Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Administration d'un réseau d'entreprise : Du quotidien jusqu'aux projets

Yanis BELHAMEL

DOCAPOSTE

Responsable entreprise : Bertrand Hernandez

Responsable académique : Arnaud Février

2021

Table des matières

Introduction

Dans le cadre mon diplôme universitaire et Technologique, j'ai effectué un stage de fin d'étude de 10 semaines au sein de l'entreprise DOCAPOSTE, filiale du groupe « La Poste », dont l'activité s'articule autour du traitement numérique de l'information.

J'ai intégré la Direction des Systèmes d'Information (DSI) de DOCAPOSTE et plus précisément l'équipe d'Administration Réseaux.

Après une présentation de l'entreprise qui m'a accueilli, ce rapport présente les différentes missions que j'ai réalisé au cours de cette expérience :

Une partie de mon activité a été d'accompagner l'équipe dans ses charges quotidiennes d'exploitation de l'infrastructure réseaux et télécoms.

J'ai également pu prendre part à des missions plus ponctuelles comme :

- La normalisation et le renommage du parc d'équipements
- L'urbanisation de racks d'hébergement en Datacenter
- Le déménagement d'un site de production industrielle.

1 Présentation de l'entreprise

1.1 Le groupe « La Poste »

La Poste est une entreprise publique connue grâce à une histoire commune aux français depuis plus de six siècles. D'administration d'État (dirigé par un ministère), La Poste est passée en 1991 au statut d'Établissement public à caractère industriel et commercial pour enfin devenir en 2010 une société anonyme à capitaux 100% publics.

Grâce à son modèle multi activité, La Poste affirme sa position d'opérateur de services de proximité humaine. C'est aussi la meilleure stratégie pour ne passer à côté d'aucune opportunité et s'inscrire dans la durée. Pour cela, les activités ont été organisées en 5 branches ce qui permet de répondre aux enjeux d'aujourd'hui et de demain…

Fig. Branches du groupe « La Poste »

Le groupe se résume également en quelques chiffres clés :

- 24,7 milliards € de CA dont 24,4% à l'étranger.
- 17.100 points de contact sur l'ensemble du territoire.
- Présence dans 230 pays et territoires avec DPDgroup/Geopost.
- 1ère flotte électrique au monde avec 37.524 véhicules électriques.
- 253.000 collaborateurs dont 52,4% de femmes.
- 160 métiers dans les 5 branches d'activités.
- 4ème recruteur de France et 13ème dans le numérique.
- 1ère entreprise utile selon les Français.
- 23 milliards d'objets délivrés /an dans le monde.
- 1er hébergeur de données de santé en France via sa filiale DOCAPOSTE.
- 1er prêteur aux collectivités locales.

1.2 La branche Numérique

La branche Numérique est au cœur du développement et de la transformation du Groupe La Poste en s'appuyant sur les besoins du client final, qu'il soit une entreprise, une administration ou un particulier, touché directement ou indirectement. Elle a un double rôle :

- Une activité commerciale : développer du chiffre d'affaires avec ses business units – DOCAPOSTE, Mediapost Communication et laposte.fr ;
- Une activité de transformation : moderniser les process internes, développer de nouveaux services pour le compte des branches afin d'accélérer la transformation du Groupe et d'affirmer sa position dans le numérique.

Ses 8000 collaborateurs accélèrent quotidiennement la transformation numérique. Développeurs, data scientists, product manager officers (PMO)… la branche Numérique réunit une diversité d'expertises complémentaires autour de la confiance numérique et ce, avec des valeurs partagées :

• **Sécurité.**	• **Neutralité**	• **Pérennité**	• **Universalité**
Confidentialité des données (prestation de serment, déploiement de la charte DATA).	Garantie d'un même service pour tous.	Des valeurs historiques et des offres durables dans le temps.	Des offres qui donnent la maîtrise aux utilisateurs et qui s'adressent à tous.

Fig. Valeurs de la branche Numérique

1.3 DOCAPOSTE

1.3.1 Présentation Générale

Filiale numérique du Groupe La Poste, DOCAPOSTE accompagne toutes les entreprises et administrations dans leur transformation numérique : Elle leur propose des solutions adaptées à l'ensemble de leurs besoins, les aides à fluidifier et à sécuriser leurs échanges et transactions, et elle les soutient dans leur stratégie et leur rythme de transformation.

