de l'ensemble des réseaux de communication, quelle que soit leur finalité, pour la confier à l'administrateur réseau du site.

Cependant, les services chargés des différents réseaux avaient chacun leur méthode de documentation. Lors des changements d'attribution de la responsabilité des réseaux, ces documents ont été transmis, souvent de manière partielle et toujours de manière informelle. De plus, la forme de ces documents étant très éloignée de celle maîtrisée par l'équipe qui les récupérait, ces informations ne furent que rarement exploitées et jamais mises à jour. C'est pourquoi, alors qu'il existe aujourd'hui pléthore de documents portant sur les réseaux de la raffinerie, ils sont peu ou pas exploitables.

2.2. L'exigence permanente de sécurité en raffinerie

2.2.1. Les dangers

Une raffinerie est une collection de réservoirs (*bacs*, *sphères*), de réacteurs (*unités*) et de tuyaux (*pipelines*, *lignes*... selon l'usage). Tous ces éléments contiennent des hydrocarbures : du pétrole brut en entrée, des produits raffinés issus de la transformation de ce pétrole brut en sortie. Le traitement de ce pétrole brut est appelé *procédé*. Ce procédé présente un certain nombre de dangers. Des hydrocarbures

risquent d'être répandus accidentellement, des gaz toxiques générés par le procédé peuvent être relâchés... Un bref inventaire des risques liés à quelques substances présentes sur le site est présenté ci-après :

Tableau I : quelques substances dangereuses présentes sur le site et risques associés

Substance	Risque associé
Hydrocarbures et notamment HAP (hydrocarbures aromatiques polycycliques)	Incendie / Explosion / Intoxication / Empoisonnement / Maladies liées aux composants CMR (cancérogènes, mutagènes, reprotoxiques) / Asphyxie
Azote	Anoxie / Brûlure thermique froide
H2S (hydrogène sulfuré / sulfure d'hydrogène)	Anoxie / Explosion
Benzène	Maladies liées aux composants CMR (cancérogènes / mutagènes / reprotoxiques)
HF (acide fluorhydrique)	Brulûre chimique (l'acide traverse la peau et s'attaque directement et rapidement aux os)
Sources radioactives	Maladies liées aux composants CMR (cancérogènes / mutagènes / reprotoxiques)

Toutes ces substances engendrent, pour le personnel sur site, les populations voisines et l'environnement, des risques pouvant mener à l'accident grave (terme pudique pour désigner le décès sur le lieu de travail). Le maître mot du travail en raffinerie est donc « Sécurité ».

2.2.2. La gestion des risques

La maîtrise de ces risques passe par l'aménagement des conditions de travail et des comportements individuels et collectifs. Les entreprises sous-traitantes font l'objet d'une surveillance particulière car elles représentent plus de la moitié des personnes présentes sur le site.

Ainsi, les Entreprises Extérieures (EE) doivent, avant d'être autorisées à travailler, constituer un dossier d'entreprise recensant l'ensemble des activités que l'EE

effectuera sur le site, les risques associés à ces activités et les mesures compensatoires que l'entreprise s'engage à mettre en œuvre.

De plus, chaque personne d'une EE intervenant sur le site doit suivre une formation particulière qui permet à son employeur de lui délivrer une habilitation au travail sur les sites chimiques et pétrochimiques. Cette habilitation, de niveau 1, est nécessaire pour être autorisé à travailler sur le site. Les chefs d'équipe, ou dans le cas d'un travailleur détaché individuellement le membre de l'EE, doivent recevoir une habilitation de niveau 2 leur permettant de remplir les formalités autorisant chaque activité sur le site. Ces habilitations sont à renouveler tous les quatre ans. En complément, une sensibilisation aux risques spécifiques au site et aux comportements à adopter est assurée par le service Sécurité (les pompiers) du site. Cet « accueil sécurité » est conclu par un questionnaire test. Pour être autorisé à travailler à l'intérieur de la raffinerie, il est nécessaire de fournir plus de la moitié des réponses justes. Cet examen est valable deux ans.

Une autorisation de travail doit être établie entre Total et l'EE pour autoriser les travaux, identifier les risques spécifiques à ces activités et les mesures à prendre par chaque acteur. Cette autorisation pouvant être délivrée pour des travaux s'étalant sur plusieurs jours, un bon de validation établi quotidiennement recense les tâches du jour, et encore une fois, précise les risques présents et les mesures à adopter.

L'ensemble de ces mesures est destiné à prévenir les risques liés à de mauvais comportements ou à une mauvaise coordination des différentes activités sur le site (risques de co-activité). Ce sont des procédures contraignantes mais structurantes qui obligent à planifier les activités (les bons de validation sont signés la veille pour les travaux du lendemain) et à réfléchir avant d'agir, même si cela consomme beaucoup de temps : il est impossible d'agir dans l'instant.

Enfin, chaque personne présente sur le site doit, au moins une fois par an, suivre « l'école à feu », un stage d'une demi-journée consacré à la lutte anti-incendie et dont le point culminant est l'exercice pratique individuel d'extinction d'un feu d'hydrocarbure à l'aide d'un extincteur. Cet exercice rappelle les règles de sécurité en vigueur sur le site et encourage l'ensemble du personnel, quelle que soit son entreprise d'appartenance, à les appliquer au quotidien.

La sécurité est donc au cœur de ce projet comme de l'ensemble des activités sur le site. Elle est souvent vécue au quotidien comme une contrainte mais permet également de travailler sereinement.

3. Les travaux en raffinerie : l'exemple du passage de câble

Travailler en raffinerie est complexe. Voici l'exemple des étapes nécessaires au passage d'un câble entre deux bâtiments : une fibre optique.

Sur un site normal, passer une fibre optique nécessite de commander une fibre standard, de l'acheminer dans une gaine (un fourreau) reliant les deux bâtiments et de sertir les connecteurs. En raffinerie, la fibre optique est fabriquée à la demande (minimum mille mètres) car elle nécessite une sur-gaine particulière pour résister à d'éventuels contacts avec des hydrocarbures. Elle coûte donc très cher et nécessite un délai d'environ deux mois pour sa fabrication.

Ensuite, l'usage des fourreaux est prohibé en raffinerie : si des hydrocarbures venaient à s'infiltrer dans le sol ils pourraient s'accumuler dans les cavités formées par les fourreaux, créant des accumulations de substances explosives. Ainsi, tout câble est enfoui au moyen d'une tranchée (une *fouille*). Ce câble est donc « perdu » dans le sol et ne sera jamais retiré. Creuser une fouille nécessite un permis particulier associé à une autorisation de travail. Il faut prendre des précautions pour ne pas endommager lors du creusement les éventuels liens ou tuyaux déjà enfouis mais également se méfier de l'accumulation de gaz dans la tranchée. En effet, le gaz le plus dangereux et le plus répandu est le H_2S (sulfure d'hydrogène ou hydrogène sulfuré) qui a la particularité d'être plus lourd que l'air et extrêmement toxique. Toute personne devant travailler dans une fouille doit donc effectuer des contrôles d'atmosphère avant et pendant son intervention et être accompagnée.

La pose d'un lien entre deux bâtiments ne peut donc prendre moins de six mois. La moindre tranchée est très onéreuse : cette dépense doit être planifiée. C'est pourquoi tout projet nécessitant une extension du réseau de la raffinerie est toujours très long et très cher.

Justifier ces investissements peut être ardu. Sans l'aide d'un plan à long terme pour en démontrer l'utilité, ces installations sont souvent pratiquées selon des procédures d'urgence et génèrent de facto des tensions nuisant à la qualité de la réalisation. Ce projet doit donc, en donnant une vision à long terme des investissements nécessaires, permettre de justifier ces projets d'extension des réseaux et faciliter leur financement.

4. L'objet du projet : les réseaux de la raffinerie

4.1. Pourquoi plusieurs réseaux ?

Les réseaux informatiques doivent apporter des solutions à des problèmes opérationnels soulevés par les clients. Ces besoins de communication sont divers et appellent des réponses différentes. Ainsi, sur la raffinerie, plusieurs réseaux informatiques cohabitent. S'ils sont basés sur des technologies comparables, voire même identiques, ils n'en sont pas moins distincts dans leurs finalités et donc leurs architectures. Les réseaux sont donc regroupés en périmètres, chaque périmètre répondant à un besoin particulier. Il existe un périmètre bureautique pour lequel la priorité est donnée à la performance, un périmètre industriel où priment disponibilité et intégrité et enfin un périmètre pour les entreprises extérieures sur lequel pèsent beaucoup moins de contraintes.

La sécurité influe également sur la segmentation en plusieurs réseaux. La restriction d'accès est une manière de répondre efficacement aux besoins de sécurité. S'il est impossible d'accéder à une ressource, alors il est impossible de l'altérer. Ainsi, le partage en périmètre facilite la mise en sécurité des informations. De plus, les « portes d'entrée » de ces périmètres sont clairement identifiées et disposent de « vigiles » capables de ne laisser pénétrer que les individus ou trafics autorisés. Ainsi, les réseaux aident à constituer des « bunkers » étanches et protégés.

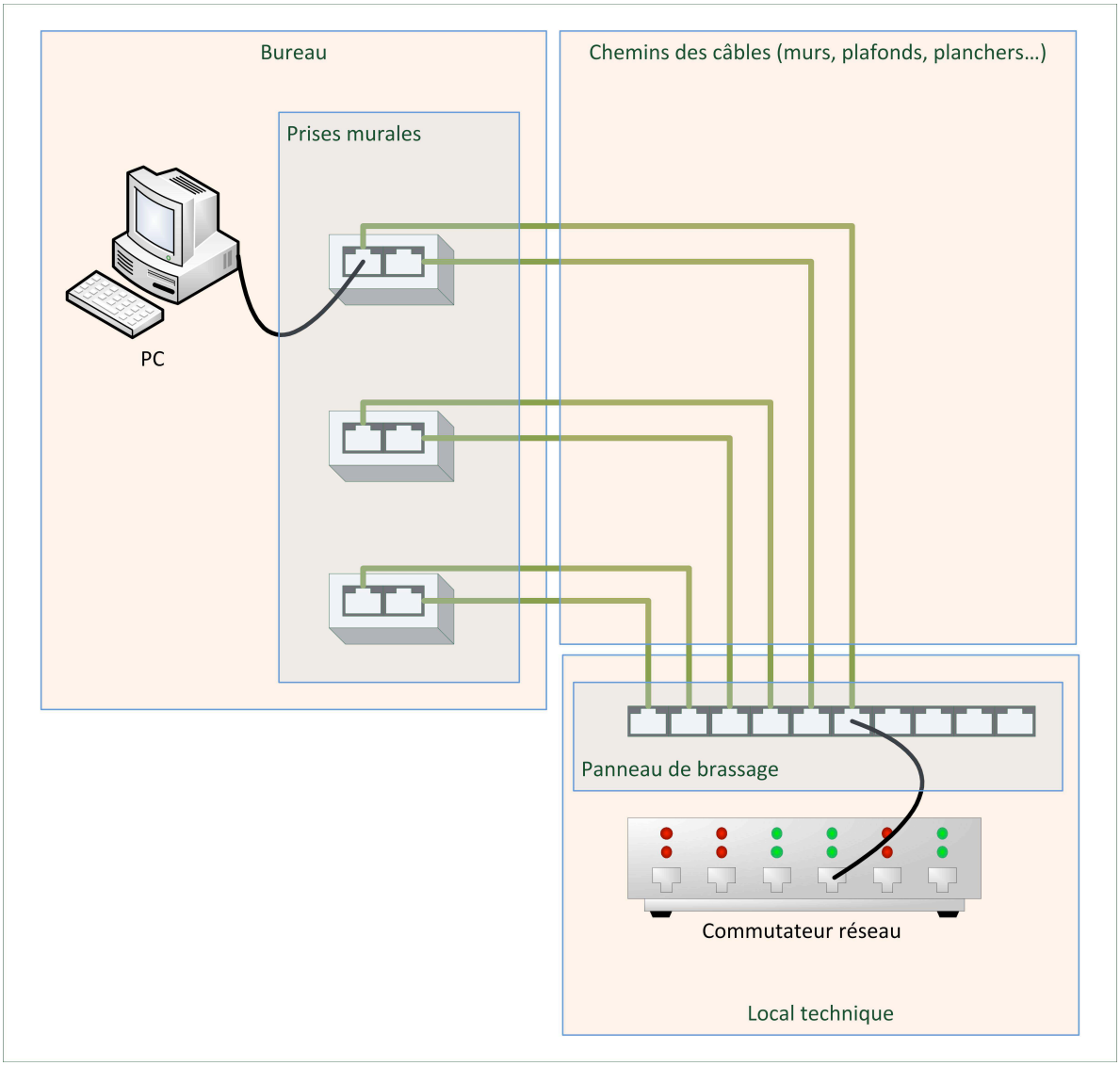
4.2. Quels équipements dans un réseau ?

Un réseau est un ensemble de nœuds reliés par des liens. Ces nœuds peuvent être destinés à simplement acheminer le trafic sans se soucier de sa nature : ce sont des commutateurs. Le périmètre constitué par un ensemble de commutateurs est étanche et ne sait pas communiquer avec d'autres périmètres. D'autres équipements servent à interconnecter ces périmètres. On parle alors de routeurs. Ils ont une connexion dans chaque périmètre qu'ils interconnectent. Ils échangent entre eux des informations sur les différents périmètres qu'ils connaissent, afin de constituer des « routes », chemins que les informations empruntent pour aller d'un périmètre à l'autre, sans que ces périmètres ne soient nécessairement contigus.

Le raccordement d'un élément périphérique (PC, téléphone, serveur...) à un réseau nécessite que ce dernier propose une « prise » standard. Dans le cas des réseaux sans fils, cette prise est intangible mais bien présente. Sur un site où les connexions se font par câble, cette prise se présente sous la forme d'un connecteur mural au

standard RJ-45. Derrière cette prise se trouve un câble qui chemine dans les murs, les plafonds et les planchers des pièces jusqu'au local technique où se trouve le commutateur réseau du bâtiment. Cependant, il est inutile de raccorder tous les câbles directement au commutateur. En effet, selon les lieux, seule une prise sur trois ou quatre est réellement utilisée, les autres étant des réserves : il est moins coûteux de poser de nombreuses prises dans les bureaux lors d'une seule installation plutôt que de le faire à la demande. Il faut donc procéder à une opération de raccordement dans le local technique entre le commutateur et la prise murale que l'on souhaite utiliser. Cette opération est nommée « brassage ».

Le câblage réseau d'un bâtiment se présente donc ainsi :



Principe du câblage réseau d'un bâtiment

Ce schéma ne représente pas l'interconnexion entre les commutateurs constituant l'ensemble du réseau. En effet, ces interconnexions sont réalisées sur le même principe en exploitant des liaisons entre les bâtiments. Sur ce schéma, il est clair que brasser l'ensemble des prises posées conduit à mettre en place un commutateur supplémentaire et augmente d'autant le coût de l'installation. Les proportions ne sont pas respectées : en général : les locaux techniques proposent une prise de commutateur pour trois prises murales. Cependant, dans certains locaux très densément peuplés, cette proportion tombe à moins d'une pour deux.

L'arrivée de postes téléphoniques connectés au réseau informatique — téléphones « IP » — a causé beaucoup d'inquiétudes concernant les besoins en câblage. Pour éviter de devoir multiplier le nombre de prises nécessaires sur les commutateurs, les téléphones IP d'entreprise embarquent un micro-commutateur : ils ne nécessitent qu'une seule prise sur le commutateur et servent de relais à la connexion réseau du PC. Le poste téléphonique est donc l'intermédiaire imposé pour la connexion du PC au réseau local. Le schéma de connexion au réseau dans un bureau est donc le suivant :

Schéma de connexion au réseau dans les bureaux

Dans l'ensemble du groupe Total, les équipements réseau, commutateurs et routeurs, sont tous fabriqués par une seule entreprise : Cisco. Cette uniformité, basée sur un contrat cadre accordant des conditions d'achat extrêmement avantageuses au Groupe en contrepartie de l'exclusivité d'approvisionnement, est gage de fiabilité. Ce contrat a mis un terme à des années d'achats anarchiques basés sur des critères de prix ayant abouti à une diversité excessive des équipements réseau. Or l'uniformité, même si elle

est synonyme de perte de liberté, aide grandement dans la gestion des réseaux et apporte des gains de productivité importants : il n'est plus nécessaire de procéder à des appels d'offre, l'installation et le support des équipements sont standards et prennent peu de temps et la compatibilité entre équipements n'est plus un problème. Cependant, le risque d'incident majeur provoqué par un problème généralisé à l'ensemble des équipements de la marque ne peut être écarté. Pour s'en prémunir, seuls les équipements validés par l'équipe informatique centrale du Groupe figurent dans le contrat cadre et bénéficient d'une réduction importante. Pour les autres, le prix est dissuasif.

4.3. Pourquoi une configuration des équipements réseau ?

Tout au long de ce document, il sera question de configuration des équipements réseau. Si cela revêt beaucoup d'importance, c'est qu'un réseau informatique est constitué d'éléments polyvalents dotés de nombreux paramètres permettant de répondre à de nombreuses contraintes. Si ces équipements sont si chers, c'est que les fonctions qu'ils proposent permettent de limiter le nombre d'éléments à gérer et ainsi de faciliter l'administration des réseaux.

Ainsi, il n'est pas nécessaire de disposer d'un équipement pour les PC et d'un autre pour gérer les téléphones. Pourtant, ils fonctionnent sur des réseaux différents car leurs contraintes sont différentes. Le délai d'acheminement d'un fichier n'est pas critique alors que celui de la voix l'est. Pour éviter une attente, si désagréable lorsque l'on téléphone aux antipodes, entre le moment où l'on parle et où l'interlocuteur répond, il est nécessaire de maintenir un délai d'acheminement de la voix de bout en bout inférieur à deux cent millisecondes. Afin de pouvoir garantir un délai d'acheminement raisonnable, il est prudent de réserver un réseau particulier pour ce trafic. Sur un équipement réseau classique, il n'est pas possible de séparer les réseaux ni de les faire, en cas de besoin, cohabiter sur la même prise réseau. L'investissement dans un commutateur « intelligent » permet donc d'économiser l'achat d'un équipement supplémentaire, synonyme de sur-consommation de place, d'énergie, de climatisation... Ainsi, un commutateur intelligent acheté environ deux mille cinq cents Euros permet d'éviter de devoir maintenir entre quatre et six commutateurs dont le prix unitaire serait de cinq à six cents Euros. Même si l'écart de prix à l'achat est faible, les gains en installation, maintenance et support sont

considérables. À ceci s'ajoute le gain de place, très appréciable dans une usine où chaque mètre carré est compté.

Dans une entreprise, faire cohabiter de nombreux réseaux est indispensable, minimiser les dépenses également. En regard de ces contraintes, disposer d'équipements configurables est nécessaire. La gestion de ces configurations est une part importante de l'administration des réseaux.

5. Le projet

5.1. Les besoins

La raffinerie souhaite disposer d'informations concernant ses réseaux informatiques : l'architecture mise en place, les ressources utilisées et celles restant disponibles. De plus, des incidents ont mis en évidence la nécessité de disposer d'outils de supervision permettant d'analyser les problèmes et d'y proposer une solution rapide.

L'administration du réseau est assurée par une entreprise sous-traitante, Ipsilan. Pour assurer la meilleure transition possible en cas de remplacement du personnel détaché sur site, Ipsilan a proposé de consacrer une prestation à la rédaction d'une documentation exhaustive de l'architecture et des modes opératoires d'administration pour que l'usine dispose de toutes les informations utiles sur les ressources réseau dont elle dispose et que le fonctionnement du réseau ne soit plus dépendant d'une seule personne.

Cependant, une part de la documentation concerne les évolutions du réseau dans le temps : la maintenance préventive et les modifications d'architecture peuvent s'inscrire dans une vision à long terme des ressources réseau. Actuellement, l'absence de cette vision à long terme, d'un objectif clair pour l'évolution du réseau informatique pénalise les projets et coûte cher : les ressources installées le sont dans l'urgence, avec du retard et sont sous-dimensionnées faute de budget anticipé. Ces installations urgentes se plient malgré tout aux exigences de sécurité mais avec des procédures accélérées qui gênent l'activité normale. La vision à long terme doit être si possible élaborée par le management et au moins le compter parmi ses sponsors pour la rendre crédible. Ayant les connaissances techniques, Ipsilan est en bonne position pour proposer un objectif pour les réseaux qui soit cohérent avec celui, imposé par le management, de l'usine.

5.2. L'analyse des besoins

L'ensemble des acteurs est d'accord sur la nécessité d'établir une stratégie de gestion du réseau informatique. Cette stratégie est une trajectoire tenant compte de l'existant pour atteindre un objectif précis. En premier lieu, il faudra établir cet objectif puis recenser cet existant et documenter son fonctionnement et enfin définir cette trajectoire. Ainsi sont intégrés les besoins exprimés ci-dessus.

La définition de l'objectif appartient au management. Cependant, ne disposant pas d'informations suffisantes (enjeux, moyens...) il n'a pas les moyens de cerner cet objectif technique avec précision. C'est donc Ipsilan qui devra proposer un cadre de réflexion sur cet objectif. Ce cadre devra se baser sur les priorités données par la direction de l'usine et devra être suffisamment précis pour permettre de comprendre ses enjeux et suffisamment souple pour autoriser des arbitrages ou des réorientations sans le remettre en question.

La documentation de l'existant est basée sur un inventaire des ressources. S'il existe effectivement un tel document, il ne porte que sur les équipements réseau (commutateurs et routeurs) et n'est plus mis à jour depuis trois ou quatre ans. Il n'existe pas d'inventaire des liens existants. De plus, le fonctionnement des équipements réseau n'est pas documenté clairement et les bribes d'information sont dispersées dans de nombreux répertoires et de multiples fichiers de formats divers et variés sur un partage réseau. Le projet doit produire un ensemble de documents, de l'inventaire aux modes opératoires, facilement accessible et aisément compréhensible.

La trajectoire reliant l'existant à l'objectif est avant tout un guide permettant de planifier des actions. Cependant, de même que l'objectif peut être modifié, la trajectoire doit pouvoir intégrer des aléas sans que l'objectif ne devienne alors impossible à atteindre. C'est pourquoi la trajectoire doit être revue régulièrement. Le projet doit donc fournir un ensemble d'étapes basées sur des hypothèses.

5.3. Les livrables

La liste des livrables a été négociée et a servi à dimensionner une nouvelle prestation facturée au client. La fourniture des documents est basée sur une facturation forfaitaire, gage pour le client de la maîtrise des coûts et contrainte pour le prestataire de respecter les délais sous peine de perdre de l'argent.

Les livrables portent essentiellement sur la documentation stratégique et opérationnelle du réseau informatique. Ainsi, les objectifs, l'existant et la trajectoire sont déclinés en documents immédiatement applicables.

Les documents sont regroupés en trois pôles : l'architecture, l'administration et l'exploitation. Les documents de la section « architecture » décrivent l'existant et les possibilités d'évolution dans le cadre d'une stratégie d'évolution. La section « administration » regroupe les politiques de gestion, les procédures et les modes opératoires nécessaires au bon fonctionnement du système. Enfin la section « exploitation » regroupe les informations nécessaires aux opérations quotidiennes sur le réseau.

Un document proposant un objectif à long terme pour le réseau informatique, hors cadre de la liste des livrables négociée, doit également être établi.

5.4. Le planning

Ce projet s'inscrit dans le cadre du changement de plateforme bureautique imposée par le groupe Total. Ce changement nécessite de bien connaitre l'existant mais également de pouvoir rapidement savoir si les infrastructures en place pourront accompagner cette opération et une identification rapide des évolutions à apporter aux infrastructures. L'installation des nouveaux systèmes débutant en novembre 2011 sur la raffinerie, le projet doit s'attacher à produire au plus tôt les éléments documentaires et dans tous les cas avant septembre 2011.

5.5. La méthode

Le projet est découpé en trois segments : la définition d'un objectif, la documentation des éléments existants et de leur fonctionnement et enfin de la manière d'atteindre l'objectif sur la base des éléments existants : la trajectoire.

La définition d'un objectif, selon ITIL (*Information Technology Infrastructure Library — Bibliothèque pour l'infrastructure des systèmes informatiques*) version 3, consiste à recueillir la stratégie de l'entreprise et à la décliner en stratégie informatique. Dans le cadre de ce projet, la stratégie informatique sera ainsi détaillée en objectif pour les réseaux.

La documentation des éléments existants nécessite un inventaire mais également une structure de documentation. Le réseau étant découpé en couches standards selon le modèle « IP », il a paru naturel d'organiser l'architecture existante selon ce concept.

Cette partie de la méthode est détaillée dans la section concernant la réalisation de la documentation.

Il est nécessaire d'établir, en fonction de l'objectif, des critères d'avancement mesurables. La trajectoire doit produire des jalons et des moyens de mesurer le degré d'atteinte de l'objectif à ces échéances. Les budgets étant négociés annuellement, il est judicieux de placer des jalons sur la même période.

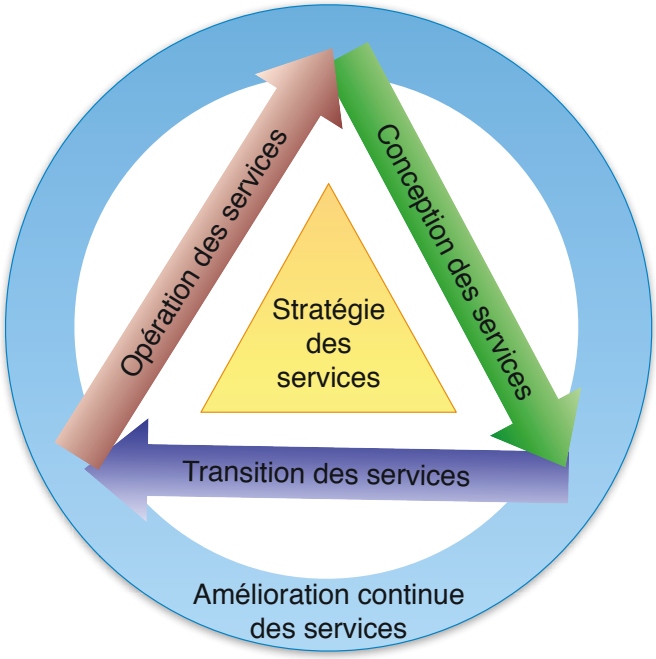
Chaque segment peut disposer de sa propre approche pour arriver à la production des documents attendus. Cependant, la ligne directrice est de toujours partir des besoins du client qui sont considérés comme l'objectif à atteindre et de décliner ces besoins en moyens de les satisfaire. Cette technique permet de concentrer les efforts sur les éléments qui seront réellement utiles au client et évite de se disperser sur des points accessoires. Cette approche est celle préconisée par ITIL qui a donc fourni un nombre important d'éléments pour la réalisation de ce projet.

5.5.1. L'apport méthodologique d'ITIL

ITIL est un recueil de « meilleures pratiques » ayant, à l'origine, pour but de réduire les coûts et d'augmenter la qualité de l'exploitation informatique. Cette vision est maintenant élargie à l'ensemble de la DSI dans la version la plus récente d'ITIL et est même devenue une norme pour la qualité des services informatiques (ISO 20 000) et sert de base à une réflexion sur la création d'une norme de gestion des services, se détachant ainsi de la spécificité informatique pour s'intéresser à tout type de service.

Il existe à ce jour trois versions d'ITIL. La version 1 est obsolète. La version 2 est la plus implémentée actuellement mais ne s'intéresse qu'à la production informatique. La version 3 est sur le point de la supplanter car elle porte sur l'ensemble de la DSI et des services qu'elle propose. Dans ce document, nous parlerons principalement des processus de la version 3.

ITIL propose des processus de référence construits à partir de retours d'expériences recueillis en entreprise. Ces processus sont regroupés en cinq grands pôles : la stratégie, la conception, la transition, l'exploitation et l'amélioration continue des services informatiques.



Organisation générale du référentiel ITIL version 3

Un certain nombre d'éléments gravitent autour de ce noyau. En particulier, il existe des études de cas qui apportent des retours d'expérience sur des implémentations réussies ou non d'ITIL. Ces documents fournissent des éléments de réponse à la question de la mise en place d'ITIL en présentant des démarches complètes et leur critique.

Dans ce projet, la manière de décomposer les problèmes et certains processus sont les éléments les plus exploités d'ITIL.

5.5.2. L'urbanisation des systèmes d'information

La méthode d'urbanisation des systèmes d'information est une démarche de mise en adéquation des ressources informatiques avec les besoins des utilisateurs. Cette démarche peut être utilisée pour implémenter les processus ITIL par exemple. C'est un outil d'alignement du système d'information sur la stratégie de l'entreprise.

Cette méthode se base sur des cartes établies à différents niveaux d'abstraction. Ces niveaux sont généralement au nombre de quatre : la vision métier, la vision fonctionnelle, la vision applicative et la vision technique. Il existe des règles permettant de passer d'un niveau à un autre pour établir les cartes et ainsi s'assurer que le plus bas niveau (le niveau technique) est parfaitement la déclinaison d'un besoin réel exprimé au plus haut niveau (le niveau métier). Ces cartes sont utiles pour

décomposer le système d'information en blocs aisément compréhensibles. Elles servent à décrire des architectures abstraites puis de plus en plus techniques.

Les règles de passage permettent une implémentation aisée et garantissent que le changement de niveau se fait en conservant le même sens (la même signification). Ainsi, alors que le premier document est parfaitement lisible par un utilisateur des systèmes d'information, le dernier est très technique et requiert un certain niveau d'expertise. Pourtant, ils sont établis en cohérence et décrivent la même chose. Ils sont simplement adaptés à des publics différents à qui ils permettent de communiquer. Cette démarche est légèrement contradictoire avec ITIL : l'urbanisation fait communiquer des mondes en traduisant les langages des uns et des autres l) où ITIL propose un langage commun, quel que soit l'interlocuteur. L'avantage de l'urbanisation est qu'elle ne nécessite pas de changer les habitudes de formulation des problèmes et s'insère donc sans difficulté dans une organisation existante, là où ITIL est mis en place en changeant l'organisation.

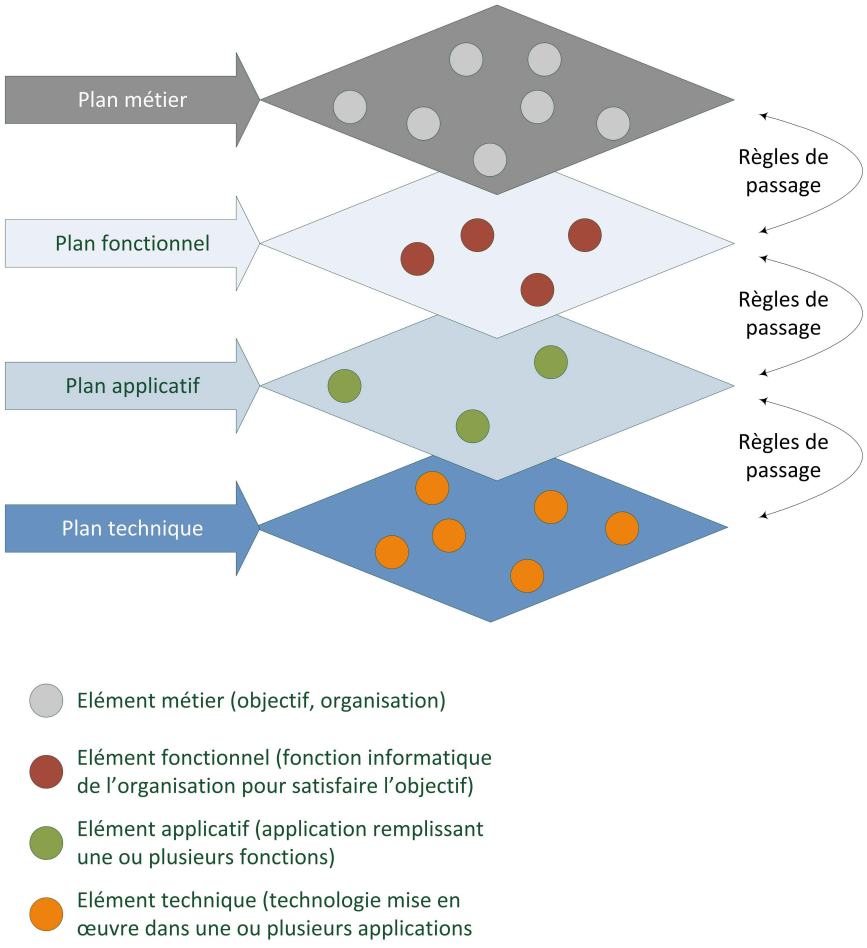


Schéma de principe de la méthode d'urbanisation

Cette méthode, avec quelques aménagements décrits dans la partie traitant de la documentation, a fourni les principes directeurs de la rédaction des documents : leur hiérarchie, leur constitution... Les documents ont été adaptés, dans leur forme et dans leur contenu, au public visé. L'identification de ce public a été débattu lors d'une réunion de présentation des premiers documents afin de s'assurer que la direction adoptée était correcte.

6. La séquence de réalisation du projet

Cette présentation du contexte met en évidence les besoins actuels liés à l'historique d'un site industriel de traitement de matières dangereuses. Le traitement de ces besoins a été décomposée en plusieurs étapes qui sont détaillées ci-après. Ces étapes sont présentées dans l'ordre dans lequel elles ont été réalisées, même si certaines se chevauchèrent.

Les chapitres suivants présentent successivement le travail réalisé sur la finalité de ce projet, la documentation de l'installation existante (vision statique des réseaux), les outils de gestion (vision dynamique) et enfin la proposition d'améliorations.

La finalité du projet

La gestion des réseaux informatiques est une activité de longue haleine. L'interrompre, même pour une courte période, implique de grandes difficultés lors de sa reprise. C'est pourquoi ce projet s'attache, au-delà de sa réalisation proprement dite, à donner un cap, un sens aux actions de gestion afin qu'elles conservent une orientation efficace dans le temps.

Ce cap, c'est un objectif à long terme. Selon ITIL, un objectif doit être « SMART » : Spécifique, Mesurable, Atteignable, Raisonnable et Temporellement défini. Ce chapitre a pour but de montrer le travail fourni pour établir des objectifs qui satisfassent ces critères tout en restant cohérents avec la stratégie de l'entreprise qu'ils servent. En premier lieu, la notion d'objectif à long terme est définie. Puis sont exposés les objectifs de l'entreprise et leur déclinaison pour les réseaux. Une partie est spécifiquement consacrée à l'environnement de l'entreprise et son influence sur ses objectifs. Enfin, l'objectif à long terme de l'activité de gestion des réseaux est détaillé.

7. Qu'est-ce qu'un objectif à long terme ?

D'après le référentiel ITIL, la stratégie d'entreprise est un ensemble de choix, d'objectifs et de règles de gestion soutenus par un plan d'action, un budget et un portefeuille de projets. Ici, les objectifs sont clairement exposés par le gestionnaire du site, les règles de gestion sont imposées (pour partie par la législation, pour une autre partie par le Groupe) et les choix sont laissés à l'appréciation de la direction de l'usine. Ces choix portent notamment sur le portefeuille de projets qui sert de base au plan d'action et à la négociation du budget.

Le portefeuille de projet contient l'ensemble des projets du site. Ces projets incluent tous une composante « système », c'est-à-dire une partie d'automatisme ou d'informatique. C'est dire le degré d'importance des systèmes d'information dans toute la vie de l'usine.

Ce portefeuille de projets peut comporter des projets purement informatiques, qui ne sont pas proposés par des clients mais par le service Systèmes pour améliorer la qualité des services proposés. Ce projet se place dans ce cadre, afin d'apporter au management une vision des évolutions possibles ou nécessaires pour garantir un service de la qualité requise et de pouvoir planifier la mobilisation des ressources.

Les projets servent à atteindre un objectif. Avant de se lancer dans des projets, il faut avant tout disposer d'objectifs validés, c'est-à-dire dont le bien-fondé est vérifié par la direction. Ne pas disposer d'objectif revient à ne pas pouvoir justifier de projets. C'est pourquoi, ici, nous nous intéressons à la définition de ces objectifs plutôt qu'à la constitution d'un portefeuille de projets. Si ces objectifs sont validés, ils seront alors déclinés en projets.

Ces objectifs doivent répondre à des besoins, voire même doivent permettre d'anticiper ces besoins. C'est le rôle du management de l'entreprise pour les objectifs stratégiques de l'usine. Ensuite, il est possible de décliner ces objectifs pour les systèmes informatiques et donc le réseau de l'entreprise.

8. Les réseaux et les objectifs de l'entreprise

8.1. Les objectifs de la raffinerie

Déterminer les objectifs de l'entreprise est chose relativement aisée. Adepte des techniques de management modernes, la direction a à cœur de faire partager ses objectifs au personnel travaillant sur le site. C'est particulièrement vrai en période de difficultés économiques. Ainsi, Sécurité, Fiabilité, Rentabilité sont les trois objectifs de la raffinerie. Ils sont hiérarchisés : la rentabilité est directement héritée de la fiabilité qui peut être considérée comme un des résultats de la sécurité.

La sécurité est la valeur fondamentale de l'usine. Elle est au cœur des préoccupations quotidiennes. La sécurité, sur le site, c'est la prévention des dommages aux personnes, aux installations et à l'environnement. Beaucoup d'efforts sont déployés par l'ensemble des personnes travaillant sur le site pour travailler en sécurité.

La fiabilité est un gage de qualité. L'usine est fiable si le procédé est maîtrisé et reproductible et donc s'il est possible de garantir une qualité constante de fabrication. Des dommages causés aux installations mettent à mal cette fiabilité, peuvent causer du tort aux clients finaux et impactent la rentabilité du site.

La rentabilité est l'objectif final de l'entreprise. Le secteur du raffinage en France est en crise, toutes les installations fonctionnent à perte et certaines sont déjà en cours de fermeture définitive. Dans ce contexte, abaisser le point mort de l'usine, réduire les coûts et conserver les clients sont des points critiques pour la survie du site. Ainsi, une usine fiable et sûre disposera de meilleurs atouts face à ses concurrentes dans un milieu où les moins rentables disparaîtront.

Ces objectifs sont accompagnés de dispositifs de mesure : les indicateurs. Ils sont établis le plus souvent mensuellement et sont affichés à la vue de tous sur un panneau lumineux à l'entrée du site.

De plus, en 2011, comme tous les trois ans, une contrainte supplémentaire est venue se greffer aux objectifs de l'entreprise : le Grand Arrêt (GA). Cet arrêt complet de l'ensemble des installations de la raffinerie est une contrainte légale dont l'exécution est placée sous le contrôle de l'état via l'autorité de tutelle de la raffinerie : la DRIEE (Direction Départementale et Interdépartementale de l'Environnement et de l'Énergie). Ainsi, durant cinq semaines, des travaux de maintenance et des inspections règlementaires sont effectués. Le résultat de ces inspections conditionne la délivrance d'un permis d'exploitation sans lequel la raffinerie ne peut exercer son activité. Lors de cet arrêt, la raffinerie ne produit plus : ce temps est, du point de vue comptable, une perte nette. La réussite de cet arrêt est donc de satisfaire les critères d'inspection avec un budget très limité. Aussi, les équipes informatiques doivent, en un temps record, fournir et assurer le retrait d'infrastructures de communication à des installations temporaires installées quelques jours avant le début de l'arrêt et déposées quelques jours après sa fin. Cet arrêt mobilise environ deux mille personnes pour un effectif normal de l'usine de sept cents personnes, entreprises extérieures incluses. Cet afflux de travailleurs va de pair avec des besoins importants de moyens de communication. En premier lieu, l'installation à moindre coût de réseaux informatiques performants sur des zones de travail temporaires (bungalows placés au plus près des unités de production) normalement non desservies est un véritable défi.

8.2. La contribution de l'informatique à l'atteinte de ces objectifs

A priori, l'informatique est impuissante à éviter les accidents, améliorer la qualité des réactions chimiques et réduire les coûts. La contribution de l'informatique à l'atteinte des objectifs stratégiques de l'entreprise n'est pas évidente. Pour autant, elle n'est pas inexistante mais sa méconnaissance est source de frustration pour les informaticiens qui souffrent d'un grand manque de reconnaissance de la part des autres services de l'usine. Ainsi, un gain de productivité ne sera jamais crédité à l'installation d'une nouvelle application mais une perte de temps sera imputée à l'informatique. Si ce problème est classique pour l'ensemble de la filière informatique, il est particulièrement sensible dans un contexte de chasse aux postes inutiles. Le travail de mise en relief de la contribution de l'informatique à l'atteinte des objectifs de l'entreprise présenté ici

a donc une finalité double. Il s'agit de justifier auprès de la direction de l'entreprise de la cohérence des objectifs informatiques avec les siens propres. Mais il faut également rassurer les informaticiens qui de plus en plus doutent de leur réelle valeur ajoutée à l'heure de l'externalisation des tâches d'exploitation et de maintenance des infrastructures bureautiques.

8.2.1.L'informatique et la sécurité

L'informatique se doit de faciliter la mise en sécurité des postes de travail. Elle y contribue selon deux axes : la mise en place de systèmes permettant un contrôle fin et réactif des unités de production et la mise à disposition d'outils facilitant le partage de l'information relative à la sécurité.

Les dispositifs de contrôle de production (systèmes de conduite) sont des moyens informatiques permettant de ne plus exposer les opérateurs aux dangers présents dans les unités de production. Le pilotage des unités de production consiste à la fois à entretenir la production mais également à contrôler cette production afin qu'elle s'effectue dans de bonnes conditions de sécurité. Les personnes peuvent agir depuis une salle de contrôle, à la fois pour éviter un arrêt intempestif de la production mais également pour procéder à l'arrêt d'urgence et à la mise en sécurité des personnes et des installations en cas d'incident majeur Les outils de pilotage à distance permettent de concilier ces objectifs contradictoires. De plus, l'informatique apporte des outils d'historisation des messages et des actions permettant, en cas d'incident, de procéder à une analyse fine. Cette analyse peut être, en cas d'accident notamment, une obligation légale.

Lors d'une enquête judiciaire, de nombreux éléments informatiques forment des commencements de preuve. Ainsi, les données recueillies par les systèmes de mesure et les ordres donnés au système de conduite, le SNCC — Système Numérique de Contrôle de Conduite — sont des informations pouvant servir à établir la chronologie d'un accident et les responsabilités des acteurs. Dans ce contexte, il est important de s'assurer que les données stockées sont fiables et qu'elles ne sont pas modifiables après leur recueil.

L'arbre des causes est la méthode standard d'analyse des incidents et accidents. Cette méthode nécessite de situer l'ensemble des facteurs ayant contribué à l'événement dans le temps. Les journaux informatiques des alertes et actions sont la source principale d'information et souvent la seule ayant valeur de commencement de

preuve. De même, en cas d'accident majeur, les automates peuvent réagir très rapidement et contribuer efficacement à une réduction des risques sur le site. C'est par exemple le rôle des automates de sécurité gérant l'ensemble des dispositifs d'arrêt d'urgence de la raffinerie et centralisés dans trois locaux stratégiques de la raffinerie.

Une part importante du dispositif de sécurité de la raffinerie est son référentiel de sécurité. Ce référentiel est constitué d'une base de données documentaire informatique recensant les procédures à appliquer au site. Ces procédures tiennent compte des spécificités de l'usine et sont enrichies par des retours d'expérience des problèmes survenus sur d'autres installations comparables à travers le monde. Tout le système documentaire repose sur des outils informatiques. Ces informations, mises à disposition de l'ensemble des personnels de l'entreprise sont consultées régulièrement. Il est important de garantir une bonne disponibilité et une excellente fraicheur des données du système.

8.2.2.L'informatique et la fiabilité

La fiabilité globale de l'usine est directement dépendante de celle de son système de conduite. L'indisponibilité, un manque de précision dans les réponses ou une erreur de programmation de ce système peuvent générer des coûts importants, par baisse de qualité du produit fabriqué voire même pour cause d'arrêt intempestif d'une unité.

L'arrêt d'une unité est forcément très coûteux. Le directeur technique de la raffinerie considère que certaines installations peuvent entraîner dans leur arrêt celui de l'ensemble de l'usine, conduisant à une perte d'exploitation considérable. L'arrêt non désiré doit donc absolument être évité.

C'est pourquoi les données recueillies et les consignes données par les opérateurs doivent être transmises sans aucune altération et sans délai. L'informatique est, dans ce contexte, essentielle pour la bonne marche des unités de production. La contribution de l'informatique à l'objectif de fiabilité est plus concrète qu'à celui de sécurité. Il est assez facile de constater que l'ensemble des outils de pilotage et de contrôle de la production sont informatiques et que la bonne marche des unités repose sur celle du système de conduite. En l'absence de ce système, il est impossible de fabriquer des produits dans les conditions de sécurité et de qualité prescrites.

8.2.3.L'informatique et la rentabilité

L'usine ne pourrait pas être exploitée sans l'informatique. C'est une preuve de la contribution de cette activité à la création de valeur de l'entreprise. Cependant, la mesure de cette contribution est subjective. En effet, s'agissant d'une activité participant à l'ensemble des tâches de production mais ne constituant jamais une tâche à part entière, il est difficile de mesurer la part de richesse créée par l'informatique. Cette difficulté place les informaticiens en position de faiblesse lors des négociations budgétaires, face à d'autres services dont la rentabilité est objectivement établie et importante.

Dans ce contexte, disposer d'une feuille de route à long terme approuvée, sinon établie, par la direction, est indispensable pour que l'informatique puisse toujours contribuer à la rentabilité des activités de production.

8.2.4.L'informatique et le Grand Arrêt

Les techniques les plus diverses sont employées pour satisfaire la demande de liaison en minimisant les coûts. Ainsi, en 2011, pour la première fois, une liaison WiFi a été installée pour éviter le passage d'une fibre optique et ainsi diviser le coût de la liaison par un facteur dix. Cette solution n'est cependant pas adaptée à la desserte de nombreux postes de travail et ne saurait remplacer une liaison filaire ou optique pour satisfaire des besoins intensifs.

8.3. La part des réseaux dans les objectifs informatiques

Les réseaux informatiques sont une partie essentielle des systèmes d'information actuels et doivent donc contribuer fortement à l'atteinte des objectifs informatiques. En effet, la sécurité informatique repose bien souvent sur la redondance : la duplication des informations voire des dispositifs de traitement. Cette redondance, pour être efficace, doit être implémentée sur des emplacements distants les uns des autres afin d'être moins vulnérables aux contraintes environnementales pouvant affecter un lieu (coupure d'électricité, panne du système de climatisation...) Les réseaux prennent alors tout leur sens en permettant de garantir des duplications rapides et fiables.

De plus, la conduite de l'usine depuis une salle de contrôle serait impossible sans un réseau permettant de séparer les commandes des actuateurs. Cette séparation, nécessaire pour la sécurité, la traçabilité et la maîtrise de la qualité, repose de plus en plus sur des technologies informatiques.

Enfin, dans un groupe international où la concentration des moyens sur des « centres de ressource » est un gage d'économie, les réseaux informatiques sont la clef de voute de toute l'infrastructure, permettant à la fois d'accéder à ces ressources centrales à distance et rendant possible l'exploitation à distance des systèmes locaux.

Ainsi, les réseaux informatiques se voient affecter les mêmes objectifs que l'usine. Que les réseaux satisfassent les besoins de sécurité, de fiabilité et de rentabilité qui leur sont propres contribueront à l'atteinte par l'entreprise de ces mêmes ambitions. Les réseaux doivent, pour répondre aux besoins des clients, satisfaire les contraintes de sécurité, de fiabilité et de rentabilité imposées. Ces trois aspects sont intimement liés et ne peuvent s'envisager individuellement ou du moins aucun ne peut être privilégié au détriment des deux autres : il faut trouver un équilibre.

8.4. La sécurité et la fiabilité des réseaux de l'usine

La sécurité, dans ce contexte, s'entend comme une garantie de fonctionnement selon la conformité à trois principes : la confidentialité, l'intégrité et la disponibilité. La fiabilité peut s'envisager comme une composition de l'intégrité et de la disponibilité.

La confidentialité est la raison d'être de la séparation entre les réseaux telle qu'elle est en place sur l'usine. En fonction du degré critique des informations qu'ils acheminent, des périmètres ont été définis. Ces périmètres sont alors eux-mêmes segmentés pour parvenir à une définition fine des accès aux informations. Ainsi, il existe quatre grands périmètres, le plus critique pilotant directement les équipements de l'usine (vannes, moteurs...) et le moins critique étant utilisés pour la bureautique. Cependant, même dans le périmètre bureautique, plusieurs zones de confiance cohabitent. Certains équipements sont visibles de l'ensemble des ordinateurs du Groupe, d'autres ne sont accessibles que par ceux du site. La gestion de ces restrictions n'est faisable que depuis certains ordinateurs du site dont l'accès n'est autorisé qu'à une poignée d'informaticiens locaux.

L'intégrité et la disponibilité sont implicitement requises à leur niveau maximal. Ainsi, on s'attend à ce que les réseaux informatiques n'altèrent pas les données qui leur sont confiées et qu'ils soient opérationnels en permanence. La disponibilité est elle-même dépendante de la capacité des réseaux à absorber la charge d'information confiée. Cette capacité peut se mesurer et son évolution peut s'anticiper.

Cependant, il est illusoire de vouloir garantir ces niveaux de service sans mesurer les ressources à associer à ces exigences. Ainsi, la disponibilité permanente des réseaux

nécessiterait des moyens actuellement inaccessibles. Le but de l'établissement d'une trajectoire pour atteindre cet objectif est de mettre en évidence cette impossibilité actuelle et de créer une série d'échéances dotées d'objectifs intermédiaires atteignables.

8.5. La rentabilité des réseaux informatiques

Combien rapporte un réseau informatique ? Combien coûte-t-il ? La différence entre les deux nous donne-t-elle une valeur objective de la rentabilité des réseaux ?

Il est semble-t-il aisé de mesurer le coût du réseau informatique. Il suffit d'additionner les coûts d'achat et de maintenance des équipements, les redevances d'abonnement aux services de télécommunication et le coût des ressources humaines consacrées à son exploitation. Cependant, il faut également prendre en compte d'autres coûts, moins faciles à quantifier : la consommation d'électricité, de climatisation voire de mètres carrés dans les locaux sont difficilement mesurables.

Le gain financier procuré par les réseaux informatiques est encore plus difficile à évaluer. Si tout le monde s'accorde pour dire que l'activité ne pourrait plus être effectuée sans eux, est-ce à dire que l'ensemble des revenus de l'usine doit être porté au crédit de ces infrastructures ? En partie probablement, en totalité certainement pas. Comment en définir la clef d'affectation ? Une solution serait de mettre en évidence le coût d'un arrêt du réseau. Cependant, les données font polémique et il est impossible actuellement de disposer d'un chiffre consensuel.

Ainsi, il est demandé aux réseaux d'être rentables alors que la mesure de cette rentabilité est pour l'instant impossible. Faute de mieux, l'indicateur de rentabilité retenu sera le taux de disponibilité des réseaux. Un réseau rentable est celui qui ne supporte qu'une heure d'indisponibilité cumulée par an. Ce critère est arbitraire et servira, à l'avenir, à justifier un vrai calcul de rentabilité par le management.

9. Les défis environnementaux

L'entreprise se conçoit dans un environnement : le site et ses riverains, la réglementation, les partenaires commerciaux... sont porteurs d'opportunités et de contraintes. Dans le cas d'une usine classée Seveso seuil haut, elles sont exacerbées. L'autorité de tutelle (sous le contrôle direct de l'État via le préfet) veille au respect d'une partie de ces contraintes environnementales. Une des manifestations concrètes de cette tutelle est la présence régulière de gendarmes sur le site.

L'informatique est fortement mise à contribution par l'autorité de tutelle. Par exemple, les systèmes d'information de la raffinerie doivent mesurer les valeurs de rejet dans l'atmosphère de différents polluants et parfois même ajuster le procédé pour agir en temps réel sur ces rejets. Ils doivent également stocker les données au sein de conteneurs disposant de qualités légales (empêchant toute modification des données...) et permettre une communication efficace des résultats aux intéressés (les mairies des communes voisines...).

Les mesures des impacts des activités de la raffinerie sur l'environnement ne sont pas seulement effectuées sur le site de l'exploitation mais également sur les communes alentour, pour contrôler l'exposition réelle des populations. Ces mesures distantes sont des contraintes réglementaires. Les réseaux de télécommunication rendent possible des mesures en temps réel, très précises et garantes du respect des normes de rejet.

Il existe bien d'autres exemples de contraintes environnementales dont la satisfaction repose sur les réseaux informatiques. Ainsi le pilotage du pipeline (PLIF, pipeline de l'Ile de France) approvisionnant la raffinerie depuis le terminal pétrolier du Havre (Seine Maritime), assuré à distance, est-il entièrement dépendant d'une infrastructure de télécommunication. La sécurité des différentes stations de pompage est assurée par un système de vidéosurveillance opéré depuis la salle de contrôle pilotant le PLIF.

10. L'objectif à long terme de la gestion des réseaux

L'ensemble des contraintes exprimées vont dans la même direction : une meilleure sécurité de fonctionnement. Cette sécurité repose toujours plus sur des technologies informatiques et en particulier sur les facilités de communication promises par les réseaux. Ces réseaux sont un maillon de la chaîne de la sécurité et ce maillon est particulièrement fragile. Il convient donc de mettre en place des solutions qui permettent de satisfaire la demande de sécurité à moindre coût. Ce compromis forme l'objectif à atteindre pour les réseaux.

Les réseaux informatiques mis en place satisfont les besoins actuels de la raffinerie. Ils sont perçus comme performants et fiables par les utilisateurs. L'objectif n'est donc pas de les remettre en cause mais plutôt de leur donner la capacité de répondre aux besoins de sécurité exprimés, d'adopter des solutions capables de s'adapter facilement et à moindre coût aux évolutions de ces besoins et de procurer des éléments de prévision facilitant la négociation budgétaire.

10.1. Le niveau de sécurité requis

Ce qui est requis, c'est la sécurité au sens industriel : la garantie d'un acheminement rapide des données, sans altération d'aucune sorte. Les réseaux doivent donc être présents aux endroits nécessaires, disposer de capacités suffisantes et résister aux événements pouvant les affecter.

La présence d'un réseau se nomme la « capillarité ». Il s'agit de mesurer la capacité à fournir un service de réseau de la qualité requise à l'endroit spécifié. Les réseaux reposant sur des infrastructures physiques, il est assez facile de mesurer la capillarité, même si les différentes technologies en présence amènent des niveaux de qualité hétérogènes. La connaissance de cette capillarité est indispensable pour pouvoir fournir rapidement des services réseaux aux utilisateurs.

Mesurer la capacité d'un réseau, c'est observer la consommation de ses ressources et l'analyser. Cette mesure est effectuée par un système de supervision. La mise en place d'un tel système et donc la production d'indicateurs de charge permet de dégager des tendances et de prévoir les évolutions de capacité nécessaires. C'est un outil stratégique.

La résistance aux événements nécessite une analyse des risques pesant sur ces réseaux. Ensuite, en fonction des risques identifiés et de leur effet sur le service demandé, il est nécessaire de mettre en place des contre-mesures efficaces dans le respect des contraintes budgétaires. Néanmoins, cette analyse peut servir de levier durant la négociation des budgets.

L'objectif à long terme est donc le résultat d'une analyse de la capillarité, de la capacité et des risques. Définir le niveau de sécurité requis se résume à exprimer des exigences sur ces trois critères.

10.2. L'exigence de capillarité

La distribution du réseau dans l'ensemble des locaux de l'usine est à la fois inutile et coûteuse. Cependant, positionner des relais à des endroits astucieux permet, le moment venu, de n'avoir à effectuer que de petits raccordements économiques.

Le niveau de capillarité requis ne s'exprime donc pas en nombre de bâtiments couverts par les réseaux mais plutôt en distance moyenne séparant les bâtiments d'un accès au réseau. Cette distance, dans le cas de la raffinerie, est à pondérer avec la difficulté de réaliser l'acheminement. Par exemple, disposer d'une liaison entre un

poste électrique contenant un accès au réseau et un bâtiment peut nécessiter de nombreux mois et demander de gros moyens pour effectuer les travaux, même si la distance à parcourir est réduite à quelques mètres comme l'exemple cité en introduction l'illustre.

Il est donc important d'identifier les points stratégiques pouvant servir de « relais » ou « point de connexion de proximité ». Ensuite, il faut être attentif aux autres travaux effectués sur l'usine. Ainsi, il est possible de profiter de l'ouverture d'une tranchée par un autre service pour y glisser les liens vers le point identifié comme stratégique. Aujourd'hui, de nombreuses tranchées sont ouvertes mais peu contiennent des liens réseaux qui pourtant peuvent se révéler nécessaires par la suite. La mutualisation des travaux de fouille est indispensable car leur coût est prohibitif et dans certains cas a empêché la réalisation de liaisons.

La « veille travaux » permettant de profiter des opportunités de chantiers doit être menée par les superviseurs de travaux. En effet, dans bien des cas, le service Systèmes n'est pas impliqué car ces travaux ne le concernent pas et il n'est donc pas averti des opportunités présentes. C'est pourquoi les informations concernant les points de connexion doivent être communiquées aux services susceptibles d'effectuer des travaux à proximité.

L'objectif est de disposer d'un lien réseau à moins de cent mètres de tout bâtiment actuellement dépourvu d'accès. Cette distance s'entend « nette » : non pas à vol d'oiseau mais entre le point d'accès du réseau et le lieu où un équipement réseau terminal serai disposé. Cette distance comprend donc toutes les pertes (virages...) liées aux contraintes d'acheminements (obstacles à contourner...). Cette distance est celle, maximale, constituant un brin Ethernet en cuivre. Or les points terminaux ne sont pas dotés d'un accès direct par fibre optique : il est donc nécessaire de rester dans ce périmètre. L'atteinte de cet objectif nécessite de disposer d'une liste des bâtiments non reliés au réseau, d'une réflexion sur les trajets permettant de les desservir et d'une communication auprès des services susceptibles de faire des travaux dans ces lieux.

10.3. L'exigence de capacité

Les réseaux doivent contribuer à des communications rapides et fluides. Cependant, il s'agit d'une ressource finie dont les capacités, très coûteuses, doivent être gérées au plus près des besoins.

Il est impossible de restreindre les usages des réseaux. L'administrateur ne peut en cas de dépassement de capacité, trier le trafic et ne laisser passer que quelques messages prioritaires, les suivants étant mis en attente. Si une solution de ce genre existe, elle n'est pas mise en œuvre au niveau des réseaux mais des applications qui les utilisent. Par exemple, les services de messages courts — Short Message Service ou SMS — gèrent des millions de messages lors de chaque changement d'année civile. Il n'est pas rare que ces messages soient acheminés avec plus de douze heures de retard, simplement parce qu'une application empêche la saturation complète du réseau, ce qui entraînerait la perte pure et simple des messages surnuméraires. Dans cette situation, un dépassement de capacité se traduit par un ralentissement des acheminements et donc la perception d'une dégradation de la qualité de service mais la préservation du service (les messages sont acheminés). Dans certains cas, le manque de capacité n'a pas d'effet fort sur la productivité et ne conduit pas à la perception d'un service fortement dégradé. C'est le cas de l'accès à Internet qui, même s'il est saturé et entraîne des ralentissements, ne perturbe pas le fonctionnement de l'usine, à condition que cette saturation reste de courte durée. Cependant, un ralentissement, même temporaire, des échanges entre les ordinateurs clients et les serveurs se traduit par une baisse de productivité immédiate. Cette situation est donc inacceptable.

L'ajustement des capacités doit donc se faire en fonction d'une analyse des besoins. Ensuite, il faut disposer de mesures fines de la consommation de capacité pour pouvoir enfin l'ajuster aux besoins précédemment analysés.

Les capacités réseaux ne sont pas élastiques : il n'est pas possible de réduire la capacité durant les périodes de faible usage. La surcapacité ainsi nécessaire mais très onéreuse doit être très finement ajustée aux pics de consommation pour éviter une dérive des coûts.

L'analyse des besoins rejoint la mesure de la consommation de ressources. En effet, les données concernant les besoins ne sont pas disponibles a priori. Il est plus facile de mesurer l'usage actuel ainsi que son évolution dans le temps pour en dégager des tendances. Une exception est à noter : dans le cadre du projet « Vision » de remplacement de la plateforme bureautique une évaluation des besoins est réalisée en amont et des actions sont engagées sur la base de cette étude. Cependant, les critères d'évaluation sont obscurs et il est probable qu'ils soient empiriques et donc eux aussi basés sur des mesures de consommation de ressources.

La mise en place d'un dispositif permettant de connaitre le volume d'échanges d'informations, son évolution et même les trajets les plus empruntés est nécessaire pour mettre en place des ressources adaptées. Le volume d'échanges est évalué par unité de temps. Il est qualifié de « bande passante », car techniquement, il s'agit d'une mesure de l'utilisation d'une bande de fréquences sur un médium réseau. La bande passante totale représente la capacité totale du lien considéré, la bande passante consommée est la partie de bande passante totale occupée à l'instant de la mesure.

L'objectif est de garantir en permanence une réserve de vingt pour-cent de la bande passante totale sur l'ensemble des liens internes (hors accès aux réseaux externes). Cette valeur empirique correspond à un bon compromis observé chez les clients d'Ipsilan. L'atteinte de cet objectif nécessite la connaissance de la bande passante totale disponible, de la consommation actuelle et de l'évolution de cette consommation afin d'anticiper les besoins de modification de capacité.

La capacité, c'est également offrir la possibilité de connecter de nouveaux équipements au réseau. Cette capacité se mesure par la disponibilité de points de connexion physiques, appelés « ports ». Une bonne pratique consiste à préserver en permanence entre dix et vingt pour-cent des ports libres sur un équipement, à la fois pour conserver une marge de connexion mais également pour ne pas saturer la bande passante interne de l'équipement, c'est-à-dire sa capacité à effectuer son travail.

La mesure de la capacité actuellement disponible fait l'objet d'une section plus loin dans ce document et la partie dédiée à la trajectoire d'atteinte des objectifs détaille la méthode retenue.