DOCAPOSTE propose des offres standardisées et des solutions sur mesure pour répondre à chaque client selon ses besoins. Elle couvre tous les secteurs d'activité avec une expérience renforcée et des investissements concentrés sur 4 marchés prioritaires : Banque Assurance, Secteur Public, eSanté et Mass Market. Les services ainsi proposés se regroupent en trois composantes majeures :

• **Services documentaires**	• **Services numériques**	• **Services humains**
Gestion de courrier entrant, Gestion de courrier sortant, Dématérialisation (capture, indexation, numérisation), Composition, Éditique, Diffusion multicanal, Marketing Direct.	Identification et connaissance client, Certification et signature électronique, Plateformes (d'intermédiation ou métiers), Paiement électronique, GED / Workflow, IoT, Archivage numérique, Vote, Identité Numérique (IN).	Gestion déléguée de processus métiers, Centre de Relation Client, Conseil en UX, Recrutement de profils digitaux.

Fig. Familles de Services proposés par DOCAPOSTE

1.3.2 Stratégie

En 2018, DOCAPOSTE a posé les fondations de sa nouvelle stratégie 2023 et la synthétise au travers des éléments ci-après :

- **UNE mission** : concevoir et opérer des plateformes intelligentes qui simplifient les échanges de flux physiques et numériques BtoBtoC (Business to Business to Customer) pour les clients ;
- **3 enjeux** : accélérer la croissance, renforcer les expertises métiers, offrir une vision consolidée des solutions ;
- **4 marchés prioritaires** : Banque Assurance, e-Santé, Secteur Public, Mass-Market ;
- **5 facteurs clés de succès** : atteindre une taille critique, exceller dans nos savoir-faire, assembler les actifs, être orienté client, avoir un collectif moteur ;
- **7 savoir-faire** : UX/UI, Conseil & ressources, Offres packagées, Éditique & MD, Confiance numérique, Back-office & paiement, Plateformes & IOT ;
- **1 posture « ABCDE »** : Agilité, Business, Collectif, Délégation, Excellence.

1.3.3 Implantations Géographiques

Les effectifs de DOCAPOSTE sont répartis sur de nombreux sites internes et clients dans les départements de métropole et d'outre-mer :

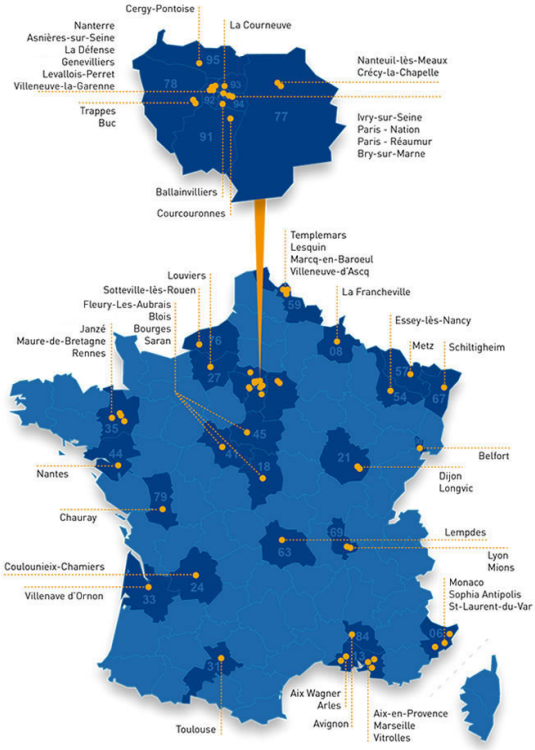

Fig. Implantations de DOCAPOSTE en France Métropolitaine

Mais aussi en Europe et dans le monde :

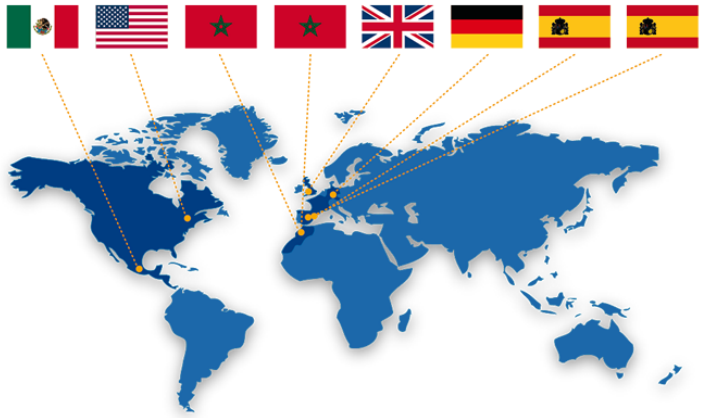

Fig. Implantations de DOCAPOSTE hors France

En parallèle de ces implantations, DOCAPOSTE héberge l'ensemble de ses systèmes d'Information autour de quatre centres de données (Datacenters) répartis sur le territoire métropolitain.