10.4. L'exigence de prévention des risques

Les risques s'entendent comme les facteurs internes ou externes au système pouvant affecter la qualité du service lors de leur survenue. Ici, la qualité sera réduite à la disponibilité puisque les autres aspects de la qualité sont englobés dans les points précédents. Dans le cas des réseaux, une indisponibilité peut être causée par une panne matérielle, la rupture d'un lien, un dépassement de capacité... La solution la plus répandue en informatique pour se prémunir contre l'indisponibilité est la redondance. Les réseaux ne font pas exception. Cependant, cette redondance a un prix très élevé et il convient de l'implémenter de manière efficiente.

Spontanément, la redondance évoque le doublement des équipements pour éviter de supporter les conséquences d'une panne. C'est un résumé un peu rapide. En effet, la

cause la plus fréquente d'indisponibilité d'un équipement réseau est un défaut d'alimentation en énergie : électricité, climatisation... Dans ce cas, il ne sert à rien de dédoubler les équipements s'ils sont branchés sur la même alimentation électrique. La redondance doit être envisagée de manière globale et non restreinte aux seuls équipements réseau. De plus, il n'est ni utile ni rentable de doubler les connexions entre les équipements terminaux et les nœuds du réseau. Ainsi, il est accepté que la défaillance d'un nœud prive de connexion au réseau un ensemble de périphériques.

L'objectif n'est donc pas de se garantir contre une indisponibilité partielle mais de limiter l'effet d'une indisponibilité d'un équipement à ce seul équipement et d'éviter une indisponibilité totale.

L'indisponibilité d'un équipement s'étend à tous les systèmes qui lui sont uniquement raccordés. Ainsi, se prémunir contre l'extension d'une indisponibilité consiste à établir des chemins multiples entre les nœuds, à l'image du réseau routier où, si un carrefour est bloqué, il est possible d'emprunter un autre chemin pour atteindre son but, pour peu que celui-ci soit différent dudit carrefour. Dans les réseaux, la redondance de chemins consiste à créer des « mailles ». Plus le réseau est maillé, plus l'effet d'une défaillance d'équipement ou de lien est restreint. Là encore, disposer d'un réseau entièrement maillé n'a pas forcément beaucoup de sens et peut coûter très cher. Pour identifier les éléments devant participer à des mailles, le fabricant d'équipements réseau Cisco propose de les hiérarchiser par nombre de connexions afin de les classer selon trois niveaux d'importance. Les plus importants doivent être maillés. Il est recommandé que ceux du niveau intermédiaire participent à une maille. Les éléments les moins importants peuvent ne pas être maillés.

L'objectif est donc de disposer de mailles pour l'ensemble des équipements de haute et moyenne importance, et si possible, pour ceux de faible importance.

Les équipements de haute importance sont ceux dont la défaillance a un effet direct sur la production de l'usine ou sa capacité à respecter les règles de sécurité ou réglementaires. Ainsi, les équipements permettant la communication avec l'extérieur sont considérés comme hautement importants. Le classement des équipements selon leur niveau d'importance est défini par un document de référence du groupe Total, rédigé par l'équipe informatique centrale et ayant un caractère obligatoire pour l'ensemble des sites du Groupe.

Dans le cas de la raffinerie de Grandpuits, beaucoup de règles sont déjà satisfaites et l'atteinte de ces objectifs nécessite simplement une formalisation de la hiérarchisation des équipements, une identification des mailles existantes et une mise en œuvre des mailles selon une priorité décroissante en fonction de l'importance des équipements.

10.5. L'objectif dans le temps

Le « long terme » pose une échéance vague. S'il est impossible de fixer une date butoir pour l'atteinte d'un objectif de cette sorte, il est admis qu'il doive être approché de très près dans les dix ans qui suivent sa définition originelle. Afin de mesurer le chemin accompli durant cette période, il est nécessaire de poser des jalons, objectifs intermédiaires permettant de constater des réussites et occasions de faire le bilan ou d'ajuster l'objectif au besoin. Ces jalons sont posés sur une base annuelle puis devront être redéfinis tous les ans. Afin de fournir des éléments utiles pour la négociation annuelle du budget du service Système qui a lieu en juin, l'année est considérée se terminer le trente et un mai de l'année civile.

Les jalons proposés pour les années 2011 et 2012 sont présentés dans le tableau ci-dessous :

Tableau II : Jalons proposés pour mesurer l'atteinte de l'objectif

Date	Jalon
31/05/2011	Production d'un plan d'objectif de capillarité sur un an
	Préconisation d'une solution de gestion de capacité
	Préconisation d'une solution de gestion des risques
31/05/2012	Mesure d'avancement sur l'objectif de capillarité et production d'un plan d'objectif de capillarité sur un an
	Mise en place de la solution de gestion de capacité et analyse des premiers écarts. Préconisation d'actions sur un an
	Mise en place de la solution de gestion des risques et analyse des premiers écarts. Préconisation d'actions sur un an

Les actions nécessaires à l'atteinte de ces jalons sont détaillées dans la partie traitant de la trajectoire d'atteinte de l'objectif. En effet, il a fallu, dans un premier temps, faire l'état des lieux de l'existant avant de pouvoir dresser la liste des actions à mener.

Connaitre ce que l'on possède est en soi une grande richesse. Savoir s'en servir est également une grande source de valeur. Alors qu'aujourd'hui une entreprise doit valoriser au maximum son patrimoine, la méconnaissance des infrastructures informatiques existantes ou de leur fonctionnement conduit à d'importantes dépenses inutiles : perdre du temps et acheter du matériel surnuméraire sont des gaspillages d'argent et d'énergie.

La documentation des réseaux installés sur le site de la raffinerie a pour but de répondre à ces deux questions : que possède-t-on et comment s'en sert-on ?

En premier lieu, un cadre de documentation a été établi, s'appuyant sur des modèles adaptés pour l'occasion. Puis deux exemples, chacun répondant à une question, viendront illustrer la solution retenue.

11. La méthode

Documenter doit s'appuyer sur une méthode facile à apprendre. En effet, rédiger de la documentation est souvent rébarbatif et doit être facilité par les outils mis à disposition pour le faire. L'établissement de la méthode a été réalisé en procédant à un recensement des informations utiles puis en trouvant une approche permettant de structurer ces informations de manière claire.

11.1. Les références méthodologiques

Il n'existe pas de norme ni de référentiel détaillé spécifiquement adapté pour la documentation des réseaux informatiques. La recherche d'information sur ce sujet renvoie invariablement à des solutions de cartographie plus ou moins automatiques du réseau. C'est réduire la gestion du réseau à une simple question d'architecture sans tenir compte des problèmes liés à la nature même du produit transporté : de l'information. Un nouvel arrivant à un poste d'administration d'un réseau doit prendre connaissance, outre de l'architecture de l'installation, des éléments de configuration de celle-ci : les règles d'aiguillage de flux, les mécanismes de protection de la confidentialité, de l'intégrité ou encore du délai d'acheminement des informations par exemple. Ces éléments sont rarement disponibles et souvent dispersés et disparates. Retrouver l'information est alors un défi rendant la transition entre administrateurs délicate et le changement de prestataire risqué. Pour documenter ces informations, il a fallu trouver une approche méthodique qui permette de garantir la clarté, l'exactitude et

l'exhaustivité des informations rédigées. Une partie du projet a donc consisté à réfléchir à la meilleure manière de documenter un réseau et son fonctionnement et donc à créer une méthode de documentation des réseaux.

11.1.1. L'encyclopédie de l'informatique et des systèmes d'information [5]

S'il n'existe pas de méthode formelle, un article de cette encyclopédie aborde la gestion de réseaux informatiques et de services. Cette référence envisage la gestion des réseaux comme une gestion de service et rejoint donc l'approche ITIL. N. Simoni y décrit des modèles de gestion qui se différencient par la réponse à un besoin de gestion. Il y a un modèle qui répond au *quoi gérer ?*, un autre au *qui gère ?*, encore un autre au *pourquoi gérer ?* et un dernier au *comment gérer ?* Cette méthode est une simplification de la méthode QQOQCP. Décomposer le problème en réponses aux questions élémentaires « Qui », « Quoi », « Où », « Quand », « Comment » et « Pourquoi » permet de disposer d'un panorama sémantique. Donner du sens à un problème permet de faciliter sa compréhension, sa modélisation et sa résolution. De plus, répondre à ces questions assure une couverture exhaustive du problème, selon les points de vue des différentes parties prenantes. La décomposition est claire, complète et compréhensible.

Cette approche a l'avantage de proposer une segmentation claire des périmètres en fonction de la question à laquelle ils répondent. De plus, cette organisation correspond à un découpage des responsabilités au sein des DSI. La direction du service informatique répond au quoi et au pourquoi, la direction opérationnelle au comment et les opérateurs au qui. Ainsi, les rôles sont facilement identifiables, ne remettent pas en cause l'attribution actuelle des responsabilités tout en les formalisant. Cette méthode est donc une bonne solution pour décrire une organisation ou un système existant.

Malheureusement, les modèles proposés dans cet article en réponse à ces questions ne répondent pas directement au besoin exprimé par le client dans le cadre de ce projet. Ils ne servent pas directement à produire de la documentation mais à guider un choix d'outil (de supervision essentiellement). Les activités d'administration sont énumérées (maintenance, exploitation, supervision, planification, sécurité) mais elles ne sont pas structurées entre elles, ce qui aurait pu déterminer un squelette de documentation calquée sur l'organisation de ces tâches. La recherche d'outils semble sous-tendue par la volonté d'automatiser au maximum la gestion du réseau. Cette recherche d'un niveau d'industrialisation poussé rejoint l'approche d'ITIL. Mais la

gestion du réseau ne peut se résumer à la contemplation de tableaux de bord mais doit s'appuyer sur des raisons claires expliquant les choix d'implémentation effectués. Ces informations peuvent efficacement prévenir les interruptions de service en permettant de prévoir les impacts d'une modification. Ne pas disposer des raisons ayant conduit à des choix revient à remettre en cause ces choix et finalement à refaire l'analyse à chaque occurrence d'un problème auquel ces choix apportent une réponse.

Outre les pertes de temps et donc de réactivité engendrées par ces multiples analyses, cette méthode de travail comporte plusieurs risques. En premier lieu, elle épuise ceux qui doivent refaire les études et la réaction naturelle est alors de ne pas faire l'effort d'analyse et de tenter les interventions en espérant qu'elles produisent les résultats attendus. Dans les faits, cela se traduit par une perte de maitrise des interventions qui est sensible pour les clients du service : les interruptions sont plus fréquentes et plus longues.

Ensuite, refaire continuellement les études consomme des ressources déjà rares. L'équipe chargée de la gestion du réseau est très restreinte et a d'autres projets à gérer. Perdre du temps sur ces tâches évitables a donc un effet négatif direct sur les coûts des autres projets informatiques.

L'article s'intéresse à la gestion du réseau mais n'envisage pas cette gestion sous l'aspect pratique de la gestion des informations pertinentes pour une bonne gestion ni même la définition de la nature de ces informations. Il précise que la documentation doit exister dès la conception du réseau mais ne s'attache pas à la définir ni à envisager que l'on doive la créer a posteriori. Cependant, dans bien des entreprises ayant construit leur réseau par de multiples itérations, la réalité est bien trop lointaine de la conception pour que la documentation d'étude, quand elle existe, puisse être exploitée.

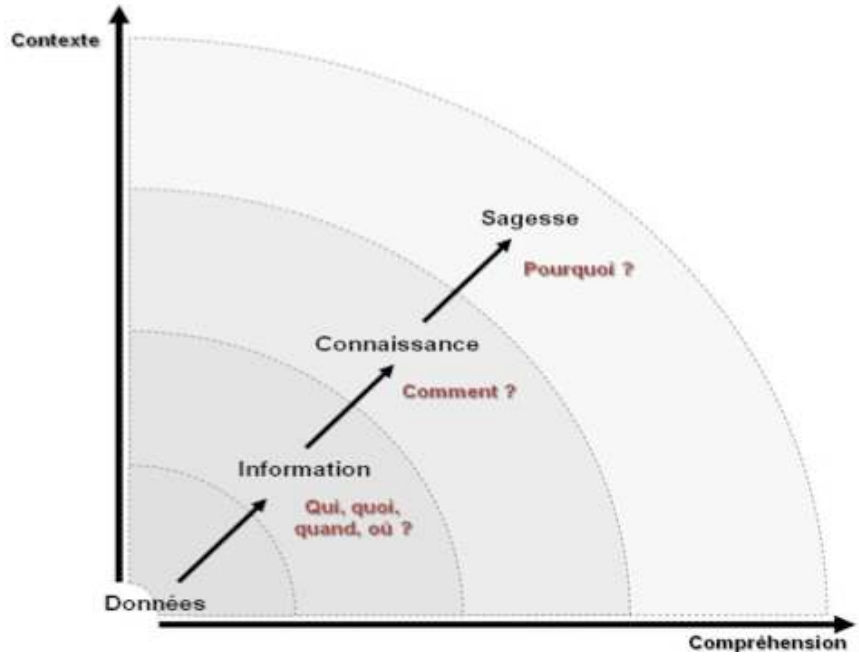
L'apport de cet article dans le cadre de ce projet est plutôt indirect. Il confirme la validité d'une approche par couches successives ordonnées depuis le haut (abstraction maximale) vers le bas (abstraction minimale). Il confirme de rôle essentiel de la documentation dans la gestion du réseau et confirme l'approche orientée « service » du réseau et se rapproche donc d'ITIL.

11.1.2. ITIL

ITIL en version 3 propose un processus de gestion de la connaissance qui semble parfaitement adapté à la finalité documentaire de ce projet. Ce processus a pour but d'améliorer la qualité de la prise de décision en garantissant qu'une information fiable et sécurisée est disponible durant le cycle de vie des services. Il s'appuie sur le modèle DIKW : Data - Information - Knowledge - Wisdom (*données, information, connaissance, sagesse)*.

Il s'agit d'un modèle de maturité, exploitant les questions du QQOQCP pour mesurer l'atteinte d'un niveau de maîtrise. Le but est de passer d'une situation subie, parfois qualifiée de chaos, à une situation planifiée où les incidents ont pratiquement disparu.

Le modèle est représenté par le schéma suivant :



Organisation de la gestion de la connaissance selon ITIL

Dans ce schéma, la progression vers la sagesse est effectuée en travaillant sur l'amélioration de deux axes : la compréhension et le contexte.

Le contexte représente ce qui entoure le service : les briques de la connaissance. Par exemple, dans la zone « Données », l'essentiel est de collecter dans l'environnement toutes les données élémentaires. L'organisation de ces données permettra de les transformer en « informations » et donc de passer à la zone suivante, ce qui correspond à une progression.

La compréhension est l'action effectuée sur les données. Ainsi, dans la zone « Données », la compréhension passe par la recherche et l'absorption de données. Le passage à la zone « Information » est marquée par des actions permettant d'en améliorer la compréhension (classement, recherche...).

ITIL exige, pour un partage efficient des connaissances, un système de gestion de la connaissance. Dans la philosophie ITIL, ce système concentre les informations issues des différents systèmes de supervision et des documents existants. Ces informations sont accessibles via une base de données de gestion de la connaissance capable de traiter des informations sous des formes très variées (textes, plans...) Mais la gestion de la connaissance ne se limite pas à de la gestion d'information. Le système de gestion de la connaissance est capable de traiter l'information, de l'agréger et de la présenter de manière synthétique et opérationnelle.

La mise en place d'un tel système de gestion de la connaissance nécessite de gros moyens : la mise en place, l'alimentation et la maintenance du système sont des tâches lourdes qui ne se justifient pas forcément au regard du périmètre finalement restreint d'utilisateurs. Cependant, la démarche de collecte des informations, de structure de leur stockage et de la facilitation de leur consultation peut être appliquée sans pour autant mettre en place un système complet et coûteux. Dans le cadre de ce projet, une structure de documentation basée sur ces principes a été proposée et implémentée sans nécessiter l'acquisition d'un système de gestion de la connaissance. La solution est certes modeste au regard des possibilités d'un tel système mais suffit à satisfaire les besoins du client.

11.1.3. L'urbanisation des systèmes d'information

L'urbanisation des systèmes d'information apporte une grande rigueur et peut servir de guide méthodologique à la rédaction d'une documentation de ces systèmes. Cependant, les vues sont principalement destinées à décrire des fonctions et des applications communiquant entre elles et l'aspect « communication » est secondaire par rapport à l'aspect « application » qui traite les informations. Dans un réseau, au contraire, la documentation s'intéresse aux flux et à leur acheminement sans prêter beaucoup d'attention aux applications utilisées car elles sont embarquées et très faiblement paramétrables.

Les règles d'urbanisation proposent une hiérarchie de blocs, chaque bloc ne pouvant communiquer qu'avec un bloc du même niveau contenu dans le même bloc de niveau supérieur. Dans les réseaux, il est fréquent de devoir représenter des flux joignant des blocs de niveaux différents, simplement parce que les blocs sont conceptuels mais non réels. Il est donc nécessaire d'assouplir certaines des règles de la méthode d'urbanisation dans ce contexte.

De plus, la transition entre deux niveaux d'abstraction (deux « plans »), est régie par des règles de « passage ». Il est ainsi possible, en connaissant un plan, d'en déduire son voisin par une simple application des règles. Si cette méthode fonctionne bien dans une phase de conception, elle peine à s'appliquer dans le monde réel. Les règles comportent alors tellement de dérogations qu'il devient impossible d'extraire un modèle général de passage d'un niveau à l'autre. Cette difficulté est pointée par N. Simoni[7]. Elle met en avant que chaque niveau d'abstraction se conçoit comme un réseau en tant que tel, indépendant des modèles établis pour représenter les autres niveaux. Ainsi, la communication entre les modèles n'a plus de raison d'être car chaque modèle est autosuffisant pour décrire les services qu'il rend.

La méthode d'urbanisation a donc été exploitée pour créer des plans pour chaque niveau d'abstraction. Elle a permis de s'affranchir de la traditionnelle représentation physique des équipements dans les schémas conceptuels au profit de blocs abstraits au sens clairement établi. L'établissement de ces schémas a été codifié dans un document expliquant la signification des blocs, la manière de disposer les blocs sur un plan et de les connecter entre eux.

La définition des niveaux d'abstraction s'est également appuyée sur deux modèles très utilisés dans les réseaux et donc facilement compréhensibles pour les lecteurs de la documentation. Il s'agit des modèles OSI et IP.

11.1.4. Les modèles conceptuels du réseau

Le modèle OSI (*Open Systems Interconnect — Interconnexion de Systèmes Ouverts*) est un standard (norme ISO 7498[1]) dont le but est de proposer un modèle conceptuel pour la fourniture de services d'interconnexion de systèmes ouverts. Un système est dit ouvert quand il communique avec d'autres systèmes. La norme propose des « prises » standard, permettant à deux systèmes de communiquer entre eux, même s'ils sont de nature différente. Ainsi, un téléphone peut-il communiquer sur un réseau

avec un serveur Internet pour afficher le menu du restaurant d'entreprise ou les prévisions météorologiques. Les services sont standards, au sens de la norme OSI, mais leur implémentation est spécifique selon le périphérique concerné. Cette implémentation est masquée et seuls les services sont visibles par les systèmes voisins.

Le modèle OSI structure la communication en sept couches superposées. Une couche ne peut communiquer qu'avec celles qui l'entourent (celle du dessus et celle du dessous). L'utilisateur se sert de la couche la plus haute qui lui masque toute la complexité de la communication. Chaque couche assure une fonction précise dans la communication. Seule la couche la plus basse, constituée du support physique de communication, permet de dialoguer avec d'autres systèmes. Toutes les autres couches servent à préparer les données pour leur transmission par la couche la plus basse.

Le schéma suivant présente la structure en couches du modèle OSI et le trajet suivi par des communications entre des systèmes. La communication de bout en bout est illustrée par le trait noir. On peut voir la descente verticale des informations à l'intérieur du système source, la transmission sur la couche la plus basse (la communication proprement dite) et la remontée des informations dans le système destinataire pour être utilisées par l'application.

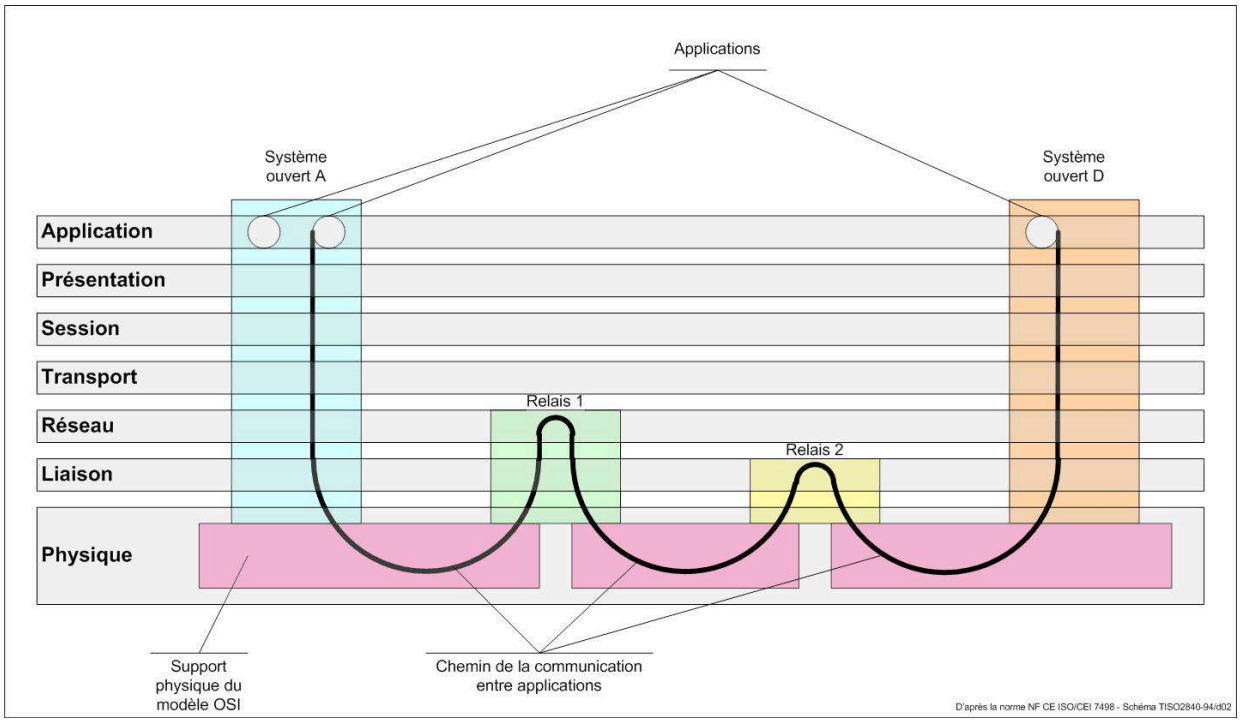


Schéma simplifié du modèle OSI issu de la norme ISO 7498[1]

Ce schéma représente des communications directes de système à système. Cependant, il est rare que les systèmes soient reliés entre eux sans intermédiaire : des équipements sont nécessaires pour relayer le message, voire pour adapter les technologies de transmission aux contraintes (distance entre les équipements, vitesse de transmission…)

Il n'existe pas de possibilité de communiquer directement de système à système sans passer par ce trajet.

Il n'est pas nécessaire que les applications qui communiquent partagent les même technologies. Ainsi, une application web peut dialoguer avec une application lourde.

Les systèmes ouverts ne sont pas tenus d'utiliser les même outils au sein d'une même couche. C'est pourquoi un système Windows peut dialoguer avec un système Unix bien que les applications et le contenu des différentes couches soient développés différemment.

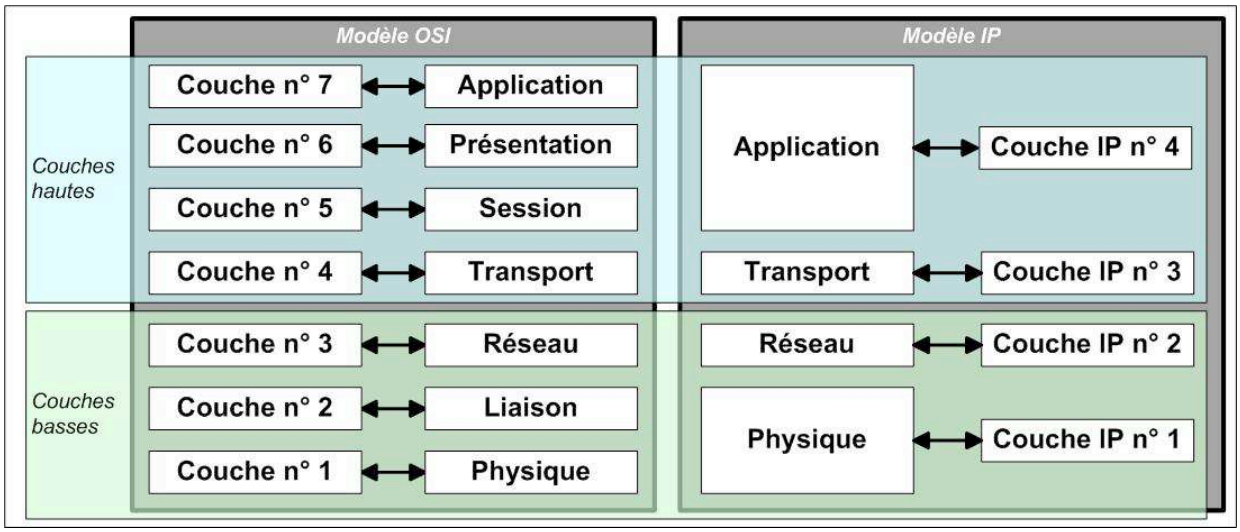
Globalement, chaque couche réalise une fonction définie par la norme. La manière de réaliser cette fonction est libre et dépend des choix du développeur. Cependant, chaque fonction doit rendre un service standard selon la norme : l'entrée et la sortie de la fonction sont précisément définies.

Tout réseau de télécommunication est peut être modélisé selon le modèle OSI. C'est pourquoi l'approche par couche se prête bien à la documentation des réseaux. En effet, la séparation des couches est clairement définie et cette structure apporte une hiérarchie indispensable pour la documentation complète de réseaux complexes. Cependant, le modèle OSI est trop complexe pour être réellement utile dans le cadre de la documentation de réseaux. En effet, les réseaux ne s'intéressent qu'aux couches basses du modèle. C'est pourquoi le modèle IP est plus adapté.

Le modèle IP (*Internet Protocol — Protocole d'internet*) est historiquement antérieur au modèle OSI mais il est spécifique au protocole IP alors que le modèle OSI est universel.

Pour la documentation, le modèle IP est pratique parce qu'il ne demande que quatre niveaux d'abstraction. Le niveau 1 (Physique) permet de prendre en compte les éléments physiques : les switches et les liens qui les relient entre eux. Le niveau 2 (Réseau) est dédié aux éléments propres au réseau : les flux, les adresses IP et les équipements qui les gèrent : les routeurs. Les couches supérieures servent à

documenter les éléments tels que les serveurs et les applications.Le schéma suivant illustre la correspondance entre les deux modèles :



Correspondance entre les modèles OSI et IP

La documentation s'appuie donc sur les techniques d'urbanisation pour la structure en couches et sur le modèle IP pour la décomposition de ces couches. Cette technique est également celle de N. Simoni qui décrit les réseaux comme des entités pouvant se concevoir à différents niveaux, selon les services qu'ils rendent. Ainsi, la documentation de ces niveaux permet de définir les services fournis.

11.2. Que documenter ?

Quelles informations sont nécessaires à la connaissance d'un réseau informatique ?

En premier lieu, il est indispensable de recenser les éléments le constituant. Puis il faut structurer ces éléments par groupes afin de simplifier la représentation par généralisation. Ceci donne une vue « statique » du réseau et permet d'en comprendre la complexité et l'organisation générale. Cet inventaire structuré doit permettre de déterminer facilement la localisation d'un élément, ses liens avec ses voisins et son rôle dans la mission d'acheminement de l'information. Il doit être suffisamment simple pour être lisible et compréhensible mais doit également être exact et exhaustif. Ce sont deux contraintes contradictoires qui ne peuvent être satisfaites simultanément. Il est donc nécessaire de trouver un compromis équilibré préservant l'essentiel des qualités de chaque contrainte.

Il faut également s'intéresser à l'aspect dynamique car un réseau doit permettre d'acheminer une marchandise immatérielle : de l'information. Il faut donc connaître les

itinéraires empruntés pour l'acheminement de la marchandise, les itinéraires de délestage en cas d'encombrements et les conditions à respecter pour que son transport n'altère pas l'information transportée. Un réseau routier comporte des restrictions de circulation : des limitations de vitesse, des itinéraires réservés à certaines catégories de véhicules ou de marchandises... Un réseau informatique comporte également des contraintes sur l'acheminement de l'information : les embouteillages et les collisions existent également sur les autoroutes de l'information. La documentation de l'aspect dynamique du réseau informatique doit permettre d'identifier les sources des problèmes afin de garantir un service d'acheminement en phase avec les attentes de ses clients.

11.3. Pour qui documenter ?

Le public de la documentation détermine le niveau de détail, le niveau de langage et la nature des informations présentes dans la documentation. Quel est le public visé par ces documents ?

En premier lieu, la documentation doit servir au management, afin de connaitre l'ensemble des éléments permettant d'acheminer des informations et de gérer l'atteinte des objectifs. Ensuite, elle peut servir à un nouvel administrateur réseau pour qu'il puisse rapidement être opérationnel.

Ces deux finalités conduisent à la production de documents différents : si les documents destinés aux administrateurs sont par nature très techniques, les informations à l'attention du management sont plutôt stratégiques et ne doivent pas être mélangées avec les détails du fonctionnement des systèmes. Ainsi, les documents doivent s'inscrire dans une structure identifiant leur public. De manière standard en informatique, les informations stratégiques sont regroupées dans des « documents d'architecture » et les informations techniques le sont dans des documents « d'administration » et « d'exploitation » selon leur usage.

11.4. Comment documenter ?

11.4.1. La vision statique

Pour s'orienter, l'être humain s'appuie sur une représentation visuelle des éléments dans un espace. C'est vrai pour le réseau routier dont une carte routière fournit une représentation avec suffisamment d'abstraction pour à la fois être exacte et être facilement lisible. C'est également vrai pour les réseaux informatiques dont une

cartographie peut aider à se représenter une partie de l'architecture tout en en masquant une partie de la complexité. Cependant, de la même manière qu'une carte ne saurait indiquer à elle seule l'état du trafic routier, la cartographie du réseau ne permet pas d'en connaître le fonctionnement mais simplement d'en appréhender la complexité physique.

11.4.2. La vision dynamique

Le réseau sert à acheminer des informations. Il faut donc connaître les trajets utilisés, les lieux et moments de congestion et établir des trajets alternatifs pour ne pas tout bloquer en cas de panne ou de maintenance. L'administrateur doit donc disposer d'une vision dynamique capable de représenter les déplacements d'information et les restrictions qui leur sont imposés. Ces informations peuvent pour partie prendre place sur des cartes. Cependant, pour des raisons de clarté, les restrictions ne peuvent pas y figurer avec une description précise. Ces descriptions doivent donc figurer sur un autre document, nommé ici « document de gestion de flux ». Il contient une matrice des flux, c'est-à-dire un tableau représentant les sources et les destinations d'informations disposées respectivement sur les lignes et les colonnes. La case située à l'intersection d'une ligne et d'une colonne contient une valeur indiquant le type d'acheminement et de restriction éventuelle associée. Un exemple est fourni plus loin dans ce document. Ce document de gestion de flux contient également les informations nécessaires pour comprendre les acheminements en détail et peut être complété par un tableau associant les restrictions mises en place et un descriptif précis.

Le document de gestion de flux est très technique et se destine à l'exploitation du réseau. Dans le cas de l'architecture et de l'administration, il s'agit plutôt d'un document d'organisation des flux reprenant les même éléments mais à des niveaux d'abstraction supérieurs.

11.4.3. Les documents à produire

Il existe de nombreux documents à produire. L'important est de les structurer de manière à faciliter leur identification, leur compréhension et leur mise à jour. L'organisation des documents a permis de créer un index de ces documents. Ainsi, tout document participant au référentiel est listé dans un tableau. Chaque entrée du tableau est un lien hypertexte permettant d'ouvrir directement le document pointé.

Cette astuce permet à la fois d'accéder rapidement aux documents et de fournir une structure claire. Cependant, elle incite à ne pas créer de nouvelle version à chaque mise à jour de document, car si le nom du fichier change, il est nécessaire de reconstruire le lien hypertexte de l'index. Cependant, l'historisation des documents n'est pas obligatoire car la documentation n'a pas, dans ce cas, un rôle de mémoire. Le référentiel décrit l'existant et son fonctionnement et non pas les itérations ayant permis de le réaliser.

Au vu des éléments précédents, la liste des documents à produire s'organise selon le tableau suivant.

Tableau III : Typologie des documents à produire

	Architecture	**Administration**	**Exploitation**
Vision statique	Plan d'architecture générale	Plan d'architecture détaillée	Plan d'architecture technique
Vision dynamique	Document d'organisation générale des flux	Document d'organisation détaillée des flux	Document de gestion de flux

La séparation entre les niveaux d'architecture, d'administration et d'exploitation correspond à la frontière établie par le modèle IP entre les niveaux 1, 2 et 3. L'architecture est une représentation de haut niveau, l'exploitation est chargée de décliner l'architecture et ses évolutions en réalité et l'administration gère le quotidien de cette installation.

Cette segmentation correspond également à celle des publics identifiés ci-avant.

11.4.4. Comment produire les documents ?

La rédaction de ces documents nécessite la collecte d'informations. Il est nécessaire de commencer au plus bas niveau par un inventaire complet des ressources réseau. Ensuite, sur cette base, il devient possible de construire les plans demandés. Cette approche d'ingénierie inverse s'impose dans ce contexte où il s'agit de reconstruire les documents à partir de l'existant.

Tous ces documents sont eux-mêmes divisés en niveaux selon l'approche de séparation des niveaux d'abstraction expliquée précédemment. Cette segmentation de

la documentation selon les niveaux du modèle IP permet de détailler progressivement les informations et donc de faire comprendre plus facilement au lecteur la complexité de l'installation et les subtilités de son administration.

La production des documents requiert de nombreuses itérations. En effet, il est nécessaire de confronter l'écrit au réel pour s'assurer de l'absence d'erreurs. De nombreuses réunions et concertations, souvent informelles, ont été nécessaires pour valider le contenu et la forme des informations placées dans ce référentiel.

12. L'inventaire des ressources

12.1. Le réseau informatique

Le réseau informatique est défini par N. Simoni[7] comme un ensemble de nœuds interconnectés par des liens servant à acheminer un flux.

Les nœuds sont de deux types : soit ils sont dits « terminaux », c'est-à-dire qu'ils utilisent les fonctions du réseau mais ne participent pas à son fonctionnement, soit ce sont des nœuds « centraux », concourant au fonctionnement du réseau. Au niveau d'abstraction réseau, les ordinateurs, serveurs et téléphones connectés au réseau sont des nœuds terminaux alors que les commutateurs (switches) et les routeurs sont des nœuds centraux. À ce même niveau, les liens sont l'ensemble des éléments permettant de relier les nœuds entre eux et se distinguent par la nature de leur substrat : soit en cuivre, soit en plastique guidant les ondes lumineuses (fibre optique).

Plus généralement, N. Simoni identifie ces trois éléments dans un réseau (le flux, le lien et le nœud) sans qu'ils soient liés à un niveau d'abstraction particulier. Si ces termes évoquent naturellement des éléments physiques (par exemple un lien est facilement assimilé à un cordon entre deux nœuds), elle montre que ces termes, selon le niveau d'abstraction considéré, peuvent recouvrir des réalités différentes. Ainsi, au niveau d'abstraction le plus élevé, le nœud sera une application communiquant avec une autre application (un autre nœud) au moyen d'un lien (un service applicatif). Ainsi, le modèle adopté dans ce document est utilisable dans d'autres types de documentation comme celle de systèmes informatiques.

Cependant, ce projet ne s'intéressant qu'à la documentation des réseaux selon les couches basses du modèle OSI, les nœuds seront assimilés à des commutateurs réseau et les liens à des câbles de nature diverse interconnectant ces commutateurs.

12.1.1. Les liens en cuivre

Les liens les plus répandus sont les cordons réseau composés de fils de cuivre et terminés par un connecteur en plastique de type standard RJ-45 : les câbles Ethernet. Ils servent principalement dans les liaisons de courte distance car ils sont inutilisables sur des distances supérieures à 100 m.

Le câble utilisé pour les installations de téléphonie analogique ne connaît pas ces limites de distance (il est utilisable sur plusieurs dizaines de kilomètres) mais ne permet pas de transporter les débits nécessaires aux équipements informatiques actuels. Un câble de téléphone est composé de plusieurs paires de câble car un téléphone nécessite deux fils pour son fonctionnement. Les câbles reliant les bâtiments entre eux peuvent donc disposer de plusieurs dizaines de paires téléphoniques. Le plus volumineux installé dans la raffinerie compte ainsi cent douze paires.

12.1.2. Les fibres optiques

Une fibre optique est un tube en plastique dont l'intérieur est transparent et est conçu pour empêcher la lumière de s'en échapper. Il est ainsi possible de transporter la lumière sur plusieurs kilomètres selon le type de fibre utilisé. La source lumineuse est un laser car sa lumière est naturellement cohérente et se prête donc à un confinement efficace dans le conduit optique. La lumière est modulée (elle varie en intensité au cours du temps) selon un code normalisé et permet donc de transporter les informations entre les nœuds.

La fibre optique est de loin le lien le plus coûteux et le plus complexe mis en œuvre. Il est fragile et supporte difficilement les variations de température, l'exposition à la lumière environnante, les vibrations... Il nécessite de grandes précautions lors de sa mise en place et de son utilisation. De plus, les conditions environnementales spécifiques à la raffinerie imposent des protections supplémentaires. Enfin la grande variété des connecteurs déployés sur le site (SMA, SC, LC, ST, MTRJ...) nécessite d'entretenir un stock très hétérogène de câbles d'interconnexion : les jarretières qui sont des fibres optiques dotées de deux brins et dont les connecteurs sont sertis à la fabrication.

12.2. Le périmètre

La première difficulté soulevée par ce projet est de définir son périmètre. En effet, les ressources réseau sont de natures différentes et il est nécessaire de fixer des limites claires. Un des avantages de cette définition est de rendre possible la sous-traitance de l'inventaire.

Le projet s'intéresse exclusivement aux nœuds centraux et à l'ensemble des liens qui les interconnectent. Sont exclus les liens entre nœuds terminaux et les liens entre les nœuds terminaux et les nœuds centraux. Les nœuds terminaux sont inventoriés à part, soit par leurs responsables dans le cas des serveurs et des ordinateurs de bureau, soit automatiquement par le système de téléphonie dans le cas des téléphones. Les serveurs sont reliés au réseau au moyen de câbles facilement identifiables même sans repérage spécifique et la connexion des équipements de bureau suit la même logique. Il est donc inutile de recenser et documenter ces liaisons. Une exception a été adoptée pour que les liens entre les équipements réseau et les automates soient inclus dans le périmètre. Le périmètre est donc constitué des éléments réseaux actifs (les nœuds centraux) que sont les commutateurs réseau (switches), des liens entre ces éléments (les fibres optiques) et les connexions optiques des automates.

12.3. Les données à inventorier

L'inventaire des switches doit comporter tous les éléments nécessaires à leur identification et à leur exploitation. Il doit donc comporter pour chaque switch un nom unique, une référence de marque, de modèle, des informations sur ses capacités (nombre de ports réseau et leur type), la version de système d'exploitation installée, la localisation physique précise (bâtiment, baie, emplacement dans la baie) et l'appartenance à un contrat de maintenance. Le nom doit également être porté sur l'équipement au moyen d'une étiquette autocollante. Cependant, cette méthode ne permet pas un repérage très pratique : certains équipements ne laissent un espace que de quatre à cinq millimètres de hauteur. Les étiquettes sont donc parfois très difficilement lisibles.

Placer des repères sur les fibres optiques est indispensable. Il est également nécessaire de disposer de documents permettant de connaitre l'existence des liens, leurs qualités et leurs disponibilités. Cette documentation prend généralement la forme de plans permettant d'identifier rapidement les cheminements possibles. Ces plans ne

permettant pas de porter les informations de disponibilité, une solution est de leur adjoindre une liste des usages. Par différence, il est ainsi possible de connaitre les disponibilités de chaque lien.

L'inventaire des fibres optiques se compose donc de trois étapes : identifier le lien, identifier ses capacités et usages et le repérer. Il doit produire trois résultats : un document d'architecture (sous la forme d'un plan), un document de capacité et d'usage des liens et un repère placé sur l'ensemble des liens.

12.4. Le repère physique des liens

Pour distinguer chaque ressource individuellement, celle-ci doit porter un nom unique. Or s'il existe une habitude historique pour nommer les nœuds, il ne s'agit pas d'une convention formelle et les noms sont hétérogènes dans leur forme, rendant possibles des confusions entre équipements. De même, les liens sont parfois nommés, de manière anarchique, à leur création mais le plus souvent ne portent aucune indication.

Une tentative de repérage des liens avait été entreprise par le passé. Cette méthode consistait à placer aux deux extrémités des liens une étiquette imprimée sur du papier ordinaire, découpée et placée dans un support. Cette solution présentait plusieurs inconvénients. En premier lieu, il n'était pas possible de repérer les liens au moment de leur installation car les salles hébergeant ces liens ne disposent pas des moyens informatiques nécessaires (PC et imprimante). Le repérage devenant compliqué il était rarement effectué. De plus, les supports étant petits (5 x 20 mm) l'inscription était difficilement lisible. Enfin, ces supports ne permettaient pas de repérer facilement des liens de petite dimension, tels que des brins de fibre optique.

Afin de déterminer une convention de nommage standard, une approche par la norme IEC 81346[3] a été tentée. Cette norme, intitulée « Systèmes industriels, installations et appareils, et produits industriels -- Principes de structuration et désignations de référence » propose une solution universelle de nommage et de repérage de tout objet et des liens entre ces objets. Elle a l'avantage d'être simple à mettre en place et de fournir une très grande lisibilité des repères. Les informations portent un sens propre (nature de l'équipement selon une nomenclature intégrée à la norme par exemple) et elles sont structurées (des symboles séparateurs portent la signification de la liaison). De plus, la notation est très compacte.

Cette norme n'a malheureusement pas pu être utilisée car sur le site personne ne connaît le code utilisé (elle n'est pas exploitée dans l'usine). Ainsi, ces repères si

pratiques se révèlent être dénués de sens pour leur public et perdent toute leur utilité. Cependant, les principes généraux d'étiquetage ont été intégrés dans la solution retenue telle que détaillée ci-après.

En premier lieu, il a fallu sélectionner l'information à faire figurer sur le repère des liens. Lors d'une réunion avec le chef du service Systèmes et le responsable des infrastructures, nous avons décidé que les seules informations à porter sur un lien étaient les noms des équipements connectés à chaque extrémité du lien. Ainsi, même si l'acheminement d'une communication nécessite la connexion de plusieurs liens pour former une chaîne, chaque élément de la chaîne permettra d'identifier rapidement quels sont les équipements concernés. Cette solution est conforme aux recommandations de la norme IEC 81346 qui précise que les acheminements doivent porter un repère unique sur tous les liens y participant, quel que soit le nombre de connexions intermédiaires.

Ce choix arrêté, il a été possible de quantifier la taille de l'information à porter sur les repères. Un automate est ainsi repéré par une combinaison de cinq à dix caractères. Un switch ou un routeur portent un nom sur vingt à vingt-cinq caractères. La différence de taille a provoqué une réflexion sur la pertinence de porter le nom entier des équipements sur les repères. Cependant, afin de rendre l'identification rapide et unique (sans ambigüités), la mention du nom complet des switches a été adoptée.

De plus, les liens sont de tailles diverses. Des fils téléphoniques d'un diamètre d'un millimètre aux fibres optiques de quatre centimètres de diamètre il était nécessaire de trouver une solution universelle. Celle-ci devait pouvoir s'adapter aux contraintes du site (poussière notamment) et du lien (rayon de courbure des brins optiques par exemple).

Il était important que la solution soit aisément transportable et permette d'identifier les liens rapidement sans nécessiter de matériel compliqué à mettre en œuvre. En effet, une solution contraignante a peu de chance d'être effectivement utilisée au quotidien.

Enfin, cette solution devait être peu coûteuse, même si aucun budget n'avait été arrêté a priori et résister à un usage à long terme (rester lisible malgré les années car certains liens sont en place depuis quarante ans).

Sur la base de ces pré-requis, un tour d'horizon des différentes méthodes de repérage disponibles sur le marché a été effectué. Il existe de nombreuses solutions permettant de placer des repères sur des câbles. Elles vont du plus modulaire (des lettres et

chiffres individuels assemblés manuellement pour former l'identifiant) au plus spécialisé (des étiquettes imprimées sur une imprimante spécifique).

12.4.1. Le repère unitaire fermé pour fil

Ce repère est destiné à repérer les fils individuels. Il permet de générer des codes numériques par assemblage successif de bagues. Afin d'éviter la rotation de ces bagues autour du fil, elles sont clipsées les unes aux autres. Ainsi, la rotation n'empêche pas la lecture de code.

Exemple de marquage de fil par repère unitaire fermé

Cette méthode n'est cependant pas satisfaisante car elle ne permet pas de disposer de lettres (il est donc impossible de former des noms) et surtout il n'est pas possible de l'utiliser sur les jarretières optiques dont les connecteurs sertis empêchent de glisser une bague sur le lien ou sur les câbles.

12.4.2. Le repère unitaire ouvert puis fermé pour fil

Évolution de la solution précédente, il permet d'étiqueter des jarretières optiques malgré la taille des connecteurs car le repère est « fermé » (enroulé autour du brin) par l'opérateur lors de la pose. Cette fermeture est irréversible.

Exemple de repère unitaire ouvert puis fermé

Cependant, il est impossible de repérer des câbles avec cette solution. De plus, il n'est pas possible de disposer de lettres pour former les noms des équipements.

12.4.3. Le repère unitaire pour câble

De même que pour les solutions précédentes, le système repose sur l'assemblage par l'opérateur d'une combinaison de symboles. Cependant, ces symboles sont disposés sur un support, une sorte de barre en plastique terminée par des ouïes permettant de les fixer sur un câble à l'aide d'un collier. Il est ainsi possible de repérer des brins et des câbles pour peu que l'on puisse y fixer un collier de serrage, ce qui dans le contexte présent ne pose aucun problème.

Exemple de marquage de câble par repère unitaire

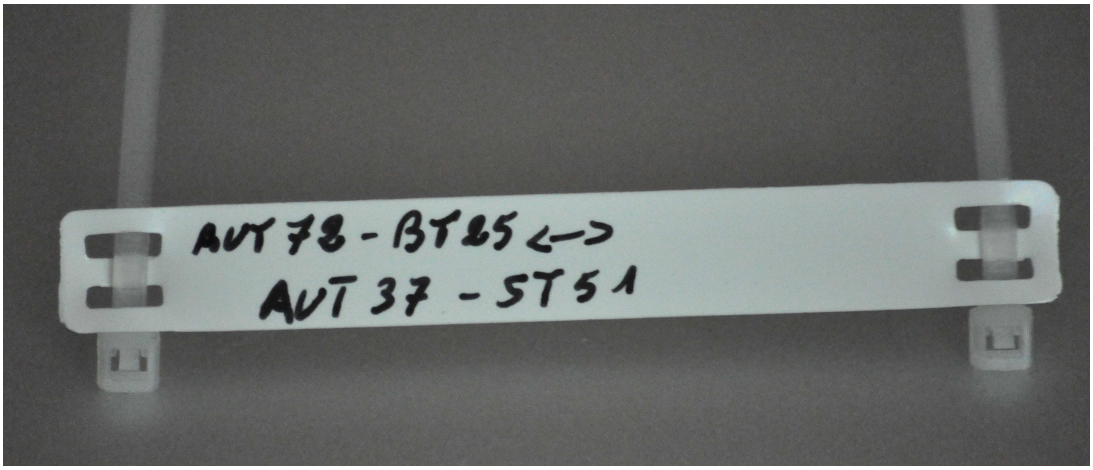
L'inconvénient majeur de ce système réside dans l'espace contraint qu'il réserve aux bagues de symbole. Il est impossible de faire tenir sur un porte-repère l'ensemble des informations nécessaires au repérage selon la convention retenue précédemment.

12.4.4. La plaquette pour fils et câbles

Cette solution est constituée d'une plaquette en plastique blanc percée à ses extrémités pour supporter des colliers de serrage. Ces étiquettes peuvent être rédigées par l'opérateur ou bien imprimées au moyen d'une imprimante spécifique.

Exemple de plaquette pour fils et câbles

Cette solution a été préconisée car elle permet de repérer les liens quelle que soit leur dimension, elle est facile à mettre en œuvre et à retirer, elle permet de repérer des liaisons en place et elle permet de mentionner des noms d'équipement. Cependant, au vu du prix de l'imprimante (environ mille Euros) et du fait que cette imprimante ne peut être facilement transportée sur site (elle ne fonctionne pas sur batterie et elle est lourde et encombrante) et même si les impressions permettent de s'affranchir des variations de qualité de l'écriture manuscrite des différents opérateurs de repérage, les inscriptions manuelles ont été privilégiées.



Exemple d'usage d'une plaquette pour fils et câbles

Le prix de revient de l'étiquette est d'environ un Euro (hors prestation de pose), ce qui est négligeable au regard du prix d'une jarretière optique (environ trente Euros). Cette solution a été adoptée en réunion avec l'ensemble des acteurs intéressés, après étude des solutions alternatives.

12.5. La méthode de repérage

Le repérage doit être à la fois exact et exhaustif. En effet, il importe que toutes les connexions soient étiquetées, mais plus que tout, il faut que les étiquettes comportent des informations exactes. Une information fausse peut conduire à de mauvaises manipulations pouvant avoir un effet désastreux selon l'équipement affecté. Le repérage des connexions n'a donc de sens que si les équipements connectés sont eux-même repérés.

Ainsi, la première étape a été de construire un inventaire des machines connectées aux liens réseau et d'identifier leur appartenance au périmètre défini précédemment. Cet inventaire a permis de recueillir quelques informations primordiales : le nombre

exact d'équipements et leur localisation par exemple. Ces données ont permis de mesurer l'avancement du repérage des liens.

Ensuite, le repérage des liens proprement dit a été délégué à un stagiaire courageux. Il lui a fallu suivre les acheminements brin par brin. Le résultat de ses recherches a permis de dresser une liste exacte des liens d'interconnexion, de leur nature et des acheminements entre les switches réseau. Ce travail considérable effectué avec le plus grand sérieux permet aujourd'hui de connaître les chemins possibles entre bâtiments et les réserves de liens disponibles. Ces informations sont inestimables et utilisées pratiquement quotidiennement. Même s'il subsiste quelques erreurs, la qualité du résultat de cet inventaire est révélatrice d'un important investissement personnel de la part du stagiaire.

Le repérage est une activité fastidieuse et difficile. Chaque fibre optique a d'abord été recensée. Un tableau a été établi, comportant le numéro de la fibre, son tenant et son aboutissant, son nombre de brins ainsi que sa longueur, quand l'information était disponible (environ 15 % des cas). Ce recensement a nécessité de visiter tous les lieux où une terminaison de fibre optique se trouvait ou était supposée se trouver. De proche en proche, en exploitant les informations dispersées dans les baies hébergeant les terminaisons optiques, les divers documents parfois fournis lors de l'installation d'une fibre ou les connaissances des équipes sur place, la liste des fibres optiques a été dressée.

Ensuite, chaque brin de fibre optique a été renseigné dans un tableau. Ce tableau a servi de base à la seconde phase de l'inventaire. Pour chaque brin, le tableau a été renseigné avec l'état du brin (utilisable ou hors service) et le tenant et l'aboutissant de la liaison. Il a fallu examiner les extrémités de chaque brin, tirer délicatement sur les interconnexions de ces brins pour en identifier l'autre extrémité puis renseigner le tableau. Parfois, le brin de la fibre optique est directement raccordé à un équipement, ce qui permet de définir le tenant ou l'aboutissant de la liaison. Parfois, il s'agit juste d'un raccord entre deux brins pour créer un acheminement. Dans ce cas, tant que l'équipement terminal n'est pas connu, il faut se contenter de renseigner la correspondance de raccordement dans le tableau.

La qualité du travail a été contrôlée par confrontation des informations recueillies avec la réalité : des liaisons ont été suivies et l'acheminement ainsi repéré a été comparé avec celui produit lors de l'inventaire et les étiquetages ont été vérifiés. De plus, les

informations sont régulièrement exploitées pour établir des plans lors de projets. Lors de ces travaux, un écart a été constaté sur moins d'un pour-cent des repérages, soit dix erreurs sur environ deux mille brins optiques inventoriés.

12.6. L'exploitation des résultats du repérage

Tout inventaire apporte des surprises. Ainsi, lors des visites de lieux aussi divers que les salles informatiques ou des postes électriques haute tension (de 5 500 V à 63 000 V), de nombreuses anomalies ont été relevées : des acheminements partiellement construits ont dû être retirés, des équipements portant plusieurs noms ont été renommés... Après cette phase de nettoyage, les résultats ont été exploités pour produire les documents attendus : un plan contenant l'ensemble des liaisons optiques recensées sur le site et un document recensant l'ensemble des capacités des liens optiques.

La qualité première d'un plan est la lisibilité. S'il ne respecte pas cette recommandation, il est source d'erreur, de confusion et de mauvaises décisions. Dans le cas d'une raffinerie où plus d'une vingtaine de bâtiments de tailles très variées sont à représenter, l'usage d'un plan à l'échelle est impossible sur une feuille de taille A4 ou A3. En effet, certains locaux seraient invisibles, quand leur taille est de l'ordre de trois mètres au carré sur un site de trois mille mètres de long par quatre mille mètres de large.

Le plan généré ne tient donc aucun compte de l'importance ni de la localisation exacte des bâtiments. Cependant, un soin particulier a été apporté à sa lisibilité afin de permettre une impression au format A3 et une compréhension aisée sur un écran d'ordinateur de 19 pouces (le standard des postes de travail sur le site). Ce plan a été divisé en deux car une zone concentre une densité exceptionnelle de liens et leur représentation perturbait tout le reste du document. Depuis, ce document est mis à jour lors de l'installation de nouveaux liens.

L'ensemble des brins de fibre optique est géré depuis un tableau au format Microsoft Excel. Il contient un onglet par salle constituant une extrémité de lien et dans chaque onglet se trouve un tableau par fibre optique. Chaque tableau contient autant de colonnes qu'il y a de brins dans la fibre et deux lignes. La première ligne contient les équipements connectés au brin de la fibre dans cette salle et la seconde contient les équipements connectés au même brin de la fibre à l'autre extrémité. Voici un exemple de tableau ainsi obtenu pour une fibre de quatre brins.

Tableau IV : exemple de tableau référençant l'usage des brins optiques

	Fibre J234			
Brin :	**1**	**2**	**3**	**4**
Tenant :	Equip1	Equip1	Libre	Libre
Aboutissant	SalleX-Equip3	SalleX-Equip3	Libre	Libre

Cette méthode nécessite la saisie des informations en double car il faut renseigner le tableau des deux salles. Cependant, dans l'attente d'une solution de gestion plus automatisée des ressources réseau, cette approche a l'avantage de la simplicité de mise en œuvre et de la clarté facilitant la compréhension et l'affectation de ressources.

Il existe des solutions informatiques de gestion de câblage. La plus répandue en France est le logiciel R3Web édité par la société Adnfrance. Ce logiciel est déjà présent dans la raffinerie de Grandpuits (premier site de Total équipé). Il est utilisé pour la gestion des acheminements des liaisons téléphoniques analogiques et une extension de son usage aux liens informatiques est à l'étude.

Encart publicitaire placé sur la page d'accueil de la société Adnfrance. (Copie d'écran réalisée le 17 mai 2011 sur le site www.adnfrance.com)

L'usage de la solution pour les liaisons informatiques est subordonné à une formation délivrée par l'éditeur aux équipes locales concernées dont le principe est acquis mais dont la date n'est pas arrêtée.

13. La rédaction des documents

La rédaction a commencé par une recherche documentaire pour aboutir à la construction de la méthode de documentation. Une liste de livrables a été établie sur cette base et validée par le client. Ensuite, ce dernier a validé la proposition commerciale correspondante.

Lors de ce démarrage, un certain nombre de problèmes ont été identifiés. Certains font partie des difficultés classiques lors du début d'un projet (l'organisation du projet, la forme des documents par exemple) mais d'autres sont plus inattendus, tel celle du nommage des éléments dans les documents. Il a fallu à chaque fois analyser le problème pour lui proposer une solution adaptée.

13.1. Les problèmes organisationnels

Dans un premier temps, la production des documents a été abordée de manière hiérarchique : d'abord les documents d'architecture puis les documents d'administration et enfin les documents d'exploitation. Cependant, cette organisation pose un problème : la production d'une documentation complète pour un réseau est très longue puisque chaque niveau n'est entamé que lorsque que la documentation du niveau précédent pour l'ensemble des réseaux est réalisée. Or il y a quatre à cinq réseaux à documenter par niveau et la production d'une documentation d'exploitation utilisable arrivait donc en toute fin de projet, bien trop tard selon les besoins du projet de Total de remplacement de l'infrastructure bureautique. De plus, cette approche ne permet pas de valider la démarche sur la documentation d'un réseau avant la fin du projet et ainsi rend les corrections méthodologiques très lourdes à apporter et surtout risquent de faire dériver la durée du projet.

Lors d'une réunion d'avancement, alors que les premiers documents d'architecture ont été relus et commentés, il a été décidé d'apporter plusieurs modifications aux documents sur la forme (ajouts de légendes, de précisions sur la méthode...) et sur le fond (corrections d'erreurs, précisions à apporter...) mais surtout de se concentrer sur la production de la documentation complète du réseau bureautique. Ce travail doit permettre de valider l'ensemble de l'approche tout en produisant au plus vite les documents dont le projet de remplacement des postes bureautique a besoin de manière urgente.

Le premier document produit après cette réunion a été une référence portant sur la méthode de documentation. Les modèles OSI et IP ont été présentés et l'approche

générale des documents a été explicitée. Ce document, après validation par le client, a servi de référence pour produire la documentation complète du réseau bureautique, depuis la vision globale très abstraite jusqu'à la description technique détaillée. Ainsi l'ensemble de la méthode a été confronté à la production concrète de documents.

13.2. Les problèmes méthodologiques

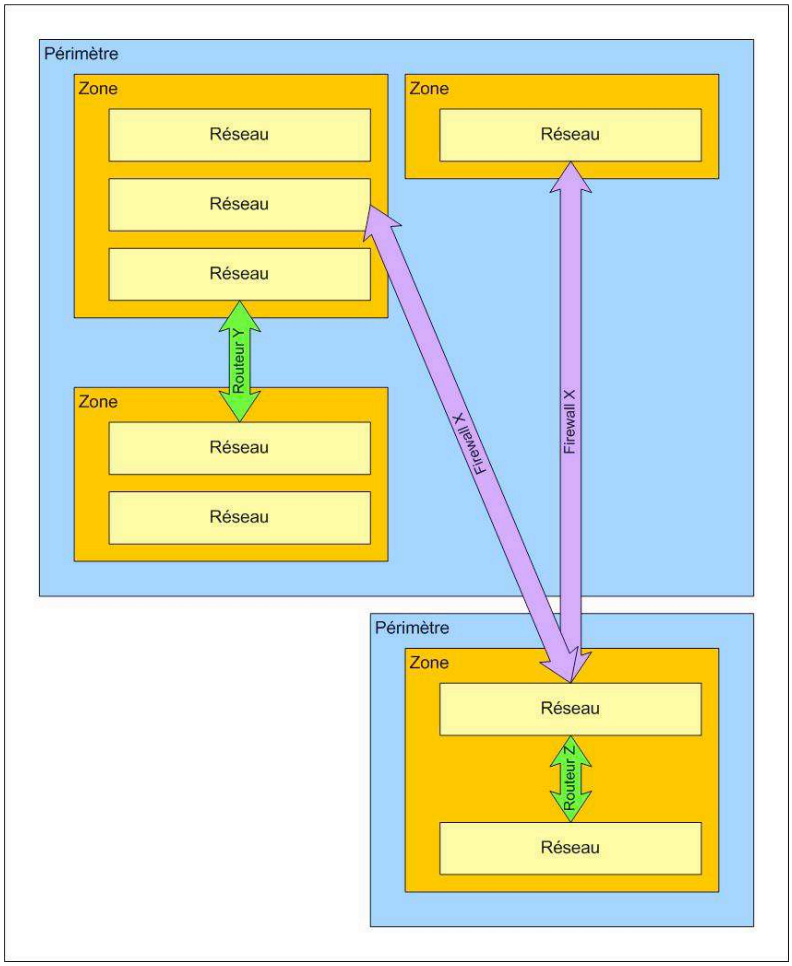
Quelques ajustements ont été nécessaires lors de la confrontation de la méthode à la réalité de la production documentaire. Ainsi, les structures de schéma, au départ plutôt axées sur une représentation géographique répartissant les informations sur un plan ont été modifiées pour adopter une structure hiérarchique dans laquelle des blocs en contiennent d'autres ou y sont connectés. Cette représentation tirée de la cartographie adoptée dans les méthodes d'urbanisation des systèmes d'information permet de grouper des éléments par niveaux d'abstraction. Cette cartographie a l'avantage d'être facilement compréhensible, même pour les lecteurs dont ce n'est pas le domaine de compétence principal.

La cartographie selon la méthode d'urbanisation des systèmes d'information repose sur le « bloc ». Un bloc est une unité de représentation. Dans le cas de la documentation des réseaux, un bloc peut représenter, selon le niveau, des équipements réseau ou bien des services plus abstraits. Un bloc peut être contenu dans un autre bloc, selon une hiérarchie précise. Cette hiérarchie, après discussion avec le client, a été limitée à trois niveaux afin de rester claire et lisible. Elle est présentée ci-dessous.

Hiérarchie des blocs dans un même niveau d'abstraction

Dans le principe de la méthode d'urbanisation, chaque bloc ne peut communiquer qu'avec un bloc de même niveau hiérarchique et situé dans le même bloc de niveau supérieur. Par exemple, il est normalement interdit de faire communiquer deux réseaux situés dans des zones différentes. Ce sont alors les zones qui doivent communiquer entre elles, si elles sont situées dans le même périmètre.

Cependant, il a été nécessaire de s'écarter de cette règle. En effet, les blocs de type « périmètre » et « zone » ne servent que de repère conceptuel mais n'ont pas de raison d'être technique. Ainsi, dans la documentation, la communication entre un réseau d'une zone et un réseau d'une autre zone, voire d'un autre périmètre, est autorisée. Cette exception est permise à condition de ne concerner qu'un seul réseau d'une zone (celui-ci jouant le rôle d'interlocuteur unique avec l'autre zone) et que la représentation orthodoxe ne soit pas conforme à la réalité. Une carte complète peut donc prendre l'aspect ci-dessous



Exemple de carte contrevenant aux règles d'urbanisation

Cette carte, fictive, illustre des zones où des réseaux ne communiquent pas entre eux, d'autres qui communiquent avec d'autres zones via différents équipements (routeur et firewall). Sur cette carte, il est aisé d'identifier les chemins possibles entre les réseaux. Ainsi, il devient facile d'établir le trajet des informations entre deux réseaux et de comprendre l'effet d'un changement de règle sur un équipement. Cette représentation a été souvent exploitée depuis sa réalisation lors de dépannage de problèmes de communication entre différents réseaux. Elle a démontré qu'elle est compréhensible,

même pour une personne étrangère au fonctionnement des réseaux. C'est même un outil pédagogique qui a été utilisé pour démontrer le respect des règles de sécurité imposées par le référentiel de Total.

Une règle fondamentale de la méthode d'urbanisation porte sur le nom des éléments. Chaque bloc doit porter un nom unique. Cette règle a été adoptée et a posé quelques problèmes détaillés dans la section suivante.

De plus, il est nécessaire de produire plusieurs cartes, en fonction des besoins du lecteur. Trois cartes ont été produites. La première est un schéma d'architecture, destiné à la compréhension du fonctionnement pour un nouvel administrateur et présentant de manière abstraite les réseaux et leurs liens de communication. Selon N. Simoni, cette description à un haut niveau d'abstraction permet de mettre en évidence les services rendus par le réseau. Ensuite, une carte décrivant les réseaux tels qu'ils sont implémentés physiquement permet à l'administrateur et à l'exploitant de visualiser la constitution logique des réseaux. L'exemple précédent est tiré de ce niveau. Enfin une carte de bas niveau représente les éléments situés à la périphérie des périmètres réseau considérés et est destinée à mettre en évidence les équipements et liaisons critiques. Cette carte doit faciliter les interventions d'un administrateur en cas de problème.

13.3. Les problèmes d'identification

Les problèmes de communication sont, on le sait, source des plus grands maux de l'entreprise. Or il est surprenant de constater qu'ils surviennent également dans des domaines très techniques, là où le vocabulaire est supposé être le même pour tous. Il n'en est rien.

La production des premiers documents a mis en évidence des problèmes assez sérieux de nommage et de représentation des périmètres réseau. Ainsi, des termes représentant pour les uns un périmètre tout entier ne s'applique pour les autres qu'à une petite portion de ce périmètre. De même, plusieurs éléments des plans portaient le même nom. L'écriture de ces plans selon l'approche de l'urbanisation a permis de mettre en évidence ces incohérences. Les règles d'urbanisation sont strictes : chaque élément doit porter un nom unique représentant sa fonction. Dans le cas présent, mettre un nom unique dans chaque case a nécessité de nombreuses itérations des plans et une consultation fréquente des différents lecteurs concernés pour valider un vocabulaire et un découpage appropriés.

De plus, ITIL apporte un vocabulaire standard pour définir les objets informatiques. Un incident, un problème, une base de données de gestion des configurations (CMDB — Configuration Management Database) sont désormais des éléments clairement définis pour l'ensemble des informaticiens, quelque soit leur domaine de spécialité. ITIL a réussi à imposer ce que la norme NF Z61-000[4] (Vocabulaire international de l'informatique) n'est pas arrivé à démocratiser : un langage commun. Là où la norme NF Z61-000 se contentait d'inventorier de manière assez sèche les termes informatiques courant et leur associait une définition, ITIL a illustré les termes dans leur contexte et a utilisé ces termes dans tous ses documents, les rendant incontournables. Cependant, nombre de termes définis par ITIL sont issus de la norme NF Z61-000.

Dans les documents produits au cours de ce projet, de nombreux termes et concepts ITIL (processus, activité, tâche et leur hiérarchie par exemple) ont été mis à profit car leur définition universelle est garante de la facilité de compréhension des informations. Cela évite les ambigüités et assure une transmission aisée des connaissances.

Apporter un vocabulaire unique sur des représentations formelles permet de faciliter la compréhension mutuelle et donc le travail en équipe. C'est un des apports principaux de la documentation pour le client.

13.4. L'audit des configurations

La rédaction de la documentation du réseau a fait apparaître des écarts de configuration sur des équipements supposés être paramétrés de manière identique car rendant les même services. Ces écarts rendent la maintenance difficile car ils demandent de la part de l'opérateur une bonne compréhension de leur raison d'être avant l'action. Un audit des configurations a donc été réalisé pour pouvoir enrichir les objectifs à court et moyen terme.

13.4.1. Les résultats attendus de l'audit

L'audit doit produire une liste de paramètres standards correspondant à la meilleure configuration attendue par type d'équipement. Ensuite, sur la base de cette liste, une liste d'équipements sera établie, identifiant ceux qui sont conforme au standard établi et ceux qui nécessitent des changements de configuration. Cette liste servira de base à l'établissement d'un planning de mise en conformité, l'objectif étant alors de mettre en conformité les équipements au fur et à mesure de l'identification d'écarts.

13.4.2. L'identification des valeurs correctes des paramètres

L'intérêt et la difficulté de l'audit des configurations est d'identifier les valeurs correctes des paramètres. Pour cela, la documentation précédemment établie est indispensable. Elle est source d'information et outil de contrôle. Ainsi, si des configurations s'écartent de l'architecture mise en place, c'est la documentation qui permettra d'identifier, de mesurer et de réduire ces écarts.

Cependant, la documentation ayant été établie sur la base de l'existant, puisqu'elle est dérivée d'un inventaire, elle ne saurait servir de référence sans être préalablement critiquée. En particulier, si une information placée dans la documentation est fausse, il faut la corriger plutôt que de dérégler le réseau.

La documentation n'est pas la seule source de référence. Les besoins d'administration peuvent imposer des paramètres spécifiques. C'est le cas, par exemple, de la taille du journal des événements d'un équipement réseau. Ce journal est très utile en cas de problème : il est la première source d'information et de diagnostic. Cependant, les équipements réseau ont un espace mémoire assez limité qui ne permet pas de conserver une trace de tous les événements sur une période infinie. Ce n'est pas non plus souhaitable car l'affichage des événements se fait par ordre chronologique, les plus anciens étant affichés en premier. Si la liste des événements est trop longue, elle devient inexploitable, particulièrement dans des cas d'urgence où une réponse doit être apportée sans délai. Cependant, il faut que la liste soit suffisamment complète pour permettre un diagnostic. De plus, il est possible d'adapter la nature des informations placées dans le journal de manière à ne conserver que celles qui sont pertinentes. Trouver la bonne « profondeur », la bonne taille pour la liste consiste donc à établir un compromis entre le niveau de détail attendu, la quantité d'événements à stocker et la facilité à les exploiter. Ce compromis est établi sur la base de l'expérience de l'administrateur et de la nature des problèmes rencontrés en fonction des équipements et de leurs capacités.

13.4.3. La réalisation de l'audit

Dans un premier temps, beaucoup d'informations ont été collectées. Les configurations individuelles des équipements ont d'abord été regroupées par périmètre afin de disposer d'ensembles comparables. Ensuite, la documentation a été exploitée pour identifier les paramètres directement liés aux besoins, comme par exemple ceux

qui peuvent influer sur la qualité des acheminements. Ainsi, les paramètres déterminant les chemins « primaires » et les chemins « de secours » ont été établis sur la base des spécifications documentaires. Les incidents importants de l'année en cours, ceux qui ont occasionné une interruption de service remarquée, ont été analysés afin de déterminer leur cause, les paramètres liés à ces causes et les valeurs à mettre en place pour éviter leur survenue, diminuer leur effet et faciliter leur diagnostic.

Ce travail d'inventaire a permis de dresser une liste des paramètres importants pour le réseau. Ces paramètres ont soit été identifiés par la documentation comme influençant directement le service aux clients soit identifiés par l'analyse des incidents comme ayant eu un impact sur le service. Pour chaque paramètre, une valeur optimale a été arrêtée. Cette valeur a été déterminée sur la base des recommandations constructeur quand elles sont disponibles, par comparaison avec des équipements n'ayant pas eu d'incident ou par retour d'expérience.

Enfin, sur la base de cette liste, l'ensemble des configurations a été recensée pour identifier visuellement les écarts. Ce recensement a été effectué manuellement car il n'existe a priori pas de moyen simple de comparer les configurations de manière automatique. Une tentative a été effectuée en utilisant un outil capable de comparer les fichiers et de mettre en évidence les différences de contenu. Cependant, de nombreuses différences sont normales et génèrent un « bruit de fond » considérable, noyant les écarts réellement importants dans un flot de légères différences. L'outil ne disposant pas d'une fonction permettant d'ignorer certains écarts et la relecture des écarts devenant bien plus longue que le simple parcours de la liste des paramètres de configuration, cet outil a été abandonné.

Certains paramètres peuvent être différents de la consigne (si un journal est plus grand que spécifié, ce n'est pas grave), incitant à tolérer des écarts pour restreindre le nombre de modifications à apporter. En effet, chaque changement est effectué manuellement et donc comporte un risque d'erreur. La limitation du nombre de changements est donc une manière d'éviter de créer des incidents en tentant d'améliorer le réseau.

Dresser cette liste a eu des conséquences inattendues car aucun de la centaine d'équipements inspectés n'était entièrement conforme. De plus, un certain nombre de paramètres nécessitent des précautions lors de leur changement pour ne pas

engendrer de rupture de service. Ce qui, au départ, devait être une simple confrontation de la documentation à la réalité est devenu un projet à part entière de par la taille de son périmètre et l'étendue des risques que la mise en conformité fait courir sur le service. C'est pourquoi les changements nécessaires à la mise en conformité n'ont pas été appliqués dans la continuité de leur recensement mais font partie de la trajectoire d'atteinte des objectifs.

Tableau V : exemple de tableau listant des paramètres de référence

Catégorie	Paramètre	Valeur de référence	Équipement 1	Équipement n
Journalisation	Taille du journal	1000000	OK	OK
	Type d'événement j	Informational	NOK	OK
	...	...	...	...
Contrôle d'accès	Login de l'administrateur	root	OK	OK
	Chiffrement des mots de passe	Activé	OK	NOK
	...	...	...	...
...	...	...	...	...

Cette inspection a donc permis de dresser une liste des paramètres non conformes par équipement, permettant ainsi de disposer d'une vue sur l'étendue de l'effort de mise en conformité à fournir. Cette vue contient également les éléments d'analyse de risque (non représentés ci-dessus), ce qui facilite la planification des opérations de mise en conformité en identifiant les opérations pouvant être menées en heures ouvrées sans impacter le service et celles nécessitant d'intervenir en dehors des périodes d'utilisation des réseaux.

La mise en conformité proprement dite est ainsi planifiée sur plusieurs mois. Les paramètres les plus critiques seront modifiés au cours d'opérations de maintenance tel qu'il s'en produit une tous les deux ou trois ans sur le site.

14. Bilan de la rédaction documentaire

Dresser la documentation (inventorier l'existant, concevoir et rédiger les documents de référence, auditer l'existant sur la base de ces documents) a coûté du temps et de l'argent. Elle a mis en évidence des problèmes de conception qui ont débouché sur une liste d'actions correctives à effectuer. Ces actions sortent du périmètre de ce projet et seront menées sur le long terme.

La lecture des règles imposées par le groupe Total ou la branche Raffinage & Marketing à la raffinerie a permis de faciliter la réalisation d'un audit de conformité réalisé en auto-évaluation depuis la fin du mois d'août 2011. Les écarts ont pu être facilement identifiés et quantifiés. Les résultats sont encourageants car il existe peu de points de non-conformité.

Les directives des référentiels internes sont également une caution forte pour certains projets, notamment de sécurisation des réseaux informatiques. Ces documents imposent pas exemple la documentation des réseaux, même s'ils ne proposent pas de modèle documentaire.

La documentation a représenté un travail d'environ six mois à temps plein, répartis sur deux ans. Ce temps a été employé à recenser, indexer, trier et lire les documents existants. Ensuite, les référentiels ont été exploités pour en extraire les informations relatives au réseau. Enfin, la structure de la documentation a été conçue pour faciliter la lisibilité et la compréhension des informations. La rédaction des documents a occupé près de deux mois à temps plein dans le cadre de ce projet.

Même si le coût de la documentation est difficile à établir, sa rentabilité n'est pas mise en doute. En effet, le remplacement de l'administrateur réseau est envisagé sereinement et la gestion des infrastructures de communication de la raffinerie est grandement facilité et fiabilisé. La documentation apporte une valeur indéniable à la prestation d'administration. C'est également un gain pour la sécurité du site puisque les installations gérées assurent pour partie le transport d'informations vitales pour la production du site et la protection des installations.

La mise à jour régulière des documents est inscrite dans les modes opératoires d'administration afin de garantir la pérennité de cet investissement et de préserver le niveau de sécurité acquis. Sans cela, la validité des documents ne dépasse pas quelques mois.

Les outils de gestion

La satisfaction des objectifs définis en première partie ne peut être instantanée. C'est à la fois impossible techniquement et très risqué. Or le contexte particulier d'une raffinerie exige de minimiser les risques s'il n'est pas possible de les éliminer totalement. Une trajectoire d'atteinte des objectifs est donc nécessaire.

Quels sont ces objectifs ? Il y en a trois grands :

1. La capillarité, afin de mettre le réseau à portée de chaque bâtiment où il risque d'être nécessaire.
2. La capacité doit permettre d'adapter le réseau aux besoins.
3. Le maillage du réseau doit le rendre résilient.

Comment atteindre ces objectifs ? Ils nécessitent de pouvoir mesurer la situation existante et l'atteinte des objectifs. Pour ce faire, il faut disposer d'outils de gestion.

La première partie de ce document a montré la nécessité de disposer d'informations en temps réel sur le fonctionnement du réseau. Une partie de la documentation est générée automatiquement par des outils permettant de disposer d'informations sur l'état du réseau. Ces outils sont indispensables pour mesurer l'atteinte des objectifs. Si l'établissement de plans de capillarité peut être effectué manuellement, les mesures de capacité et de maillage sont facilitées par ces outils.

Avant de s'intéresser directement aux actions à mener pour atteindre les objectifs, une réflexion est donc nécessaire sur les outils existants, afin de déterminer s'ils sont adaptés à la nouvelle manière de gérer le réseau et de mesurer l'atteinte des objectifs fixés.

Les prochains paragraphes s'intéressent donc principalement à la gestion outillée des réseaux, avant de passer aux actions nécessaires pour atteindre les objectifs.

15. Les protocoles de gestion de réseaux

Selon N. Simoni[7] et G. Pujolle[6], la gestion des réseaux est une démarche outillée pour visualiser l'état du réseau et disposer d'une aide au diagnostic en cas de problème. Ces outils sont des logiciels exploitant les protocoles standards de gestion de réseau. Il en existe plusieurs mais le plus répandu est SNMP[8] — Simple Network Management Protocol. Cisco a développé un autre protocole, CDP[9] — Cisco

Discovery Protocol — qui permet de compléter SNMP en découvrant automatiquement les topologies réseau.

15.1. SNMP

15.1.1. Présentation générale de SNMP

SNMP[8] — Simple Network Management Protocol — est une norme Internet décrite par la RFC 1157 pour le protocole de communication et par la RFC 1156 pour la structure des données. Elle est issue du besoin de gestion des réseaux TCP/IP et a été conçue pour être compatible avec les normes OSI.

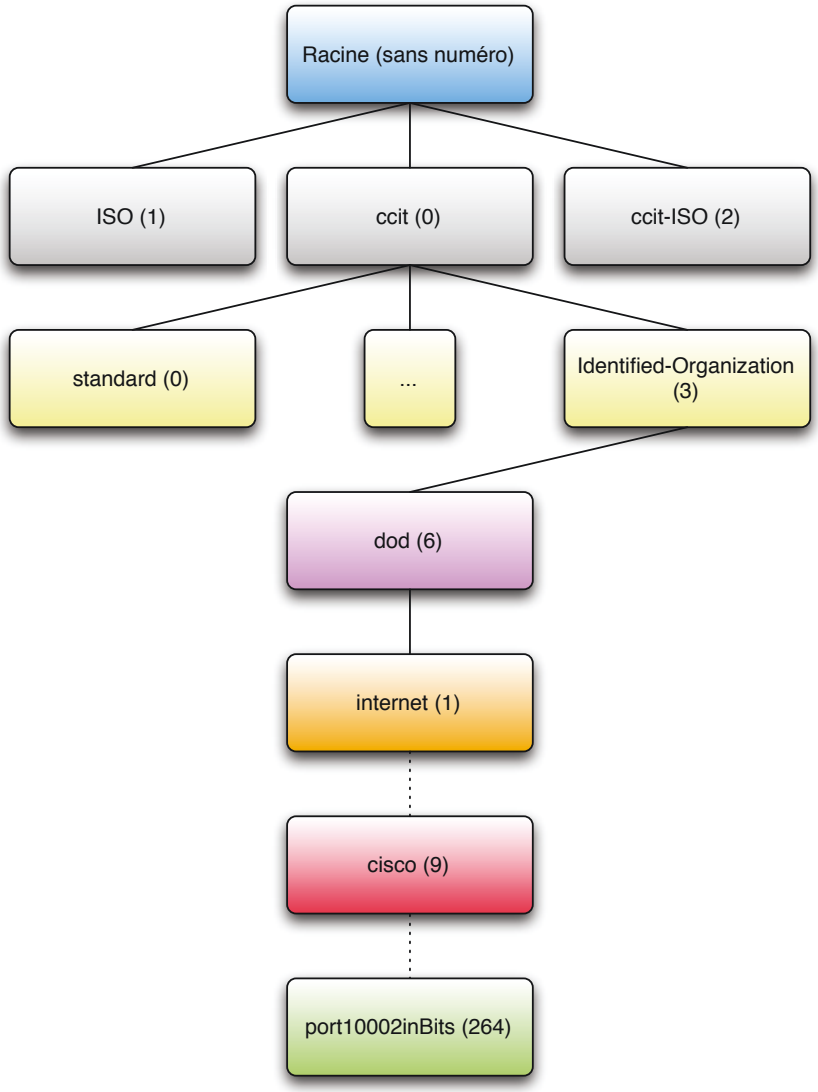
SNMP est un protocole de niveau trois du modèle OSI et repose sur deux types de composants du réseau : des agents et des serveurs. Les agents sont des nœuds du réseau géré. Les serveurs collectent les données des agents et leur donnent des instructions de configuration.

15.1.2. La MIB SNMP

L'agent stocke les informations dans une MIB — Management Information Base, sorte de micro base de données propre à chaque agent. Cette MIB est alimentée par l'agent qui y stocke les informations que le constructeur a jugées pertinentes. Dans le cas d'un commutateur réseau par exemple, on y trouve des informations propres au matériel (la liste, le type, les capacités et le nom des ports réseau...), des informations sur l'environnement (la tension électrique d'entrée, les différentes tensions générées par l'alimentation, la vitesse de rotation du ou des ventilateurs, la température ambiante...) ou des informations sur le réseau (quantité de données échangées par port, par VLAN...).

15.1.3. L'OID SNMP

Chaque information est désignée par un identifiant unique. Cet identifiant, l'OID — Object IDentifier, identifiant d'objet — est spécifique à chaque constructeur, matériel, modèle voire même version de modèle. Désigner une information contenue dans une MIB revient donc à interroger son OID. Les OID sont organisés selon une structure arborescente. Chaque nœud porte un numéro. Le principe d'organisation de la structure de données d'un agent est donc le suivant :



SNMP : schéma de principe de l'organisation des OID

Ainsi, l'OID du compteur de bits entrés sur le port 2 de l'équipement considéré est noté : 1.3.6.1.4.1.9.3.3.2.264. Il est possible, en utilisant des fonctions SNMP, d'énumérer les feuilles d'un nœud. Connaitre l'ensemble des ports réseau disponibles revient à interroger la MIB 1.3.6.1.4.1.9.3.3 (celle qui précède les ports proprement dits) et à lui demander la liste de tous ses successeurs. Cette fonction est très pratique pour établir des inventaires matériels différenciant les ports utilisés et libres.

Cependant, seules les informations proches de la racine de l'arbre sont normalisées (jusqu'au niveau des constructeurs, Cisco dans cet exemple) : chaque constructeur reste libre d'organiser les informations comme il l'entend. De même, les données stockées peuvent être de types très différents : les températures sont souvent des nombres décimaux assez petits, les volumes échangés sur un port sont des nombres entiers très grands, les descriptions sont des chaînes de caractère... De plus, les OID,

contrairement au schéma précédent très simplifié, peuvent comporter plus d'une quinzaine de nœuds, ce qui les rend dans la pratique impossibles à manipuler tel quel.

15.1.4. Les fichiers MIB SNMP

SNMP prévoit donc un système permettant de lier des noms à des OID, un peu à la manière de DNS — Dynamic Name Service — qui permet de consulter des sites Internet en saisissant un nom plutôt que l'adresse IP du serveur. Ces informations sont regroupées par type de MIB dans des fichiers au format normalisé. Par exemple, Cisco propose un fichier de description de l'ensemble des OID nécessaires pour effectuer la sauvegarde des équipements réseau. Ce fichier contient des noms mnémotechniques tels que « serverAddress » qui permet de définir le serveur vers lequel l'équipement devra écrire la sauvegarde ou « protocol » qui précise le protocole à utiliser pour la copie. Ces noms sont exploitables par les logiciels de gestion de réseau, pour peu que ces fichiers de description leur soient accessibles. Ces fichiers ne contiennent que les informations précisément liées à leur fonction. Cependant, ils peuvent eux-même être liés à d'autres fichiers de même type afin d'étendre des fonctions précédemment définies. Dans ce cas, il est nécessaire de disposer de l'ensemble des fichiers pour pouvoir réaliser une fonction. Ce système très modulaire est à rapprocher de celui des librairies utilisé lors du développement d'applications.

Les fichiers de « haut niveau », liés au protocole SNMP mais pas au matériel, sont standards. Il en est ainsi pour le fichier détaillant les OID liés à SNMP version 2 et qui sert de base à tous les autres fichiers. Ces fichiers permettent d'accéder plus simplement aux données des MIB des agents et sont donc appelés des « fichiers MIB ». Cependant, ils ne contiennent pas de données mais simplement le moyen d'y accéder plus facilement. Un fichier MIB n'est donc pas nécessaire pour accéder aux informations SNMP d'un agent. Sur le site de Grandpuits, le système de sauvegarde des équipements réseau ne se base pas sur un fichier MIB mais sur les OID directement. En effet, l'arborescence des fichiers MIB est complexe, avec beaucoup de dépendances, ce qui rend la configuration compliquée alors que la sauvegarde ne nécessite que la manipulation d'une dizaine d'OID.

15.1.5. Les échanges SNMP

Le serveur interroge les MIB afin d'en récupérer les données. Les équipements réseau sont pauvres en mémoire et ne peuvent donc pas gérer un historique des valeurs.

Pourtant, il est important de pouvoir se baser sur des données historiques pour mesurer des tendances. Cette fonction est donc recréée par le serveur qui, au fil de ses interrogations, alimente sa propre base de données avec l'ensemble des valeurs collectées. Le résultat de cette interrogation régulière de l'agent par le serveur est une information de disponibilité (l'agent est présent sur le réseau et est capable de répondre aux demandes du serveur) et des informations de qualité de fonctionnement (les valeurs sont dans un intervalle acceptable ou non, ce qui peut provoquer le déclenchement d'une alerte).

La communication entre un agent et un serveur peut être initiée par le serveur, lors d'une interrogation régulière. Dans ce cas, le serveur collecte les valeurs de compteurs que l'agent place dans ses MIB. Le serveur peut également donner des instructions de configuration aux équipements qu'il gère. Il est ainsi possible de remettre à zéro des compteurs, de modifier des seuils d'alerte ou de configurer des sauvegardes de configuration.

L'agent peut informer le serveur d'un dysfonctionnement. Ce message d'alerte est nommé « trappe » SNMP car il se rapproche de la « trappe » système informant un système d'exploitation d'une erreur irrécupérable dans un processus. Le serveur dispose d'un système de réception et de traitement des trappes générant des alertes aux administrateurs réseau. Ces alertes sont diffusées sous forme de courriel et parfois de SMS, voire même de messages vocaux préenregistrés. La gestion des trappes est importante car elle permet de minimiser le temps d'indisponibilité des équipements. Il arrive même qu'une trappe signalée et gérée à temps rende le dysfonctionnement invisible pour les utilisateurs. Ce système est donc indispensable pour maintenir une bonne disponibilité du réseau.

15.1.6. La sécurité de SNMP

SNMP est un protocole très puissant. Il est le standard de fait pour l'ensemble des réseaux reposant sur TCP/IP et tous les équipement réseau professionnels renferment un agent SNMP. Certains serveurs sont également compatibles avec SNMP, ce qui permet aux serveurs SNMP d'élargir la gestion du réseau à la surveillance des éléments périphériques. Cependant, comme nombre de normes Internet, la sécurité n'a pas été prise en compte lors de sa conception. Il a fallu attendre la troisième version du protocole pour que la communication entre l'agent et le serveur puisse nécessiter une authentification. Pourtant, avec SNMP, il est possible de récupérer,

corrompre et ré-implémenter la configuration d'un équipement. Cette mise à mal du réseau, pour peu qu'elle soit effectuée sur un nombre limité d'équipements stratégiques du réseau (trois équipements à la raffinerie de Grandpuits par exemple), permet de rendre indisponible l'ensemble du réseau en quelques secondes. Ce type d'attaque est très facile à mener, il suffit d'un accès au réseau pour récupérer les informations nécessaires car elles circulent « en clair », sans aucun type de chiffrement. Même si SNMP v3 est supporté par un nombre croissant d'agents, la reconfiguration des serveurs de supervision est ardue et le plus souvent négligée car il s'agit d'un projet à part entière, consommateur de ressources et générateur de risques.

Les directives de sécurité édictées par le Référentiel Sécurité du groupe Total imposent le recours à SNMP en lecture seule exclusivement. Cependant, dans bien des cas, l'écriture SNMP est le seul moyen de donner l'ordre à un équipement réseau de faire une sauvegarde de sa configuration sur un serveur réseau. L'obligation de sauvegarde régulière des équipements réseau figure également dans le Référentiel Sécurité Groupe. La conciliation de ces directives passe par une demande de dérogation afin d'obtenir l'autorisation de transgresser une des deux règles. Dans le cas de Grandpuits, le site a obtenu l'autorisation d'écrire des informations sur des équipements, à condition que l'équipement n'accepte les écritures que d'un nombre très limité de serveurs explicitement déclarés comme « sûrs ». La mise en place de ces restrictions est effectivement bien plus facile que de revoir complètement la configuration du serveur de supervision. Dans le cas de Grandpuits, cette démarche a également un intérêt économique : elle permet de ne pas nécessiter l'achat de la mise à jour du logiciel de supervision qui ne gère pas SNMP v3 actuellement.

16. CDP et LLDP

16.1.1. Présentation générale de CDP et LLDP

CDP[9] — Cisco Discovery Protocol — est un protocole propriétaire de niveau deux du modèle OSI destiné à découvrir la topologie réseau. Il a été développé par la société Cisco en 1994 et est depuis intégré à l'ensemble de ses équipements de niveau deux du modèle OSI. Au vu de la durée de vie de ces équipements, tous les matériels Cisco actuellement exploités le supportent. Son équivalent standard est le protocole IEEE 802.1AB plus connu sous le nom de LLDP — Link Layer Discovery Protocol. Ces deux protocoles présentent un certain nombre de points communs, Cisco ayant contribué à

la création de LLDP sur la base de ses travaux avec CDP. Cependant, LLDP ayant commencé à être implémenté en 2000, il est beaucoup moins utilisé dans les environnements homogènes (ne contenant que des équipements du même constructeur) car cela nécessiterait une migration complexe et risquée. Les deux protocoles sont cependant également supportés sur les équipements Cisco et sont même parfois exploités simultanément. C'est notamment le cas pour la connexion de téléphones sur le réseau car CDP ne les supporte pas, au contraire de LLDP. Cependant, cela nécessite d'utiliser une version étendue de LLDP, nommée LLDP-MED — LLDP Media Endpoint Device, LLDP périphérique d'extrémité — qui permet de communiquer au téléphone les informations nécessaires à son fonctionnement. Du point de vue d'un administrateur, le terme CDP désigne donc un ensemble de protocoles (CDP, LLDP, LLDP-MED) sans qu'il soit utile de les distinguer lors de la configuration d'un équipement.

16.1.2. Le fonctionnement de CDP

Le but de CDP est de permettre aux équipements de découvrir la topologie du réseau en termes de service plutôt qu'en termes de chemins. Ainsi, CDP s'intéresse aux services que les équipements réseau peuvent proposer (routage, commutation, téléphonie...) à leurs différents voisins. CDP ne s'intéresse pas à la configuration de ces liens : un autre protocole, VTP — Spanning Tree Protocol — en est chargé. CDP permet d'inventorier automatiquement les équipements réseau et de constituer automatiquement des plans du réseau.

CDP repose sur la diffusion fréquente de la liste des services proposés par un équipement à ses voisins, lesquels font de même. Ainsi, chaque équipement connaît ses voisins et stocke ces informations dans la MIB SNMP, qu'il est aisé d'interroger. Les informations échangées permettent de créer une carte des équipements en progressant de proche en proche : en interrogeant un premier équipement puis en questionnant successivement les voisins découverts. Les informations recueillies vont de l'identité de l'équipement (nom, adresse IP) à la liste des services proposés en passant par des informations très techniques (configuration des ports participant au lien avec le voisin, consommation électrique du port le cas échéant...).

Il suffit de procéder à des requêtes SNMP pour connaître l'ensemble des informations recueillies par le protocole. Pour faciliter l'interrogation de la MIB de l'équipement, CDP diffuse aux voisins le port sur lequel l'agent SNMP embarqué répond.

L'interrogation de la MIB n'est pas soumise à authentification et il est possible de construire facilement et rapidement une carte du réseau regroupant l'ensemble des équipements et des liens le constituant. Cependant, il n'est pas possible d'écrire des informations sur l'équipement. Ainsi, la corruption des données et donc l'interruption du fonctionnement du réseau ne sont pas directement réalisables par CDP. L'utilisation régulière des fonctions d'énumération des équipements voisins par SNMP permet de découvrir automatiquement les modifications d'infrastructure et donc de disposer d'une vue fidèle et quasiment en temps réel de la topologie du réseau. Le couple SNMP-CDP est donc très puissant dans la gestion de réseaux.

16.1.3. Les informations échangées avec CDP / LLDP

Les informations échangées sont structurées selon le modèle TLV — Type, Length, Value, ou type, longueur, valeur respectivement. Les informations sont placées dans le champ Valeur. Le type décrit la nature du contenu du champ Valeur et le champ longueur contient la taille du champ Valeur. Ce modèle permet d'informer les voisins de l'équipement par diffusion, sans qu'il y ait d'interrogation mais simplement une écoute. Chaque équipement peut diffuser plus ou moins de TLV, selon la version du protocole qu'il supporte. Cependant, cette structure permet de faire cohabiter sur un même réseau des équipements dotés de versions hétérogènes de CDP sans causer de problème particulier. Il existe actuellement vingt-cinq TLV différents. La version initiale de CDP en proposait sept. Les enrichissements se firent lors d'apparitions de périphériques ou de liens originaux. Ainsi, la fibre optique devenant un médium populaire, un TLV fut ajouté en 2001 pour diffuser les caractéristiques spécifiques de ce lien.

L'analyse des informations issues des TLV permet également de vérifier la bonne configuration d'équipements. Ainsi, le protocole CDP intègre un mécanisme de vérification du *duplex* d'un port (la capacité d'une prise réseau à émettre et recevoir en même temps). Si les deux extrémités d'un lien ne sont pas configurés de la même manière, une dégradation très sensible des performances du réseau survient. Cependant, sans l'aide de CDP, ce problème est très difficile à diagnostiquer car le lien semble être configuré correctement.

16.1.4. La sécurité de CDP / LLDP

L'incompatibilité entre les différents protocoles propriétaires (CDP pour Cisco, Microsoft LLTD...) développés pour gérer la topologie du réseau rend impossible la gestion unifiée d'un parc hétérogène et lie intimement un client à un fournisseur. Ce lien peut poser problème, notamment pour des raisons de sécurité : une seule faille peut être commune à l'ensemble des équipements et son exploitation peut donc avoir un impact sur tout le réseau. LLDP apporte une solution élégante et tend donc à supplanter les implémentations propriétaires. Ainsi, CDP ne propose plus de nouvelle fonction depuis 2003, laissant aux extensions de LLDP la charge d'assurer le support des nouveaux besoins en gestion de topologie réseau. Le fait que, dans un équipement Cisco, LLDP et CDP soient confondus simplifie considérablement l'administration. En effet, peu importe le protocole ayant fourni l'information, l'administrateur dispose d'une base de données complète pour découvrir et analyser la topologie de son réseau.

17. Les outils existants

Le plan logique du réseau, représentant à la fois les équipements et les liens entre ces équipements, est généré à la demande par un logiciel adapté. Il est relativement lent mais offre une bonne vision dynamique de l'installation.

La surveillance des équipements est effectuée de manière assez simpliste par un second outil, capable de fournir des alertes en cas de problème. Cet outil a cependant montré quelques faiblesses comme une configuration assez difficile et une faible réactivité.

Un logiciel supplémentaire permet de recueillir les informations concernant les liens : leur utilisation est représentée sous forme graphique. Son défaut est qu'il est impossible actuellement d'identifier les chemins les plus souvent empruntés par les informations de manière à différencier les « autoroutes » des « chemins vicinaux » et donc d'adapter les capacités en fonction des usages réels.

Les outils d'administration ont été volontairement écartés du projet. Ils permettent de procéder à des modifications de configuration ou leur sauvegarde et parfois même assurent des fonctions de supervision. Cependant, aucun logiciel d'administration proprement dit n'est disponible sur la raffinerie, essentiellement pour des raisons de coût. Par exemple, la licence du logiciel d'administration édité par Cisco est liée au nombre d'équipements concernés. Pour le site de Grandpuits, cette licence serait

d'environ dix mille Euros en prix public, sans compter le coût des infrastructures et du service nécessaires à sa mise en place.

De plus, la place de ces outils dans la gestion des réseaux est mineure. La raison en est simple : chaque configuration d'équipement réseau est unique, au moins sur certains points. Disposer d'un outil capable de diffuser une configuration identique à l'ensemble des équipements n'a donc pas forcément d'intérêt. De plus, ce genre d'opération de diffusion sont exceptionnelles et ne se produisent que lors d'un changement très important d'architecture du réseau. Dans ce cas, les administrateurs réseau préfère procéder pas à pas et l'utilité d'un système centralisé reste à démontrer.

Le seul point plaidant en faveur d'un système d'administration est la sauvegarde des équipements réseau. Cependant, il existe de nombreuses méthodes gratuites permettant d'automatiser ces sauvegardes.

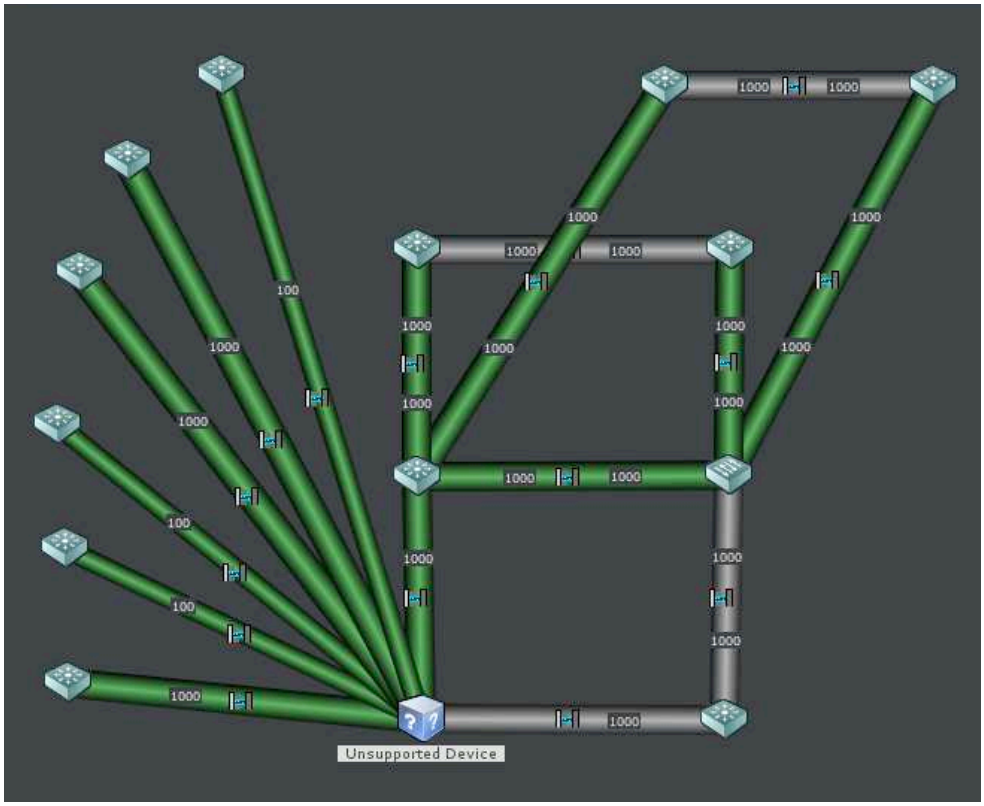
Certains outils d'administration centralisée sont indispensables. La gestion de pare-feux en est un exemple. Ainsi, à l'aide d'une seule action, les règles de filtrage sont diffusées à l'ensemble des équipements, assurant ainsi la cohérence des configurations. Cependant, il ne s'agit pas de logiciels d'administration de réseaux mais simplement d'applications liées à un service réseau particulier. Ils n'ont donc pas leur place dans une méthode générale de gestion des réseaux informatiques.

La solution de gestion en place est composée de trois outils. La cartographie du réseau est effectuée par le logiciel « Cisco Network Assistant », solution gratuite et bridée en nombre d'équipements supervisés éditée par la société Cisco, fabriquant les matériels supervisés. La surveillance des équipements est confiée au logiciel commercial « WhatsUpGold » édité par Ipswitch. Ce logiciel est dans une version obsolète. La surveillance des liens est réalisée par la solution « PRTG » de la société Paessler. Là encore, la version exploitée par la raffinerie est obsolète.

17.1. La cartographie avec « Cisco Network Assistant »

Ce logiciel fonctionne par découverte automatique des équipements présents sur le réseau via le protocole CDP. Ainsi, en disposant d'une étendue d'adressage IP, Cisco Network Assistant — CNA — peut se connecter à chaque équipement réseau dont il reconnait le type. Si l'utilisateur fournit un nom d'utilisateur et un mot de passe valable sur un équipement, CNA va automatiquement identifier les connexions avec les autres éléments du réseau et ainsi dresser une carte très complète du réseau. Cependant,

cette solution gratuite est bridée : il n'est pas possible de gérer tous les matériels réseau (même certains équipements fabriqués par Cisco ne sont pas supportés) et le logiciel ne reconnait qu'un maximum de quarante éléments réseau. Cette dernière limitation est contournée en segmentant les équipements réseau par périmètre. Cependant, le périmètre bureautique comporte environ trente-cinq équipements et la limite est proche, ce qui pose la question de la pérennité de la solution.



Cisco Network Assistant : exemple de représentation d'une topologie réseau

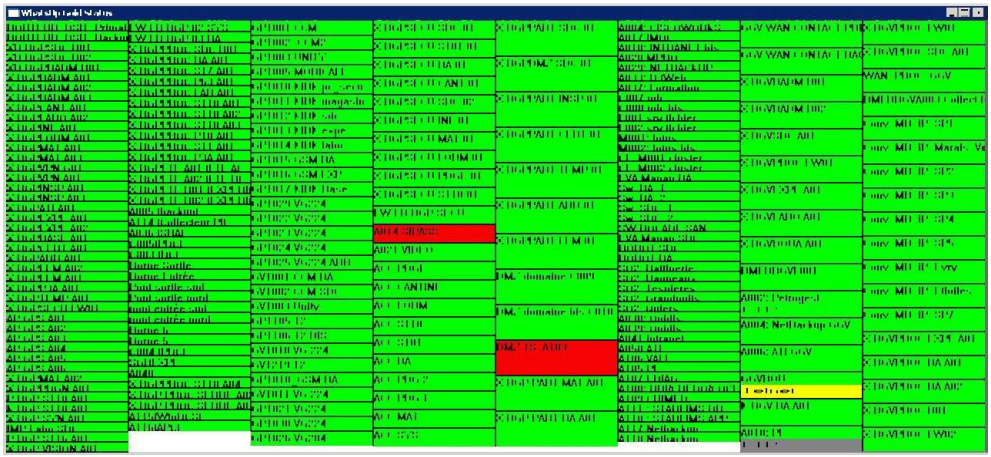
CNA répond au besoin de cartographie du réseau. S'il est impossible de disposer d'une vue globale comportant l'ensemble des équipements et des liens sur un seul écran, ce n'est pas un inconvénient. En effet, des tentatives de représentation exhaustive du réseau ont été effectuées. Elles ont produit des plans trop complexes, illisibles et dont les cheminements sont impossibles à comprendre. Quel que soit la solution utilisée, une séparation des plans par périmètre est indispensable pour qu'ils demeurent utilisables. C'est pourquoi il est préférable pour l'instant de conserver cette solution, tout en surveillant le marché pour pouvoir adopter une solution appropriée si l'une des limites du logiciel devait être atteinte.

17.2. La supervision d'équipements avec « WhatsUpGold »

Généralement, la supervision sert à produire des écrans de contrôle, à la fois clairs et complets. À cet exercice, WhatsUpGold — WUG — est excellent. Il dispose d'une vue composée de rectangles colorés, chaque rectangle représentant un équipement et chaque couleur indiquant l'état de cet équipement. Ainsi, le but est de disposer d'un écran entièrement composé d'éléments verts, signe de bon fonctionnement.

La solution est basée sur l'interrogation des équipements à intervalle régulier paramétrable. Pour chaque équipement, s'il est d'un type supporté par WUG, il est possible de surveiller non seulement la présence sur le réseau mais également la disponibilité de services de plus haut niveau (jusqu'à la couche quatre du modèle OSI).

Si un service est indisponible, le rectangle passe à la couleur rose. La dégradation de l'état d'un équipement est progressive. Un délai excessif pour recevoir la réponse est signalé par la couleur vert clair. Puis, si cela se répète à la seconde interrogation, le rectangle devient jaune. Au troisième échec, il passe au rouge vif puis enfin au rouge foncé en cas de nouvel échec. Une alerte est générée à partir de l'atteinte du niveau « rouge vif » et peut consister en l'envoi d'un courriel à une liste prédéfinie selon le paramètre le plus souvent configuré.



WhatsUpGold : écran principal — vue globale de l'état des équipements supervisés

La liste des équipements surveillés est définie manuellement dans le logiciel. De plus, rajouter un équipement d'un nouveau type impose des manipulations compliquées pour le faire reconnaître à WUG. Cette complication est telle que la surveillance est bien souvent restreinte à un standard universel de test de présence sur le réseau : la réponse à un paquet ICMP plus communément nommé « ping ».

Le paramétrage des alertes est complexe. De nombreuses options sont disponibles et il est difficile d'identifier précisément la portée de modifications : locale à l'équipement, commune à un groupe ou à l'ensemble des équipements. De plus, il est impossible de disposer d'une vue globale permettant de repérer les équipements dont les alarmes sont désactivées. L'identification et la correction d'écarts de configuration sont très longues et fastidieuses, sans qu'il soit possible d'avoir la certitude d'être exhaustif.

Le système de gradation des alertes permet d'éviter les notifications inutiles. Cependant, cela est bien souvent source de délai trop important pour les notifications. Il n'est pas rare qu'un incident soit rapporté par un utilisateur avant que WUG n'ait eu le temps de changer de couleur. Dans ces circonstances, il est difficile de justifier l'usage de cette solution.

L'adaptation de WUG aux besoins devrait donc passer par les phases suivantes :

- Acheter et installer une version supportée de WUG
- Adapter les paramètres pour fiabiliser la remontée d'alertes

Cependant, les versions les plus récentes de WUG n'apportent pas d'amélioration significative pour corriger les points faibles de la solution :

- L'intégration de nouveaux types d'équipements passe par une mise à jour de l'ensemble de la solution et est payante
- Il n'est pas possible de gérer les alertes de manière centrale

De plus, la vue sous forme de rectangles colorés est de moins en moins utile. En effet, le nombre de rectangles augmentant au fur et à mesure de l'enrichissement du réseau en équipements, les informations sont de moins en moins lisibles pour une surface d'écran donnée. De plus, les informations réellement pertinentes, telles que la liste des équipements ayant un problème, est noyée dans l'océan de rectangles verts et un changement sur un équipement n'est plus visible aussi facilement. Enfin, il n'est pas possible d'acquitter une alerte et le seul moyen de faire disparaitre une alarme prise en compte mais dont la résolution prendra plusieurs jours est de supprimer l'équipement en cause.

Ces défauts sont considérés par l'éditeur comme les fonctions distinguant sa solution de la concurrence. Ils ne seront donc pas corrigés. C'est pourquoi l'adaptation de la solution aux besoins exprimés est impossible, même en mettant à jour WUG.

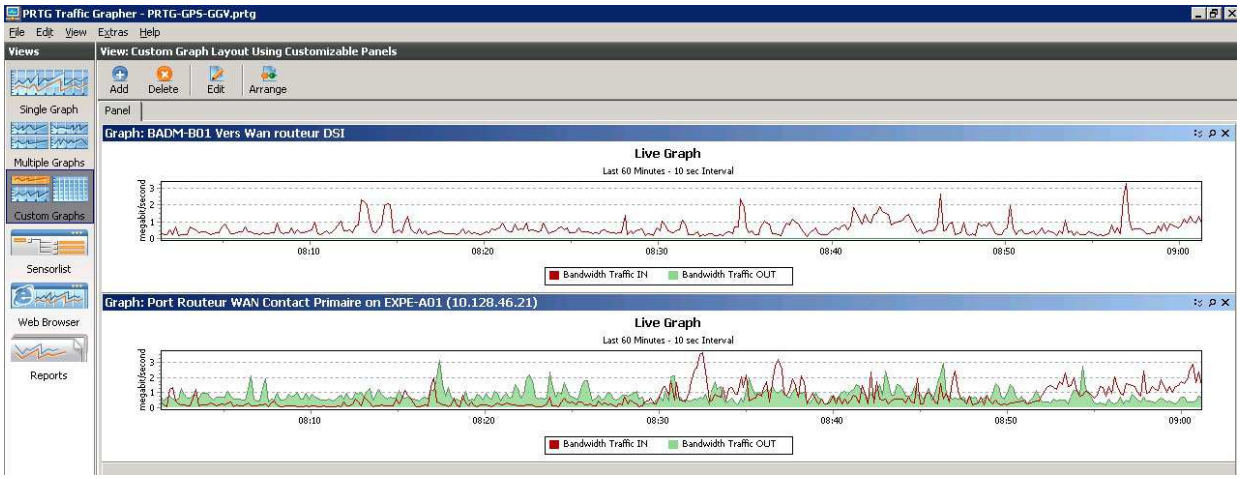
Les fonctions d'alertes dans des délais optimaux étant primordiale dans un système de supervision, il est impossible d'y renoncer. Il s'agit du seul intérêt d'une solution de surveillance des équipements réseau et de la seule valeur ajoutée du produit.

C'est pourquoi le remplacement de WUG par une solution apportant des réponses efficaces aux besoins exprimés dans le cahier des charges est nécessaire.

17.3. La surveillance de liens avec « PRTG »

L'intérêt de la surveillance des liens réside dans l'exploitation de ses résultats. Ils sont utilisés pour analyser les chemins les plus empruntés, vérifier l'adéquation des capacités par rapport aux usages et peuvent également servir à diagnostiquer des usages anormaux en suivant le trafic entre sa source et sa destination.

La surveillance de trafic repose sur l'interrogation des compteurs que renferment les équipements réseau. Les réponses à ces interrogations régulières sont stockées dans une base de données pour être ensuite consolidées. Ainsi, il devient possible de « remonter le temps » et d'afficher le trafic d'un lien sur une minute, une heure... jusqu'à un an ou plus. Dans ce cas, la définition de la mesure change : sur une heure, les échantillons seront regroupés par tranches de cinq minutes et seule la moyenne de chaque tranche sera affichée. Sur une année, la tranche sera de l'ordre d'un mois. Ces calculs peuvent impliquer des quantités importantes de données et nécessiter un temps de calcul assez long. Durant ce temps, il est important de limiter les ressources consommées par le calcul afin que le système continue la collecte de données.



PRTG : Exemple de surveillance de l'occupation de liens réseau

PRTG est plutôt efficace. Les données sont collectées sans limite de temps (selon la place disponible pour la base de données) et restituées sous forme de graphique dans

des délais raisonnables : il faut moins d'une minute pour établir une courbe d'utilisation d'un lien sur un an. La place occupée par les données est de l'ordre de douze giga-octets par an, ce qui est considérable. Cependant, il est rare d'interroger des données plus anciennes qu'un an. La purge des données obsolètes est possible mais doit être effectuée manuellement.

L'administration de PRTG est très difficile. La création de nouveaux équipements est très complexe et se base sur des types d'équipements pré-définis. L'ajout d'un nouveau type d'équipement est compliqué car PRTG ne se base pas directement sur les MIB de SNMP. Il est nécessaire d'utiliser un outil de conversion des MIB au format propriétaire supporté par PRTG pour que ce dernier reconnaisse les nouveaux modèles d'équipement. Cet outil est complexe et il est nécessaire de procéder à de nombreuses tentatives de conversion avant d'obtenir un résultat satisfaisant.

18. La recherche d'une solution unifiée

En cas d'incident, les outils de supervision sont très précieux : ils doivent permettre d'établir rapidement un diagnostic rapide et précis. C'est pourquoi disposer de trois outils différents peut poser des problèmes en cas d'urgence.

Un cahier des charges a donc été établi pour la recherche d'une solution présentant les caractéristiques suivantes :

- la création de cartes en temps réel basées sur une liste de matériel et un ensemble de services à surveiller (présence sur le réseau, possibilité de connexion à distance...)
- un système de surveillance des équipements et d'alerte rapide et facilement paramétrable. Les alertes peuvent être du type courriel, SMS...
- un système de représentation du cheminement des données et de l'exploitation des bandes passantes des liens.
- facile à exploiter et à administrer
- sans coût de licence et pouvant être installé sur un serveur âgé

Plusieurs outils existent qui satisfont plus ou moins complètement ces contraintes. Cependant, le standard du marché de la supervision sans coût de licence est un outil nommé « Nagios ». Il présente le défaut de générer des cartes difficiles à lire et ne sait pas représenter les cheminements de données. Il peut être associé à la solution de surveillance de trafic « Cacti » mais il ne s'agit plus dans ce cas d'une solution unifiée.

Cette recherche a permis de mettre en évidence une difficulté. La supervision recouvre en fait deux périmètres qui sont aujourd'hui peu conciliables : la surveillance d'équipements et la surveillance de trafic.

La surveillance d'équipements est fondée sur un inventaire, mis à jour par l'administrateur réseau secondé ou non par un dispositif automatique. Les biens placés dans cet inventaire sont interrogés régulièrement par le système de supervision qui génère une alarme si une réponse correcte n'est pas fournie dans le délai imparti. L'intervalle d'interrogation est paramétrable et peut aller de plusieurs fois par seconde à une fois toutes les quelques heures.

La surveillance de trafic est également basée sur un inventaire, lequel est mis à jour manuellement par l'administrateur. Les équipements sont interrogés selon des intervalles compris entre une et cinq minutes. Lors de cette interrogation, les équipements remettent au système de supervision les données stockées dans leur base de données : nombre de paquets transmis par port, utilisation du processeur, de la mémoire... Il ne s'agit pas d'une surveillance à proprement parler car le système ne déclenche pas d'alarme en cas de franchissement d'un seuil. Cependant, il calcule l'utilisation de la bande passante et est donc capable de dresser des cartes mentionnant les utilisations des liens.

En conclusion de ce « mini-projet », il est impossible de disposer d'une solution unique satisfaisant l'ensemble des contraintes exprimées dans le cahier des charges. La question se pose donc différemment : les outils en place peuvent-ils être adaptés pour satisfaire les contraintes, faut-il s'en satisfaire et donc négliger des contraintes ou bien faut-il les remplacer ?

19. Les remplaçants potentiels

Les logiciels existant ne sont pas exempts de défauts. Bien qu'une solution globale ne puisse être implémentée, il est intéressant d'étudier les alternatives permettant de surmonter ces défauts.

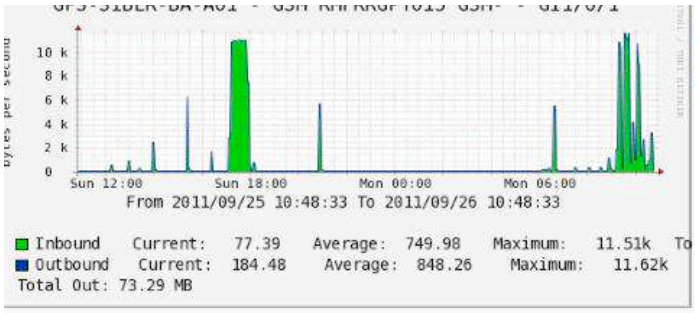
Cette étude a été conduite selon les principes directeurs suivants :

- ❖Il n'est pas nécessaire de reprendre les données historiques, afin de ne pas être contraint dans le choix du produit
- ❖La solution doit être si possible gratuite, c'est-à-dire sans coût de licence.

Les remplaçants potentiels étudiés sont Cacti pour PRTG et Nagios pour WathUpGold. Dans chaque cas, une maquette a été construite afin de valider les aspects techniques et de faciliter la comparaison entre les solutions.

19.1. Un remplaçant à « PRTG » : Cacti

Cacti est une solution open-source de surveillance de trafic réseau. Elle permet de recueillir les informations automatiquement par SNMP en interrogeant régulièrement les équipements concernés et présente les statistiques d'usage sous forme de graphique. Cacti est une application Internet basée sur des technologies standard (HTML, Javascript) qui facilite son accès et sa diffusion. Les opérations de consultation et d'administration passent entièrement par l'interface Web et sont donc réalisables depuis tout terminal doté d'un navigateur Web.



Exemple de graphique produit par Cacti

L'étude a consisté à évaluer les points suivants : reconduite des fonctions actuellement disponibles avec PRTG et disponibilité des fonctions absentes de PRTG.

Les points à reconduire sont :

- ❖L'historisation des données
- ❖La réactivité
- ❖La possibilité de consulter des graphiques sur des périodes précises

Les fonctions à proposer sont :

- ❖La purge automatique des données trop anciennes
- ❖La facilité d'administration

Cacti est, comme bon nombre de solutions open-source, un logiciel modulaire dont les fonctions de base sont restreintes mais qui dispose d'une base importante de modules complémentaires destinés à satisfaire des besoins précis. Sa force principale réside

dans la simplicité du concept mis en place, très proche de la réalité. Cacti surveille le trafic passant par les différentes prises réseau d'un équipement. Ainsi, le logiciel manipule les objets « équipement », « port réseau » et « graphe associé au port réseau ». Chaque équipement doit être déclaré manuellement dans Cacti. Lors de cette déclaration Cacti interroge l'équipement *via* SNMP et présente une liste de prises réseau disponibles pour la surveillance. Il s'agit en fait d'une énumération SNMP. Ensuite, il suffit de sélectionner les prises réseau à surveiller et de choisir un type de graphique à associer à ces prises. La création des objets dans Cacti est alors effectuée et active la collecte automatique des informations par SNMP.

Il existe plusieurs modèles de graphique. Chaque modèle répond à des besoins spécifiques. Par exemple, certains présentent des informations en bits et d'autres en octets. Cette différence est utile pour surveiller des liens ne fonctionnant pas sur la base d'octets, comme les liens WAN.

Cacti et PRTG collectent des volumes de données comparables sinon identiques. Cependant, Cacti intègre la fonction de purge automatique des données trop anciennes, selon un seuil déterminé par l'administrateur. Cette simple fonction permet de limiter les besoins en matériel (disque dur du serveur et emplacement de sauvegarde), ce qui contribue à réduire le coût de la solution.

Un des avantages de Cacti sur PRTG est de proposer une interface Web accompagnée d'une gestion très fine des droits d'accès. PRTG propose également une interface Web mais elle ne permet pas de segmenter les droits ni d'agir sur la configuration. Cacti étant conçu pour le Web, l'ensemble des opérations d'administration sont réalisables à distance. De plus, la restriction aisée des droits d'accès permet de déléguer facilement la surveillance et donc de maintenir un bon niveau de sécurité.

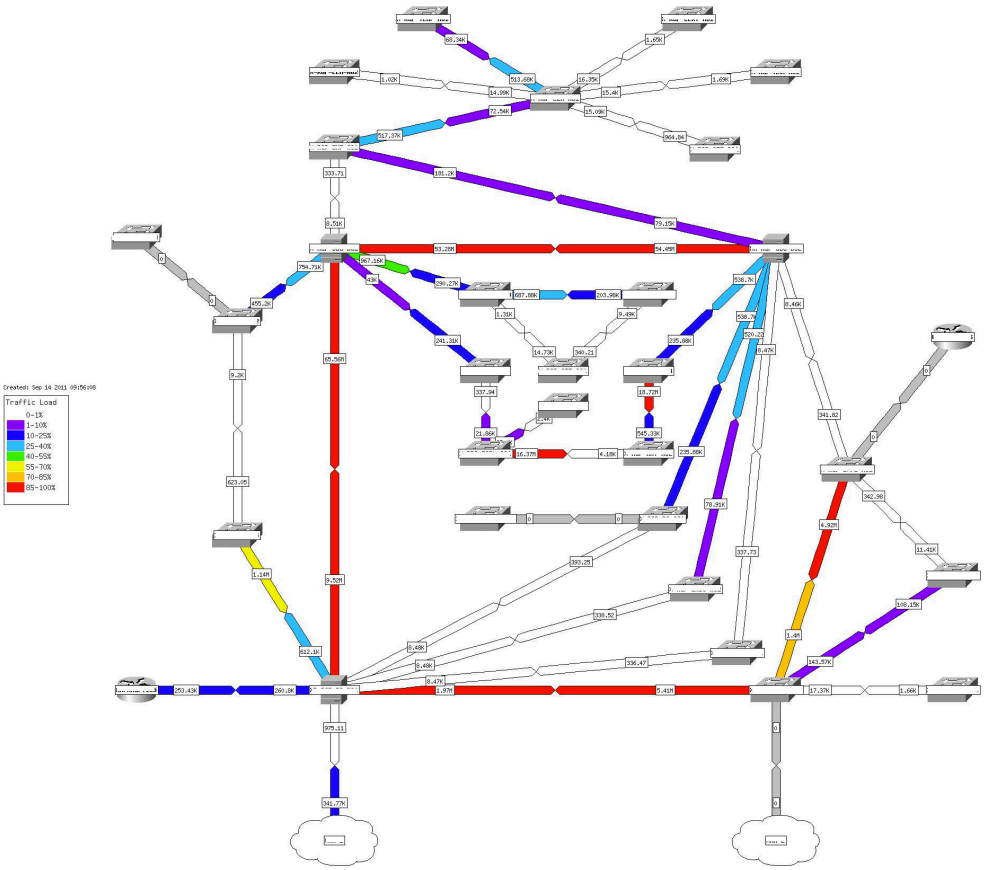
Cacti est basé sur des technologies Internet et ne nécessite qu'un serveur Web pour s'exécuter. Ainsi, Cacti peut s'insérer sans difficulté sur un serveur Intranet existant. Cette particularité facilite la phase d'intégration de Cacti dans un environnement réseau existant en réutilisant une infrastructure Web déjà disponible. De plus, dans le groupe Total, le système d'exploitation standard est Microsoft Windows. Or beaucoup de projets open-source sont conçus pour s'exécuter exclusivement sur un environnement compatible avec la norme POSIX, tel qu'UNIX ou Linux. Cacti est

pleinement supporté avec un système Microsoft Windows Server et son installation au sein du système informatique de la raffinerie ne pose donc pas de problème particulier.

A priori, les graphiques issus de Cacti ne sont pas confidentiels. En effet, l'usage des liens n'apporte pas d'information sur le contenu des messages et ne permet pas directement de concevoir une attaque ciblée. Cependant, cela peut permettre d'identifier les équipements centraux du réseau. Le risque principal vient du serveur Cacti lui-même. En effet, cette machine permet d'interroger tous les équipements surveillés en utilisant le protocole SNMP. Un accès mal intentionné à ce serveur peut avoir des conséquences importantes sur le fonctionnement du réseau.

Au cours du projet, un nouveau besoin a été formulé. Quelquefois, le lien réseau de la raffinerie vers le reste du monde est saturé. Il est souhaitable de pouvoir identifier la machine sur le réseau local responsable de cette activité anormale en un minimum de temps. PRTG ne le permet pas, et Cacti non-plus. Cependant, un composant additionnel de Cacti, nommé WeatherMap — littéralement *carte météo* — propose ces fonctions. Il permet également d'avoir une représentation graphique dynamique de l'état des liens réseau.

L'usage des liens est affiché avec un décalage de cinq minutes. Cela ne permet pas de réagir sur l'instant mais cela ne pose pas de problème particulier. En effet, la saturation d'un lien tel que le lien vers l'extérieur n'a d'importance que si sa durée est supérieure à dix minutes.



Exemple de plan Weathermap

Ainsi, un test de surveillance du trafic réseau par WeatherMap a été effectué durant un mois. Durant cette période, différentes situations ont été testées. En particulier, l'évaluation de la facilité de maintenance a été réalisée en conditions réelles, face à une importante modification de topologie sur un réseau. La mise à jour du plan n'a demandé que quelques minutes à une personne exercée. Cacti apporte donc l'ensemble des fonctions attendues. Le module complémentaire WeatherMap permet même de disposer d'une surveillance fine des trafics réseau, ce que ne permet par PRTG.

Cependant, la surveillance de trafic s'est révélée assez lourde à utiliser. En effet, par nature, cette surveillance ne permet pas d'identifier directement la machine consommant le plus de ressource mais bien de donner des indications à un administrateur, lequel doit alors procéder à des recherches sur des équipements

réseau, de proche en proche, jusqu'à identifier le port réseau créant ce trafic. Ensuite, il est possible d'identifier la machine connectée à ce port. L'ensemble de l'opération ne prend pas plus de cinq minutes mais la quantité de tâches à effectuer, l'impossibilité d'automatiser l'enquête et la nécessité de pouvoir déléguer cette investigation à une personne sans formation spécifique ont mis en évidence que Weathermap ne pouvait pas réellement être mis en production dans ce contexte.

Une autre solution a été alors envisagée pour répondre spécifiquement au besoin d'analyse du trafic. Cette solution, baptisée nTop, est elle aussi basée sur un modèle open-source. Cette évaluation est toujours en cours.

Cacti fournit une bonne réponse au besoin initial. La préconisation est donc de le passer en production. Cependant, cette migration comporte des coûts et des risques et il est probable que ceux-ci conduisent à conserver la solution actuelle tant que c'est techniquement faisable. Le besoin complémentaire sera peut-être satisfait avec nTop mais un moyen de contournement a été trouvé en faisant appel aux services de diagnostic de l'opérateur du lien Internet. Ainsi, changer l'existant ne sera probablement pas nécessaire.

19.2. Un remplaçant à « WhatsUpGold » : Nagios

Nagios est une solution « open source » de surveillance de l'état d'équipements réseau. Cette surveillance se base sur les deux modes de fonctionnement de SNMP. Dans le cas général, une interrogation régulière de la MIB des équipements permet à Nagios de vérifier que des valeurs sont retournées et qu'elles le sont dans des intervalles définis comme « normaux ». De plus Nagios peut surveiller le bon fonctionnement de services. Par exemple, Nagios peut essayer de se connecter à un serveur Web et considérer que ce dernier est opérationnel s'il renvoie une page Internet.

Nagios est un logiciel qui se contente d'exécuter des scripts à des échéances programmées et de retourner les résultats. Ce mode de fonctionnement permet d'enrichir très facilement les fonctions de Nagios. Pour ajouter la surveillance d'un nouveau service, il suffit de créer un script et de demander à Nagios de l'exécuter régulièrement. Cependant, cette approche se base sur le principe que l'administrateur de Nagios est un développeur. Dans le cas de la raffinerie, ce n'est pas le cas : il n'y a pas de développeur sur site. Cependant, sur le site, les nouveaux modèles d'équipement nécessitant la création de scripts de surveillance sont rares. En effet, les

services surveillés sont toujours les mêmes. C'est pourquoi Nagios est envisagé comme une alternative viable à WhatsUpGold (WUG) sur le site.

Nagios présente les informations de manière synthétique. Au lieu de présenter l'ensemble des équipements sur un écran, ce qui rend difficile la surveillance de nombreux équipements faute de place, Nagios expose des décomptes d'équipements. Il existe un compteur d'équipements, toutes catégories confondues, un compteur des équipements indisponibles et un compteur des services indisponibles. Idéalement, les deux derniers compteurs devraient être continuellement à zéro.

Une des grandes forces de Nagios est la variété des notifications qu'il est capable de gérer. En ce sens, il est parfaitement adapté à un usage dans l'industrie. En effet, il est utile de n'informer que les parties prenantes pouvant effectivement agir sur un défaut, en fonction du degré critique de celui-ci. Certains équipements doivent être remis en marche sans délai, d'autres peuvent tolérer une indisponibilité plus grande, de plusieurs jours parfois. Les notifications s'adaptent à cette variété de degrés d'urgence. Si dans la plupart des cas une notification distribuée à l'administrateur par courriel suffit, des alertes peuvent également être nécessaires. Ces alertes peuvent prendre la forme de SMS — Short Message Service, Service de Messages Courts — expédiés directement par Nagios en cas de défaillance d'un équipement critique. Ces notifications sont également paramétrables en fonction du moment où se produit la défaillance. Envoyer un courriel au milieu de la nuit a peu de chance de déclencher une réaction immédiate. À l'inverse, expédier un SMS en journée, alors que l'usage des téléphones portables est interdit sur le site n'a par d'intérêt. Une bonne identification des profils de notification peut faire gagner un temps précieux dans la résolution d'un incident.

Nagios est une solution retenue par nombre d'entreprises et bénéficie d'une documentation abondante. Cependant, il n'existe pas de paramétrage standard du logiciel ni même d'application le facilitant. Il est nécessaire de modifier des fichiers bruts pour ajouter, modifier ou supprimer un équipement ou bien de recourir à un module complémentaire, lui-même difficile à exploiter.

La recommandation est donc de faire évoluer la solution existante, même si la licence est assez chère (environ deux à trois mille Euros), plutôt que de mettre en place une solution dont l'efficacité ne compense pas la complexité d'exploitation. Cependant, un des grands avantages de cette étude a été de mettre en évidence le besoin de mise à

jour de WhatsUpGold et de justifier cette mise à jour, plutôt que le remplacement par une solution qui, certes, ne coûte pas de licence mais nécessite des investissements importants par ailleurs. Il s'agit en quelque sorte d'une démonstration par l'absurde : avant de mettre en place une maquette de Nagios, le financement de la mise à jour de WUG avait été farouchement refusée. Aujourd'hui, elle est en à l'étude.

19.3. Synthèse des comparaisons

Le tableau suivant résume les résultats produits par l'étude :

Tableau VI : synthèse des comparaisons d'outils de supervision

	Cartographie	**Supervision des liens**	**Supervision des équipements**
Solution existante	Cisco Network Assistant	PRTG	WhatsUpGold
Candidat au remplacement	Schémas manuels	Cacti	Nagios
Principal avantage du candidat	Aucun	Évolutif	Polyvalent
Principal inconvénient du candidat	Lisibilité incertaine	Coûts de migration	Maintenance complexe
Recommandation	Conserver la solution existante	Adopter Cacti	Mettre à jour WhatsUpGold

Seuls les avantages et inconvénients les plus importants ont été mentionnés. La mise en place effective de nouvelles solutions est pour l'instant impossible car toutes les équipes informatiques du site sont mobilisées pour assurer la migration de l'ensemble des postes de travail vers la nouvelle plateforme bureautique du groupe Total. Ce projet absorbe toutes les énergies et devrait se conclure au premier trimestre 2012.

L'ÉVOLUTION DES RÉSEAUX VERS LES OBJECTIFS

Des objectifs ont été définis en accord avec les orientations stratégiques de l'entreprise. Comment les atteindre ? Quelles évolutions faire subir aux réseaux informatiques de la raffinerie et comment intégrer ces changements pour en diminuer les risques ?

Chaque objectif est soumis à des contraintes particulières qu'il est nécessaire de prendre en compte pour l'atteindre de manière satisfaisante. L'atteinte de l'objectif ne doit pas être une démarche brutale vers cet unique but mais plutôt l'intégration de l'évolution dans l'environnement existant.

Cette partie reprend donc les objectifs définis précédemment pour en exposer les contraintes. Des exemples illustrent les difficultés rencontrées par le passé et s'y appuient pour orienter l'évolution des réseaux.

20. L'atteinte de l'objectif de capillarité

Cet objectif n'est pas mesuré par un outil mais de manière plus subjective par la facilité avec laquelle un point précis de la raffinerie peut être connecté au réseau. Ainsi, l'installation de nouvelles caméras de vidéosurveillance a nécessité la création d'acheminements en fibre optique de plusieurs kilomètres, ce qui a engendré des délais considérables. Dans un cas, ce délai fut de l'ordre de deux ans.

La difficulté principale est de convaincre de la nécessité de nouveaux acheminements sans que les projets les exploitant n'aient été encore lancés. Dans un contexte de restrictions budgétaires, il est difficile d'obtenir une liaison « de réserve », « au cas où » un besoin se fait sentir « un jour ». Pourtant, si de nombreux projets coûtent cher et prennent du retard, c'est souvent parce que le réseau n'est pas disponible à proximité.

L'administrateur réseau doit donc disposer d'une vision prévisionnelle de manière à pouvoir justifier les investissements nécessaires les années suivantes.

20.1. L'exemple de la liaison ST1 - ST2

Lors des travaux préparatoires sur l'élaboration du plan de capillarité, un lien est apparu comme manquant cruellement. Il s'agit de celui permettant de relier directement les salles techniques ST1 et ST2.

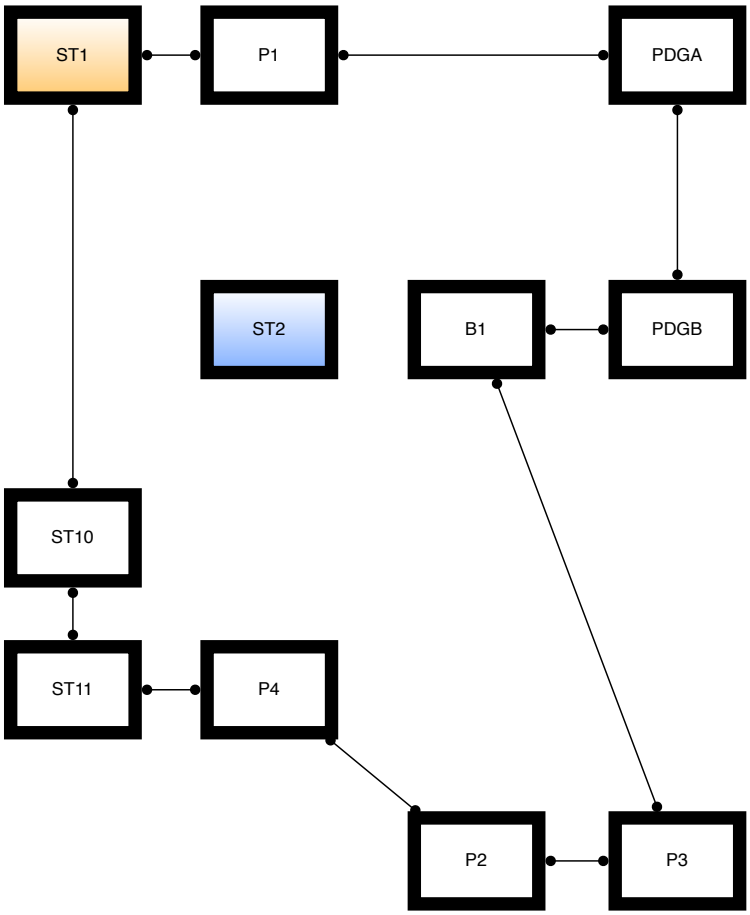
20.1.1. La situation avant le Grand Arrêt 2011

La salle ST2 n'était pas reliée au réseau. Cette salle est située au milieu d'un espace dédié aux installations temporaires durant les arrêts de maintenance de la raffinerie, à environ cent quarante mètres du point d'extrémité du réseau le plus proche : B1. En temps normal, il n'est pas nécessaire de disposer de réseau dans cette salle technique ou dans ses environs. Elle ne doit d'ailleurs son nom qu'à la présence d'un répartiteur téléphonique dans ses murs.

Pourtant, durant les périodes de Grand Arrêt (GA), cette salle est idéalement située pour fournir un accès réseau peu coûteux aux bungalows placés à ses alentours. En effet, chaque bungalow est situé à moins de cent mètres du local ST2, ce qui rend possible l'installation de câbles réseau provisoires durant un GA. L'installation d'un câble en cuivre ne coûte rien en comparaison de celle d'une fibre optique. Pour chaque GA, les bungalows sont alimentés en réseau informatique par le biais de convertisseurs délivrant un débit peu important et instable sur du câblage téléphonique. Desservir ST2 en réseau de bonne qualité nécessite donc le recours à une fibre optique mais apporte une réduction des coûts et une amélioration sensible des performances du réseau durant les arrêts.

De plus, un automate très important pour le fonctionnement de la raffinerie est implanté dans une salle nommée P2 et doit être connecté par le chemin le plus court possible à des équipements situés dans la salle ST1. Le chemin le plus court passe par une liaison entre ST1 et ST2. Cependant, pour des questions de temps, cet itinéraire n'a pas été retenu car le délai nécessaire à l'installation de cette liaison était inacceptable. Disposer de cette liaison en avance aurait donc été un avantage considérable.

Voici un plan résumant la situation. On y voit les liaisons existantes et l'isolement de la salle ST2 :



Plan de situation de ST1 et ST2

Ce plan ne respecte pas d'échelle ni de proportion particulières. Il est cependant représentatif du besoin. La liaison actuelle entre ST1 et P2 passe par les bâtiments P1, PDGA, PDGB... soit cinq jonctions intermédiaires. Une liaison entre ST1 et ST2 permet à la fois de desservir le bâtiment P2 avec moins de distance (environ vingt pour-cent de moins) et avec deux jonctions intermédiaires en moins, ce qui correspond en termes d'atténuation du signal optique à un gain de près de quarante pour-cent. Une liaison passant de l'autre côté, par les bâtiments ST10, ST11... n'est pas réalisable car nombre de liens sont saturés.

Ainsi, ce n'est pas une mais deux liaisons optiques qui sont nécessaires : de ST1 à ST2 et de ST2 à B1. La demande d'installation de lien s'est vue refusée à de nombreuses reprises car le coût des travaux (sans qu'il n'y ait eu d'évaluation précise) a été jugé excessif.

20.1.2. Le Grand Arrêt 2011

Afin de rendre la desserte réseau des bungalows de l'arrêt plus fiable et plus performante, l'installation d'un « pont » sans fil a été effectuée. Cette solution permettait de profiter des avantages d'une installation sans fil (faible coût, installation aisée) et d'éviter d'effectuer des travaux lourds pour passer une fibre optique entre ST2 et B1.

Cependant, cette solution n'a pas apporté la fiabilité et la performance attendue. Il a été nécessaire de trouver une solution permettant aux personnes travaillant dans cette zone de disposer d'un accès réseau d'une qualité satisfaisante. L'installation d'une fibre optique entre les bâtiments ST2 et B1 a donc été réalisée en urgence et a permis de résoudre les problèmes de connexion.

Cette intervention a permis de rétablir un service de qualité mais également de tester une nouvelle méthode de génie civil permettant de réduire les coûts d'acheminement et de percer des tranchées sans abîmer les câbles déjà enterrés. Un gigantesque aspirateur, dont le tuyau est d'environ vingt centimètres de diamètre, prélève la terre et la stocke dans la benne d'un camion. Cette technique, plutôt inattendue, a permis de réaliser l'installation de la fibre optique moins d'une semaine après le début de l'arrêt.

20.1.3. La liaison ST1 - ST2

Suite au GA 2011, une nouvelle demande de liaison entre les salles ST1 et ST2 a été formulée. De nouveaux arguments sont venus consolider la demande. En premier lieu, la réalisation de la liaison entre ST2 et B1 permettait d'envisager de creuser des tranchées de manière économique et peu risquée. Ensuite, disposant déjà de cette liaison, la création du lien ST1 — ST2 ne comportait plus qu'un seul volet, ce qui suffisait à faire paraître le problème plus simple. Enfin, un repérage sur site a permis d'identifier des passages de câble existants, gages de simplicité d'installation de la liaison et de réduction des coûts.

Enfin, l'argument de la réduction de la distance de l'acheminement entre ST1 et P2 a été décisif. La liaison ST1 - ST2 a été inscrite au budget 2012 du service Systèmes et a fait l'objet d'une cotation par la société chargée de la réaliser.

20.2. La réalisation de l'objectif de capillarité

Cet exemple montre combien il est difficile pour un administrateur réseau de justifier les investissements nécessaires à la mise en place d'une capillarité satisfaisante. Même si les besoins sont reconnus, l'absence de problème au quotidien et la restriction des budgets rendent l'atteinte de cet objectif difficile. C'est pourquoi il est nécessaire de disposer d'un plan d'investissement. En effet, il faut être prêt à profiter de chaque opportunité (quand un autre service ouvre une tranchée sur un itinéraire intéressant par exemple) pour améliorer la capillarité. Dans le contexte économique actuel, il est illusoire d'espérer obtenir l'installation de liaisons de réserve sans justification. Il est plus réaliste de tenir un argumentaire à jour pour pouvoir profiter de toutes les occasions se présentant.

Atteindre cet objectif nécessite donc d'être à l'écoute des projets qui pourraient voir le jour et d'envisager les différents scénarios de raccordement au réseau. Il faut également être informé des travaux de génie civil pouvant permettre de profiter de l'ouverture d'une tranchée pour y glisser un nouveau lien réseau améliorant la capillarité. Un comité de coordination des chantiers a été maintes fois réclamé pour faciliter cette information, sans résultat à ce jour.

21. L'atteinte de l'objectif de capacité

L'objectif de capacité est double. Il porte à la fois sur les équipements de connexion au réseau, afin de garantir la satisfaction immédiate d'une demande de raccordement. Ensuite, il concerne les liens du réseau, afin de prévenir tout engorgement structurel qu'il serait difficile de résoudre rapidement.

Dans une première approche, le réseau installé sur la raffinerie ne souffre pas de problèmes de capacité. Les ports réseau, ces connecteurs permettant de relier un équipement au réseau, sont en nombre suffisant et aucun cas de sous-capacité n'a été remarqué. De même, les liens ne sont pas saturés et sont capables d'absorber des charges deux ou trois fois supérieures à celles actuelles. Est-il dans ce cas pertinent de se donner comme objectif une gestion prévisionnelle de la capacité ?

21.1. La pertinence de la gestion de la capacité de connexion

Un réseau installé depuis de nombreuses années semble ne devoir évoluer que marginalement, au gré de quelques évolutions de l'entreprise. Ces évolutions restent

souvent mineures et ne justifient pas une augmentation brutale et conséquente du nombre de ports réseau. Disposer de réserves de connexion au réseau peut sembler une dépense considérable et inutile. Cependant, quelques exemples récents viennent mettre à mal cette théorie.

En premier lieu, la capacité à absorber de nouveaux besoins de connexion au réseau est inexistante (inférieure à trois prises) dans quelques locaux. Or l'arrivée de deux ou trois personnes supplémentaires, ne serait-ce que pour un renfort ponctuel, ne saurait être refusée, faute d'accès au réseau. La fourniture du service ne doit pas être décalée dans le temps pour permettre d'adapter la capacité de connexion au besoin.

Ensuite, le besoin évolue. Les serveurs, sur la raffinerie, n'utilisent qu'un seul port réseau. Ce nombre est appelé à doubler à l'avenir car l'informatique centrale du Groupe demande de plus en plus souvent la connexion au réseau des systèmes embarqués de gestion de serveur. Ces systèmes permettent, en cas de défaillance du serveur, d'agir sur celui-ci à distance. Cette fonctionnalité est certes utile dans le cas d'une externalisation de la gestion mais également pour faciliter la gestion interne au site, surtout si les serveurs sont placés dans un bâtiment distant de trois kilomètres du site de gestion. Cette situation, à l'échelle de la quarantaine de serveurs concernés, conduit à une demande de ports réseau qu'il est impossible de satisfaire aujourd'hui.

Enfin, le Grand Arrêt nécessite l'installation temporaire d'une centaine de prises réseau supplémentaires. Ce chiffre augmente de vingt pour-cent à chaque arrêt (tous les trois ans) car la mise en place de nouveaux services pour les entreprises intervenantes va de pair avec une utilisation croissante du réseau. Cette installation, pour temporaire qu'elle est, ne doit pas nécessiter une débauche d'argent et d'énergie pour sa mise en place et son retrait. La gestion de ce besoin temporaire de capacité est indispensable pour éviter toute sous-capacité, synonyme de perte de temps très coûteuse.

21.2. La gestion de la capacité de connexion

Une bonne pratique a guidé l'établissement de l'objectif de réserve. En disposant de vingt pour-cent de ports libres, le réseau est capable d'absorber les nouvelles demandes et laisse le temps de réagir face à la nature de cette demande. Si les changements sont structurels, ce seuil laisse le temps d'envisager une solution d'adaptation de la capacité, de la mettre en place et ainsi de garantir la continuité du service pour les utilisateurs. Faute de disposer de cette réserve, des situations de

saturation, incompréhensibles pour les utilisateurs, risquent de se produire. De plus, cette situation de mécontentement se prolongera dans le temps car une adaptation de cette capacité est assez longue. Par exemple, l'installation d'un nouveau commutateur réseau nécessite au moins une semaine et au plus deux mois, en fonction du stock d'équipements disponible chez le fournisseur.

Atteindre cet objectif n'est pas très compliqué : il suffit de procéder à un inventaire régulier, sur une base annuelle, de la réserve effective de ports réseau disponibles. Un outil tel que Cisco Network Assistant peut être d'une grande aide dans ce travail. La difficulté est donc moins technique qu'organisationnelle. Il est nécessaire de s'astreindre à effectuer cet inventaire sérieusement et régulièrement et surtout il importe que les résultats de cet inventaire débouchent sur des actions concrètes. Ainsi, en 2011, un tel inventaire a permis de justifier l'achat d'un commutateur réseau supplémentaire. Cela a mis fin à une situation de saturation dans tout un bâtiment et restauré une réserve de ports conforme à l'objectif.

21.3. La pertinence de la gestion de la capacité des liens

Comment une fibre optique, capable de véhiculer des informations à la vitesse de la lumière, peut-elle présenter un défaut de capacité ayant un impact direct sur la qualité de service du réseau ?

Actuellement, la bande passante installée est réputée suffisante. Cependant, certains usages spécifiques, comme la réplication de données en temps réel entre deux systèmes de stockages distants, ont montré que les limites peuvent facilement être atteintes. Cette restriction engendre des ralentissements sensibles et peuvent compromettre la bonne exécution de ces sauvegardes de données, ce qui est inacceptable. Dans cet exemple, la solution retenue a consisté à dédier un lien direct entre les deux systèmes afin que leur trafic n'ait pas d'impact sur le service. Une autre solution existe cependant : en fonction de la qualité de la fibre optique installée, il est possible d'utiliser une bande passante multipliée par deux voire par dix selon les configurations. Dans ce cas, il est important, lors de la pose d'une fibre optique, de peser les différences de coût entre une fibre de bonne qualité et deux fibres de qualité moyenne. La gestion de la capacité des liens est donc nécessaire pour économiser des ressources rares et chères mais également pour orienter les investissements sur des bases concrètes au regard des usages planifiés.

21.4. La réalisation de l'objectif de capacité

L'atteinte de l'objectif de capacité peut sembler aisée. Cependant, ce n'est pas un problème que l'on peut traiter superficiellement car la durée de vie d'une fibre optique se compte en décennies et il est économiquement impossible de poser de nouveaux liens dès qu'un nouveau besoin apparaît. Dans ce contexte, la gestion prévisionnelle prend tout son sens et revêt une importance stratégique. Cette gestion rejoint ainsi celle nécessaire à l'atteinte de l'objectif de capillarité.

La première étape consiste à réaliser un audit de l'utilisation des liens existants, puis d'en analyser les résultats. Cet audit doit donner des indications sur les liens les plus utilisés et permettre d'anticiper les actions à mener. Dans certains cas, il sera probablement nécessaire de procéder à l'installation de nouveaux liens optiques. Cette installation étant à la fois longue et coûteuse, il faut disposer de moyens objectifs de la justifier. C'est pourquoi l'atteinte de cet objectif passe par la mise en place de solutions de supervision adaptées, telles que mentionné précédemment.

22. L'atteinte de l'objectif de maillage

Le maillage, en lui-même, n'est pas nécessaire au bon fonctionnement du réseau et peut même le mettre en péril. Dans ce cas, pourquoi se donner comme objectif de généraliser cette technique ? La réponse à cette question précède la description de la trajectoire nécessaire à l'atteinte de cet objectif.

22.1. La maille, ennemie du réseau

Une maille est une solution de tolérance de panne. Le but est de pouvoir proposer, pour tout équipement réseau, un lien avec au moins deux voisins. L'ensemble de ces liens permet à un équipement de tomber en panne sans que le fonctionnement du réseau soit remis en cause.

Le réseau considéré est celui du niveau 2 du modèle OSI, formé de liens connectant entre eux des commutateurs. Parler de mailles à ce niveau est pratiquement une hérésie.

En effet, les réseaux sont constitués sur des modèles arborescents, afin justement d'empêcher qu'une maille n'existe. Ceci est dû à une particularité des réseaux commutés : la gestion de la diffusion (en anglais, *broadcast*).

Supposons qu'un PC nommé « A » veuille parler à un PC nommé « B » sur un réseau. Le problème de A, c'est qu'il doit, pour communiquer avec B, connaître l'identifiant de

B sur le réseau. Il s'agit du même problème pour un expéditeur qui doit connaître l'adresse du destinataire de son message (courrier, courriel...). Pour ce faire, les réseaux disposent d'un système de découverte. Ainsi, A va demander à l'ensemble des machines présentes sur le réseau s'il s'agit de B. Il n'est évidemment pas question pour A de connaître la liste de l'ensemble des machines présentes sur le réseau, sinon A n'aurait pas besoin de rechercher B sur le réseau. Ainsi, A va émettre une *trame de diffusion*, un message particulier demandant à B de répondre avec son identifiant.

Cette trame de diffusion, comme son nom l'indique, va être diffusée sur l'ensemble des ports réseau de l'ensemble des commutateurs du réseau. Le schéma suivant illustre un réseau comportant un PC A et un PC B appartenant au même réseau.

Les commutateurs sont représentés par des rectangles blancs, des flèches de couleur représentent les trames de diffusion. La flèche est dirigée dans le sens de la diffusion de la trame, de l'émetteur vers le destinataire.

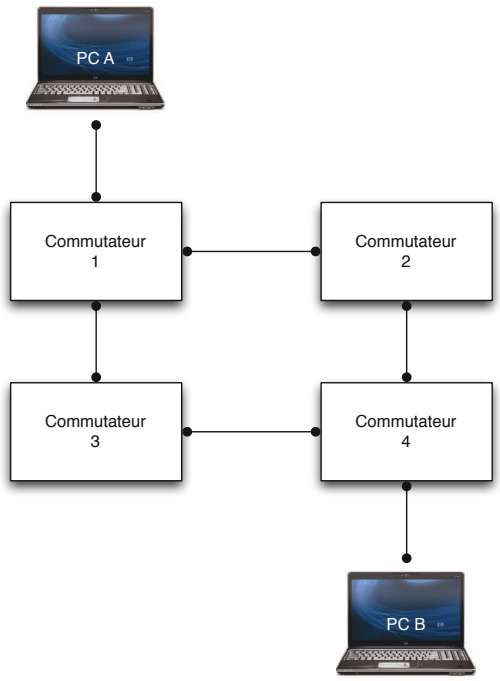
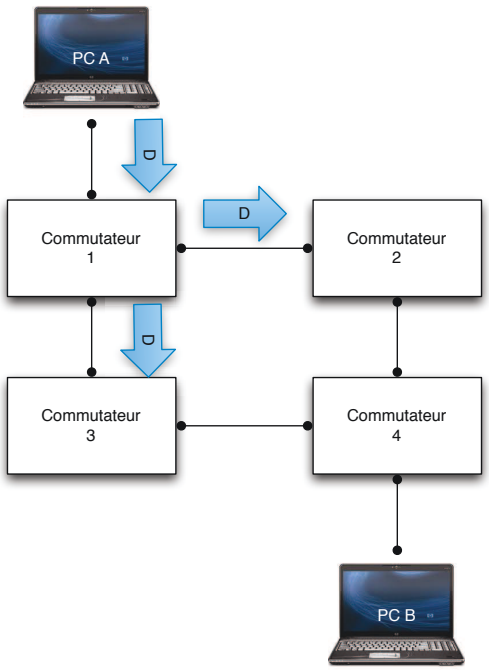


Schéma de principe d'un réseau maillé

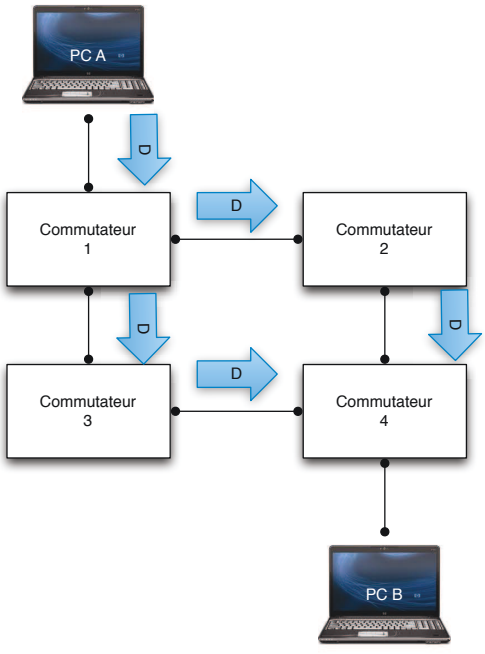
La trame de diffusion émise par A, ici représentée en bleu, arrive sur le commutateur 1. Ce commutateur l'identifie comme trame de diffusion et la diffuse à l'ensemble de ses connexions, à l'exception de celle qui a émis la trame. La trame de diffusion arrive donc sur les commutateurs 2 et 3, comme illustré ci-dessous. Cependant, elle n'est pas retournée à l'émetteur, ici le PC A.



Diffusion réseau : étape 1

À leur tour, les commutateurs 2 et 3 vont diffuser la trame de diffusion à leurs voisins, selon le même algorithme. Cette nouvelle étape de diffusion est illustrée ci-dessous.

Dans cette nouvelle étape, le commutateur 4 reçoit deux trames de diffusion. Ainsi, la première est diffusée sur l'ensemble des liens, à l'exception du lien ayant reçu cette trame. La seconde est diffusée selon le même principe.

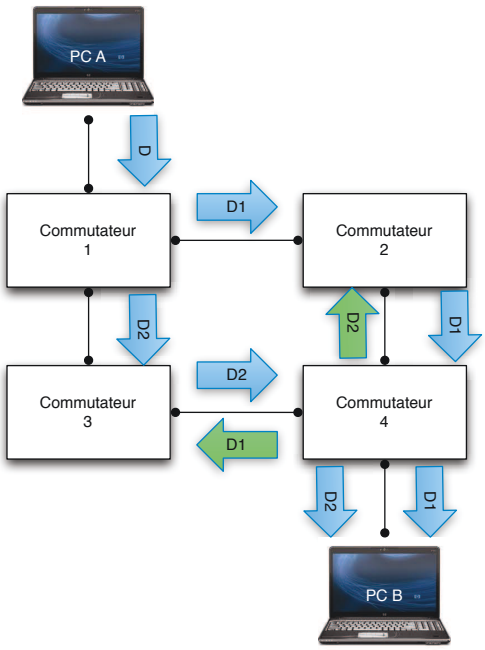


Diffusion réseau : étape 2

Le PC B reçoit donc deux trames de diffusion, alors qu'A n'en a émis qu'une. Cependant, ce n'est pas le plus grave. En effet, la trame de diffusion en provenance du commutateur 3 est diffusée au commutateur 2 et celle provenant du commutateur 2 est diffusée au commutateur 3 (flèches vertes sur le schéma ci-dessous).

Ci-après, pour plus de clarté, des numéros ont été ajoutés pour identifier les trames de diffusion en provenance des commutateurs 2 et 3. Cependant, cette représentation est inexacte car il s'agit bien de la même trame de diffusion, émise par le PC A, qui est transmise de proche en proche.

Ainsi s'amorce une *boucle réseau*. Les trames de diffusion vont se multiplier de manière exponentielle à chaque parcours de la maille sans qu'elles ne soient jamais arrêtées. Ce trafic multiplié, nommé *tempête de* broadcast*,* atteint très rapidement les limites de capacité de calcul des commutateurs : il y a saturation. Cette saturation avec des trames de diffusion empêche l'acheminement du trafic réseau. En l'espace de quelques minutes à quelques dizaines de minutes le réseau devient inutilisable. La seule solution pour rétablir le service consiste à ouvrir la maille.



Diffusion réseau : étape 3

Dans ce cas, comment concilier le bon fonctionnement du réseau et la tolérance de panne nécessaire à une installation dans un contexte industriel ?

22.2. La maille, meilleure ennemie du réseau

Une des solutions développées pour permettre la mise en place d'architecture robustes est logicielle. Un programme, embarqué dans les commutateurs, exécute un algorithme permettant de découvrir la topologie du réseau, d'identifier les chemins et les mailles et de construire une « carte » du réseau. Cette carte est très limitée : elle ne tient à jour que la liste des liens participant à des mailles. L'algorithme utilisé sur le site de Grandpuits est nommé par Cisco STP, pour Spanning Tree Protocol ou protocole de couverture d'arbre. Ce protocole est en fait inclus dans le standard 802.1D.

L'arbre, c'est le réseau. Le protocole cherche à construire un arbre à partir des mailles, en *élaguant* les branches qui conduisent à des mailles. Ainsi, dans la topologie précédente, il suffit de désactiver un seul lien pour que le réseau cesse d'être vulnérable aux tempêtes de broadcast. Cependant, en cas de rupture d'un lien ou de défaillance d'un équipement, le lien précédemment désactivé est immédiatement remis en service. Cette transition est transparente sur le réseau.

Le problème se situe lors de la constitution des mailles. Afin de ne pas être victime d'une tempête de broadcast pendant la détection des mailles, le commutateur se protège. À l'établissement d'un lien, le commutateur envoie une trame particulière. Si elle lui revient par un autre port, c'est qu'une boucle est constituée. Dans ce cas, l'ensemble des ports réseau du commutateur est fermé à la circulation des informations pour laisser le temps aux différents équipements participant à la maille nouvellement détectée d'échanger des informations de service et de choisir le lien qui sera bloqué. Cette interruption de service peut durer entre dix et cinquante secondes selon la version de STP implémentée, ce qui est une éternité en temps d'ordinateur. Cependant, la version la plus rapide permet de conserver les connexions établies et à ce titre permet des transitions pratiquement transparentes.

L'algorithme de Spanning-Tree est donc indispensable au fonctionnement d'un réseau maillé. Or, un réseau maillé est indispensable à une architecture robuste. C'est pourquoi l'objectif de maillage est tellement important et sa mise en œuvre peut se révéler ardue.

22.3. L'atteinte de l'objectif de maillage

Il est inutile de placer l'ensemble des équipements réseau dans des mailles. En effet, bien des équipements (téléphones, ordinateurs de bureau...) ne disposent que d'un seul lien au réseau et ne peuvent donc pas conserver leur connexion au réseau si le commutateur auquel ils sont reliés connaît une défaillance.

Cependant, il convient d'identifier les équipements « prioritaires », ceux dont le dysfonctionnement peut pénaliser la fourniture du service. Ainsi, certains équipements tendent à concentrer l'ensemble des liens vers les autres équipements. Dans cette topologie, dite « en étoile », la perte de l'équipement central entraîne l'arrêt complet du réseau. Ainsi, la première étape pour atteindre l'objectif de maillage est d'identifier les nœuds vitaux.

Ensuite, une analyse devra déterminer les actions permettant d'établir les mailles. Ces actions peuvent nécessiter l'installation de nouveaux équipements ou de nouveaux liens. Dans ce cas, l'atteinte de cet objectif devra être couplée avec l'atteinte de ceux cités précédemment afin de disposer d'une politique cohérente.

Enfin, un budget prévisionnel devra être établi pour donner une visibilité au management lors des négociations annuelles.

Conclusion

Ce projet a mis en évidence la complexité de la gestion des réseaux d'un site industriel. Les objectifs proposés ne peuvent être atteints rapidement et les jalons posés ont pour but de mesurer les progrès effectués.

Lors de la présentation des objectifs, quelques jalons devaient être atteints à la fin du mois de mai 2011.

Tableau VII : Rappel des jalons proposés pour mesurer l'atteinte de l'objectif

Date	Jalon
31/05/2011	Production d'un plan d'objectif de capillarité sur un an
	Préconisation d'une solution de gestion de capacité
	Préconisation d'une solution de gestion des risques

La production d'un plan d'objectif de capillarité a été réalisée, avec cependant un peu de retard. Ce projet ayant débuté en février 2011, le plan d'objectif de capillarité n'a été finalisé qu'au milieu du mois de juin. Par la suite, les projets en cours et les congés d'été ont rendu difficile le respect des délais de négociation budgétaire. Ainsi, le passage de la fibre optique entre les locaux ST1 et ST2, point clef de ce plan, n'a été inscrit au budget qu'au mois de septembre 2011.

La préconisation d'une solution de gestion de capacité a été réalisée en retard. En effet, la priorité était de produire le plan d'objectif de capillarité pour l'inscrire au budget. Au regard des sommes mises en jeu, la solution de gestion de capacité peut être mise en place en cours d'année alors que l'installation de nouveaux liens optiques nécessite le déblocage de sommes par la direction de la raffinerie. De plus, la solution préconisée est déjà en place (Cisco Network Assistant) et il suffit de consacrer un peu de temps à exploiter cet outil.

La préconisation d'une solution de gestion des risques n'a pas été réalisée complètement. En effet, les solutions de supervision peuvent, à elles trois, être considérées comme un système de gestion des risques. Cependant, elles ne sont pas configurées dans cette optique. Il est impossible de disposer, avec ces outils, d'une carte des risques et des mesures compensatoires adoptées. Le contexte économique très difficile rend l'acquisition d'une solution intégrée peu probable et l'établissement

d'une préconisation très peu prioritaire. C'est pourquoi les risques sont toujours gérés individuellement, sans politique ni outil global.

L'objectif de capillarité s'appuie sur une documentation difficile à entretenir. Le choix d'une solution de gestion des informations est difficile. Il faut choisir entre une solution commerciale l'ergonomie discutable mais bénéficiant d'un support par l'éditeur et une solution sur mesure développée en interne mais dont la pérennité est incertaine. Ce choix, maintes fois retardé, devrait être effectué durant le mois d'octobre 2011. Dans tous les cas, la documentation dressée au cours de ce projet servira à alimenter la solution pour qu'elle soit opérationnelle dès sa mise en place.

La solution adoptée pour gérer la capillarité servira également à l'objectif de capacité. En permettant de connaître l'état des liens (utilisé ou non), elle permettra de disposer facilement de statistiques objectives. L'outil Cisco Network Assistant viendra compléter ce dispositif en apportant les données relatives à l'utilisation des ports réseaux. L'administrateur réseau du site sera alors responsable de la production d'un rapport consolidant ces informations et indiquant les évolutions à effectuer.

L'objectif de maillage conjugue les deux précédents. La documentation produite lors d la réalisation de ce projet a mis en évidence des besoins de maillage. Sans une capillarité ou une capacité suffisante, il est impossible de mettre en place les mailles nécessaires à un fonctionnement sûr du réseau. C'est pourquoi les outils mis en place pour l'atteinte des deux précédents objectifs seront exploités pour atteindre celui de maillage. Réciproquement, l'objectif de maillage permettra de justifier des projets d'amélioration de la capillarité ou de la capacité.

Ce projet, en formalisant des objectifs, en établissant les bases documentaires et en critiquant les solutions mises en place, a permis de donner une structure cohérente aux tâches d'administration et d'exploitation des réseaux informatiques de la raffinerie. Cette organisation forme un véritable système de gestion des réseaux.

La gestion des réseaux, qui ne saurait être réduite à la mise en place de solutions de surveillance de fonctionnement des équipements, prend ainsi toute sa place au sein de la direction informatique comme contributrice de production de valeur pour l'entreprise.

23. La méthode générale de gestion des réseaux

Gérer des réseaux informatiques ne s'improvise pas. Il faut respecter des étapes, être rigoureux et ne pas la considérer comme une activité sporadique mais bien comme une tâche quotidienne.

Le premier élément clef de succès de l'implémentation de cette méthode est la définition de son périmètre. Elle ne s'intéresse qu'aux réseaux informatiques de l'entreprise, tels qu'ils ont été définis dans la première partie de ce document. Il n'est pas question de documenter des systèmes informatiques et les seuls éléments concernés sont les nœuds et les liens constitutifs des réseaux, à l'exception des équipements terminaux. Cette restriction est indispensable afin que l'accès aux informations demeure aisé. De plus, cette approche est nécessaire dans les cas où les parties « système » et « réseau » du service informatique sont gérés par des entités différentes et a fortiori si elles sont externalisées.

En premier lieu, la méthode repose sur l'information. Il faut constituer d'une part une bibliothèque contenant l'information statique, la documentation de l'architecture, les procédures et les modes opératoires. D'autre part, les informations dynamiques issues de la supervision sont indispensable à l'observation et au diagnostic.

En second lieu, la méthode repose sur des personnes compétentes pour exploiter ce système documentaire. Les règles de documentation sont écrites mais sont inutiles si leur lecteur les ignore ou ne dispose pas des moyens nécessaires à leur mise en œuvre. Le gestionnaire des réseaux est responsable de son outil de gestion et doit le maintenir en bon état de fonctionnement. Il doit également pouvoir transmettre ces informations sans risque pour leur qualité.

Enfin, la méthode facilite le partage des informations. Si cela peut comporter des risques, le classement des informations permet d'attribuer finement les droits de lecture ou de modification aux publics concernés.

23.1. La bibliothèque

La bibliothèque doit être organisée de manière à ce que chaque information soit facilement accessible, sans que le lecteur n'ait à la chercher longuement au sein de nombreux documents. La solution retenue est l'index structuré. L'index est présenté selon une hiérarchie, chaque branche de la hiérarchie contenant les même types d'information.

Voici l'index structuré tel qu'il a été retenu pour la documentation de la raffinerie :

Tableau VIII : exemple d'index structuré partiel de la documentation des réseaux

Type	Site	Intitulé	Date Relecture	Date Validation
Méthode	Tous	Règles de documentation		
		Convention de nommage		
Architecture	Tous	Architecture globale		
	Grandpuits	Architecture Bureautique		
		Architecture Industriel		
		Architecture Partemaires		
	Gargenville	Architecture Bureautique		
		Architecture Industriel		
Exploitation	Tous	Règles de sécurité		
	Grandpuits	Changement des paramètres de sécurité		
	Gargenville	Changement des paramètres de sécurité		
Administration	Tous	Administration de la téléphonie		

Il va de soi que la structure doit être adaptée à chaque installation documentée. Chez un autre client d'Ipsilan, cette structure a été modifiée car bien qu'il s'agisse de gérer

plus de quarante sites, seuls trois profils de site cohabitent. Cependant, les types de documents restent identiques.

La séparation entre « architecture », « exploitation » et « administration » peut sembler floue. C'est pourquoi elle est précisée dans le document « règles de documentation ». L'architecture regroupe l'ensemble des informations liées à la structure de l'installation. L'exploitation régit les changements à apporter à l'architecture. L'administration consiste à effectuer régulièrement des modifications qui ne portent pas sur l'architecture. Ainsi, les documents d'architecture contiendront les différents plans. Les documents d'exploitation incluront les règles, procédures et modes opératoires des changements d'architecture. Les documents d'administration porteront sur les règles, procédures et modes opératoires des opérations sans conséquence sur l'architecture, comme l'installation d'un nouveau téléphone par exemple.

Cette séparation est nécessaire car elle permet de segmenter précisément le public auquel les documents sont destinés. Ainsi, les documents d'architecture, souvent consultés mais rarement modifiés, sont destinés aussi bien à l'administrateur des réseaux qu'au manager chargé de valider une nouvelle installation ou au prestataire devant proposer une solution à un nouveau besoin. C'est pourquoi les documents d'architecture ne contiennent aucune information technique : ni marque ou modèle d'équipement, ni adresse IP. En effet, le manager n'est pas intéressé par ces informations mais plutôt par un schéma clair et épuré facilement compréhensible par quelqu'un dépourvu de la connaissance technique de l'administrateur. De même, l'administrateur ne consulte pas ces schémas pour obtenir des données techniques mais pour assimiler les chemins empruntés par les informations.

Chaque document est lui-même segmenté en niveaux de documentation. Le premier niveau correspond à une vision macroscopique de l'objet documenté. Ce niveau permet de comprendre le fonctionnement global de l'objet, son utilité et l'impact d'une défaillance sur les objets avec lesquels il est lié. Le deuxième niveau correspond au niveau 3 du modèle OSI. Il s'agit d'une vision d'assez haut niveau du fonctionnement de l'objet, permettant de s'abstraire des contraintes physiques pour comprendre la logique régissant son comportement. Enfin le troisième niveau, basé sur le niveau 2 du modèle OSI, s'attache à décrire le raccordement physique de l'objet avec ses voisins. Cette description s'intéresse, à chaque niveau, d'avantage aux interactions avec les autres systèmes plutôt qu'au fonctionnement interne de l'objet.

Ainsi, chaque niveau doit permettre de comprendre comment chaque objet communique. Souvent, le fonctionnement interne de l'objet est décrit par un document technique du constructeur des éléments constituant l'objet. Ainsi, un périmètre réseau est constitué de commutateurs. Il n'est pas question de décrire dans un document les liens entre les éléments d'un même périmètre (cette information est du ressort de la supervision) ni le fonctionnement d'un commutateur (lequel est documenté par le fabricant et devrait être maîtrisé parfaitement par l'administrateur réseau). Par contre, les filtres restreignant la communication entre deux périmètres ou entre deux zones du même périmètre doivent être détaillés car aucun outil de supervision ne pourra en fournir la liste, ni en décrire les raisons d'être, les règles de fonctionnement ou les manières de les implémenter.

La structure de l'index des documents permet ainsi à quiconque sachant ce qu'il cherche de le trouver sans délai. Si cette structure peut déconcerter au départ (cela a donné lieu à de longues démonstrations au début du projet), elle a finalement été adoptée parce qu'elle est claire et simple. Elle limite le nombre de chemins à explorer et guide le lecteur vers le document recherché, sans ambiguïté.

La structure seule ne permet pas d'identifier le contenu du document. L'index doit contenir des entrée pertinentes, exprimant de manière claire et concise le contenu ou au moins le thème du document. Ces entrées peuvent être différentes du nom réel du document. Dans ce cas, il est préférable de remplacer l'entrée statique par un lien dynamique tel un lien hypertexte qui va pointer vers le document sans que le lecteur n'ait à se soucier de l'emplacement réel du document. Cette logique est portée à l'extrême par des outils tels que Microsoft Sharepoint qui permettent de masque toute la complexité du système de gestion de fichiers et assurent directement l'archivage et la création de versions de documents. L'outil de travail collaboratif prend alors tout son sens. Cette approche n'a pas été testée dans le cadre de ce projet car la raffinerie ne dispose pas d'un tel outil. Cependant, une implémentation basée sur Microsoft Sharepoint a été réalisée avec succès chez un autre client d'Ipsilan.

23.2. La supervision

La bibliothèque ne fournit que des informations statiques. La supervision apporte les outils nécessaires à l'observation du fonctionnement du réseau au cours du temps. La supervision est souvent basée sur deux outils, parfois regroupés dans un seul et même logiciel.

Le premier outil de supervision doit procurer une vision globale du système. Cette vision est très utile à tout nouvel administrateur. Cependant, pour rester lisible, cette vision globale doit être hiérarchisée selon plusieurs niveaux d'abstraction. Ces niveaux prennent souvent la forme de plans tels que ceux établis par Cisco Network Assistant. Même des petits réseaux peuvent comporter des particularités topologiques rendant les plans difficiles à lire. Il est alors nécessaire de séparer les réseaux par périmètres et parfois même par zone afin de limiter le nombre d'éléments représentés. Les schémas d'architectures peuvent servir de base à la définition du contenu des plans.

Le second outil de supervision doit être capable de fournir en temps réel des informations et des alertes sur le bon fonctionnement des réseaux. Tous les équipements constituant le réseau doivent être surveillés par cet outil, sans exception. C'est pourquoi la mise à jour de l'inventaire des matériels, figurant dans l'index des documents, doit être assortie d'une mise à jour de l'outil de supervision. La mise en place d'un tel outil est complexe mais est grandement simplifiée par la qualité de l'étude préalable qui régit son installation. Les paramètres d'alerte (qui alerter, dans quel cas, selon quelles modalités...) sont des paramètres clefs de succès. Il est très difficile de régler précisément un système de supervision avec des paramètres flous.

Ces deux points mettent en évidence une difficulté réelle de la gestion des réseaux. S'il est spontanément admis que des outils de supervision sont nécessaires, il est beaucoup plus difficile de faire accepter à un client d'investir dans un système documentaire de qualité. Pourtant, sans documentation, la mise en place des outils de supervision est un leurre. S'il est impossible de disposer des critères précis pour constituer les plans par manque de schéma d'architecture, s'il est impossible de vérifier l'exhaustivité du parc supervisé par manque ou imprécision de l'inventaire, alors il est impossible d'avoir une vision nette du fonctionnement du réseau.

Il est théoriquement possible de piloter une voiture dont les fenêtres ont été occultées, simplement avec une carte, une boussole, un chronomètre et un indicateur de vitesse. En réalité, personne ne s'y risquerait. Pourtant, parce qu'il est théoriquement possible de limiter la gestion des réseaux à leur supervision, beaucoup d'entreprise négligent de disposer d'une documentation de leur réseau.

La supervision doit fournir des informations dynamiques et pertinentes. La fréquence de mise à jour des informations est un paramètre sensible. Une fréquence trop élevée consomme beaucoup de ressources matérielles et réseau et peut engendrer des faux

positifs (détection de problèmes transitoires sans importance, voire de problèmes inexistants). Une fréquence trop basse peut prévenir la détection de défauts et empêcher le diagnostic de problèmes liés au réseau. De plus, selon l'interrogation pratiquée par le système de supervision, la fréquence doit être adaptée. Par exemple, il est souvent peu important de surveiller le serveur Web embarqué dans un équipement. Dans ce cas, une période de test de dix minutes peut être acceptable. En revanche, un dysfonctionnement des fonctions réseau d'un équipement doit être détecté en une minute, voire moins pour les équipements les plus critiques.

De plus, l'action déclenchée par la détection d'un défaut doit être sérieusement étudiée. La méthode généralement adoptée pour alerter les administrateurs est l'envoi automatisé de courriels à une liste de diffusion. La plupart des alertes donnent alors lieu à de véritables raz-de-marée de courriels, noyant l'information réellement pertinente sous un océan de parasites. Ce comportement est dû à la notification systématique de l'ensemble des défaillances. Ainsi, si de nombreux équipements sont accessibles par un seul chemin, la rupture de ce chemin va entraîner une alerte par équipement détecté défectueux. Chaque alerte peut alors déclencher un courriel automatique. Dans le pire des cas, chaque service surveillé déclenche une alerte et la prolongation du problème dans le temps entraîne une répétition de l'envoi de courriels. La défaillance d'un seul équipement chez un client d'Ipsilan a ainsi suffi a générer l'envoi de plus de neuf cents courriels ! Dans ce cas, l'arrêt du système de supervision est le seul moyen efficace pour autoriser le diagnostic, ce qui va à l'encontre de sa raison d'être. La notification doit être limitée au strict nécessaire et ne pas pouvoir générer des masses incompréhensibles d'information. Ce point, souvent négligé dans le cadre d'un projet de mise en place d'une solution de supervision, est pourtant essentiel. Peu de solutions du marché savent vraiment gérer de manière efficace les notifications. La complexité des réglages peut pénaliser la facilité de maintenance de la solution. De nouveaux arrivants sur le marché, tels que NEDI[12], se différencient précisément sur la gestion des notifications face aux solutions traditionnelles, moins souples.

Les solutions de supervision sont dérangeantes : elles interrompent le travail de l'administrateur pour lui signaler un dysfonctionnement. Cette interruption, pour inopportune qu'elle soit, est indispensable. Dans le cas d'un système devant fonctionner en permanence, la notification se doit également de cibler des contacts disponibles en permanence. Là encore, une étude doit être menée. En effet, maintenir

une astreinte en dehors des heures ouvrées n'est pas chose aisée. C'est en premier lieu un choix entre faire et faire faire. La notification doit-elle parvenir à un salarié de l'entreprise ou bien à une entreprise ? Dans le premier cas, il convient de se rapprocher du service des ressources humaines et d'obtenir l'accord des personnes concernées. Dans l'autre cas, l'astreinte doit être régie dans un contrat encadrant les modalités d'action et précisant les moyens d'intervention. Dans le cas d'une usine classée Seveso seuil haut, la nécessité de l'habilitation des intervenants, de la délivrance d'une autorisation de travail et d'un bon de validation peuvent pénaliser la rapidité de rétablissement du service si celle-ci requiert une intervention sur site.

Les modalités de notification (courriel, surveillance d'un écran de contrôle, alerte téléphonique...) sont également des points délicats d'un système de supervision. Le choix est à faire en fonction des niveaux de services négociés, des délais d'interruption acceptables. Le recours à un partenaire d'astreinte externe peut également conditionner certaines options. Ainsi, un courriel laisse une trace horodatée dans les systèmes de l'expéditeur et du destinataire. Cette information sert souvent de base de temps pour la mesure des délais d'intervention et de résolution de problème. Les systèmes d'alerte téléphonique sont beaucoup moins fiables et les messages peuvent être retardés considérablement en fonction de la charge du réseau de l'opérateur téléphonique. Dans ce cas, les deux horodatages diffèrent de manière importante, pouvant mener à des conflits selon les termes du contrat. De plus, les hypothèses de fonctionnement supposent qu'une partie du réseau reste opérationnelle et permet l'envoi des notifications. Toutes ces questions influent grandement sur le choix de la solution de supervision et sur la définition de son architecture. Alors que, bien souvent, un produit de supervision est envisagé comme un produit « clef en main », il se révèle être un ensemble doté de très nombreux paramètres complexes et dont aucune des valeurs n'est évidente. L'ajustement des paramètres est une des missions de l'administrateur du réseau afin de pouvoir disposer d'un système pertinent et exhaustif.

23.3. Les difficultés et les limites de la méthode

Lors de la mise en place de cet outil méthodologique, la première difficulté a été de faire adhérer les personnes constituant son principal public : l'équipe informatique locale. Lors des premières réunions d'avancement, l'originalité de l'approche a déconcerté quelques participants. La méconnaissance du modèle OSI par certains a

obligé à expliquer cette norme dans le document d'organisation, ce qui l'a considérablement alourdi. Il a également, fallu éviter de prononcer le mot « ITIL » en réunion. Cette méthode est associée dans l'esprit de l'équipe informatique locale à un certain nombre de difficultés organisationnelles au sein de la DSI de Total ayant des conséquences négatives sur la qualité de service ressentie par les utilisateurs. Utiliser le nom « ITIL » garantissait un rejet immédiat de cette approche. La remise en cause de la solution de supervision a été parfois perçue comme inutile, alors même que simultanément des demandes d'amélioration étaient formulées.

Globalement, les difficultés à l'instauration de cet outil ont été humaines. La pédagogie et quelques techniques de gestion du changement ont été très utiles pour faire accepter cet outil.

Cette méthode présente également quelques limites. Comme pour toute méthode, avant de pouvoir utiliser les informations disponibles, il est nécessaire de lire, a minima, le document de structure expliquant l'organisation des documents. Or, comme l'a écrit D. Pennac, « à y regarder de près, personne n'a jamais le temps de lire.[13] » C'est particulièrement vrai dans le cadre professionnel, quand il s'agit pour un intervenant extérieur d'intervenir en urgence dans le cadre d'une astreinte nocturne. Dans ce cas, il vaut mieux intégrer aux documents un aide-mémoire très court (une feuille A4 recto-verso) comprenant les points clefs nécessaires à un dépannage rapide. Ce document doit lister les outils les plus importants et en donner les moyens d'accès sans toutefois inclure les mots des passe éventuellement nécessaires. Ces derniers devront être traités selon la politique de sécurité en vigueur dans l'entreprise.

La structure même des documents constitue une limite. En effet, ils sont rédigés en utilisant deux outils. Si le traitement de texte Microsoft Word fait partie des logiciels installés par défaut sur l'ensemble de postes de la raffinerie, les schémas illustrant les documents sont créés avec Microsoft Visio, seulement disponible sur demande et dans une version ancienne. Ainsi, l'évolution des schémas nécessite de mettre à jour deux documents, le dessin proprement dit et le texte dans lequel il est inclus. Cela, combiné avec la nécessité de gérer les versions de chaque document pour historiser les changements, peut dissuader de maintenir les informations à jour lors de changements. La gestion automatique des versions de Microsoft Sharepoint est alors d'une grande aide. Cependant, disposer d'un outil unique permettant à la fois de créer du texte et de les illustrer par des schémas techniques faciliterait grandement la

maintenance des documents. À ce jour, aucun logiciel proposant ces fonctionnalités n'a été identifié.

La supervision soulève également quelques difficultés. L'exemple des notifications a été précédemment évoqué, qui peut représenter un véritable obstacle à une utilisation efficace des outils.

La difficulté de mise à jour du système, notamment lors de l'ajout de matériels inédits, soit dans leur modèle, soit dans leur contexte, peut conduire à délaisser cette solution. Dans un réseau, tous les équipements doivent être supervisés. Cela inclut leur présence dans le système et l'association d'une politique de notification pertinente. Pourtant, certaines entreprises prennent le risque de ne pas superviser une partie de leurs équipements, souvent parce qu'ils ont un comportement instable et génèrent un flot trop important de notifications ou bien pour des raisons financières, chaque équipement pouvant nécessiter l'acquisition d'une licence. Parfois, la notification est temporairement désactivée, notamment lors de maintenances planifiées, mais l'administrateur peut oublier de la réactiver. Ce problème est impossible à détecter automatiquement. Seul un audit régulier des équipements pour lesquels les notifications sont désactivées permet de vérifier la pertinence de cet état. Cependant, peu d'outils permettent ce genre d'audit. L'administrateur doit alors vérifier les équipements un par un. Outre l'aspect fastidieux de cette tâche répétitive, le temps nécessaire à l'audit d'un parc de moyenne envergure (l'audit de deux cents équipements peut demander une semaine de travail, à raison de dix minutes par équipement) relègue cette action à des moments de moindre activité. Concrètement, un audit n'est mené que lors d'un apport temporaire de main-d'œuvre, en le déléguant à un stagiaire par exemple.

Toute méthode est une référence à adapter au contexte dans lequel elle est appliquée. Celle exposée ici ne fait pas exception. Plus que son contenu actuel, c'est la compréhension de l'approche retenue qui permet de l'implémenter dans d'autres entreprises. Il n'est pas question de proposer une solution unique mais de donner une façon souple et pratique d'aborder la gestion des réseaux informatiques. Cette technique, testée chez Total puis dans une entreprise n'ayant aucun point commun avec la raffinerie de Grandpuits, a montré une grande facilité d'adaptation. Aujourd'hui, la mise en place de cette méthode permet aux entreprises de valoriser leur documentation et leur supervision au sein d'un système cohérent, aisément exploitable et maintenable.

Bibliographie

Normes :

[1] NF EN ISO/CEI 7498 — Modèle de référence de base pour l'interconnexion des systèmes ouverts. Afnor, 72p, 1995.

[2] NF EN 62491 — Systèmes industriels, installations et appareils et produits industriels. Etiquetage des câbles et des conducteurs isolés. Afnor, 35p, 2008.

[3] IEC 81346 — Systèmes industriels, installations et appareils, et produits industriels - Principes de structuration et désignations de référence. ISO, 326p, 2009

[4] NF Z61-000 — Traitement de l'information — Vocabulaire international de l'informatique. Afnor, 418p, 1986.

Ouvrages :

[5] J. Akoka, I. Comyn-Wattiau. Encyclopédie de l'informatique et des systèmes d'information. Vuibert, 1941p, 2006.

[6] G. Pujolle. Les réseaux, édition 2011. Eyrolles, 786p, 2010.

[7] N. Simoni, S. Znaty. Gestion de réseau et de service : similitude des concepts, spécificité des solutions. Dunod, 479p, 1997.

Liens internet :

[8] Request For Comments SNMP : http://www.ietf.org/rfc/rfc1157.txt Consulté le 09/07/2011

[9] Norme 802.11AB et Cisco Discovery Protocol : http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html Consulté le 22/07/2011

[10] Norme IEEE 802.1D et Spanning-Tree Protocol : http://standards.ieee.org/getieee802/download/802.1D-2004.pdf Consulté le 01/10.2011

[11] Animation illustrant le fonctionnement du Spanning-Tree Protocol : http://www.cisco.com/warp/public/473/spanning_tree1.swf Consulté le 01/10/2011

[12] Solution de supervision NEDI : http://www.nedi.ch Consulté le 01/11/2011

Ouvrages hors champ :

[13] D. Pennac. Comme un roman. Folio, 198p, 1992.

[14] R. Kipling. Just So Stories. Macmillan & Co, 122p, 1902.

Résumé / Summary

Français

La gestion des réseaux informatiques est un enjeu crucial pour les entreprises qui en dépendent toujours plus. Cette gestion est le plus souvent partielle, déléguée à des outils de supervision incomplets ou inadaptés. En formalisant une méthode réunissant documentation structurée et supervision, ce projet apporte une solution durable à ce problème. Testée dans un contexte industriel où la défaillance de réseaux peut conduire à des catastrophes, cette approche a montré ses avantages et inconvénients. Elle a également prouvé qu'elle pouvait être adaptée à d'autres contexte et mis en évidence sa rentabilité.

Mots-clefs : gestion des réseaux informatiques, documentation, supervision, réseaux, télécommunications.

English

The management of IT networks is a crucial stake for organisations as their activity relies on it more and more. Managing the network if often a partial solution based on unadequate or incomplete supervision tools. Formalizing a methode that combines structured documents and network monitoring, this projects aims at providing a long-term solution to this problem. While tested in an industrial context where network failure can drive to a disaster, this technique demonstrated its pros and cons. It also made an evidence of its adaptability to other situations and it's profitability.

Keywords : IT network management, documentation, monitoring, networks, telecommunication.