1.3.4 Clients de DOCAPOSTE

90% des entreprises du CAC 40 sont clientes DOCAPOSTE. Au total, ce sont plus de 23.000 administrations et entreprises de toutes tailles et de tous secteurs d'activités qui font confiance en DOCAPOSTE. Ci-dessous quelques exemples classés par secteur :

Fig. Clients Représentatifs de DOCAPOSTE

1.3.5 DSI - Solution Numériques

Mon intégration chez DOCAPOSTE s'est déroulée au sein de la Direction des Systèmes d'Informations « Solutions Numériques ». Cette DSI est constituée d'environ 120 personnes et dispose de deux entités, DSI Solutions Numériques basée à Aix en Provence et la DSI Confiance basée à Ivry sur Seine. Elle est en charge de l'hébergement et de l'exploitation IT pour 6 des 7 Business Units de DOCAPOSTE. Elle s'intègre à la société comme un pôle de compétence transverse comme le montre l'organigramme ci-dessous :

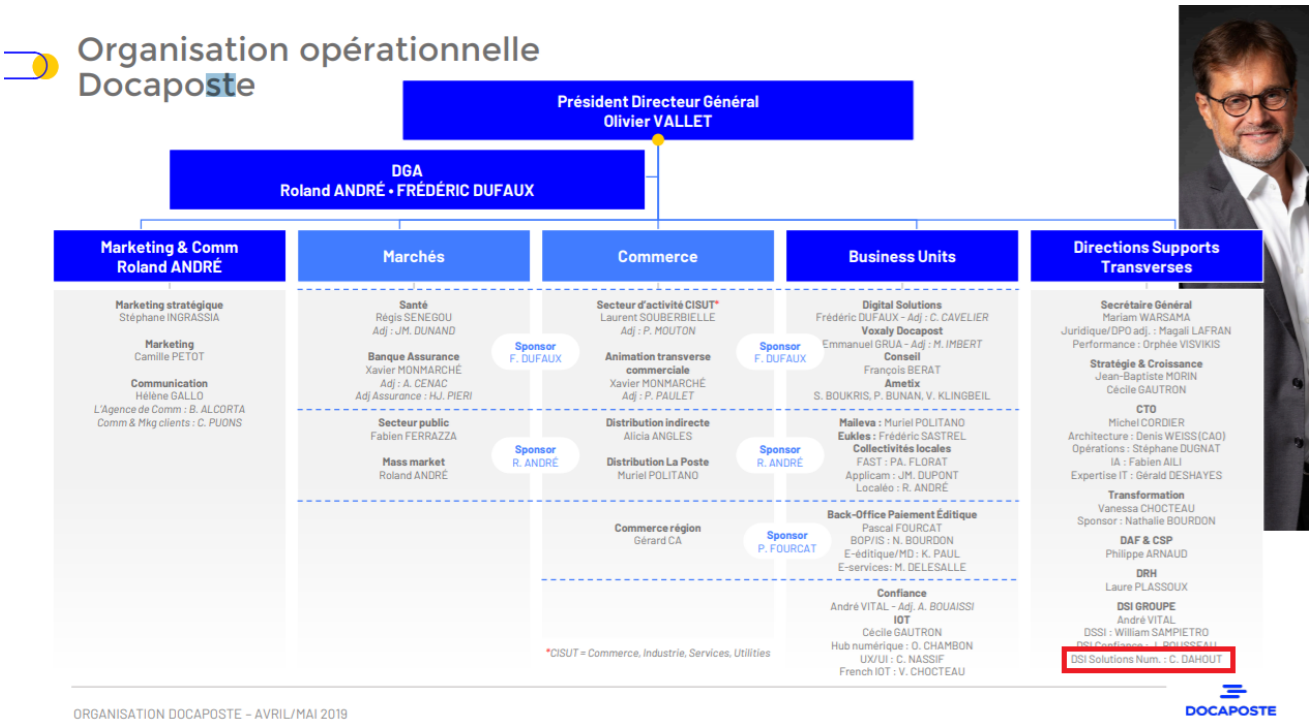

Fig. Intégration de la DSI-SN au sein de DOCAPOSTE

1.3.6 Direction Technique

La Direction Technique de la DSI-SN regroupe les activités d'architecture et d'exploitation des éléments IT des systèmes d'information de DOCAPOSTE.

Elle articule ses 30 collaborateurs autour de 4 pôles de compétence :

- Architectures IT
- Bases de Données
- Systèmes
- Réseaux

Elle assure un rôle tout au long de la vie des projets de DOCAPOSTE : des offres d'avant-vente à l'exploitation quotidienne des infrastructures.
Dans le cadre de mon stage, j'ai pu intégrer l'équipe réseaux et conserver une relation privilégiée avec les autres équipes.

1.3.7 L'équipe d'Administration Réseau

L'équipe « Admin Réseau » est en charge de l'exploitation, du maintien en conditions opérationnelles (MCO) et des évolutions de tous les composants IT permettant d'échanger des informations.

Elle participe également à la vie des solutions techniques retenues par un échange quotidien avec les équipes d'architecture, les fournisseurs de services et les intégrateurs de matériel.

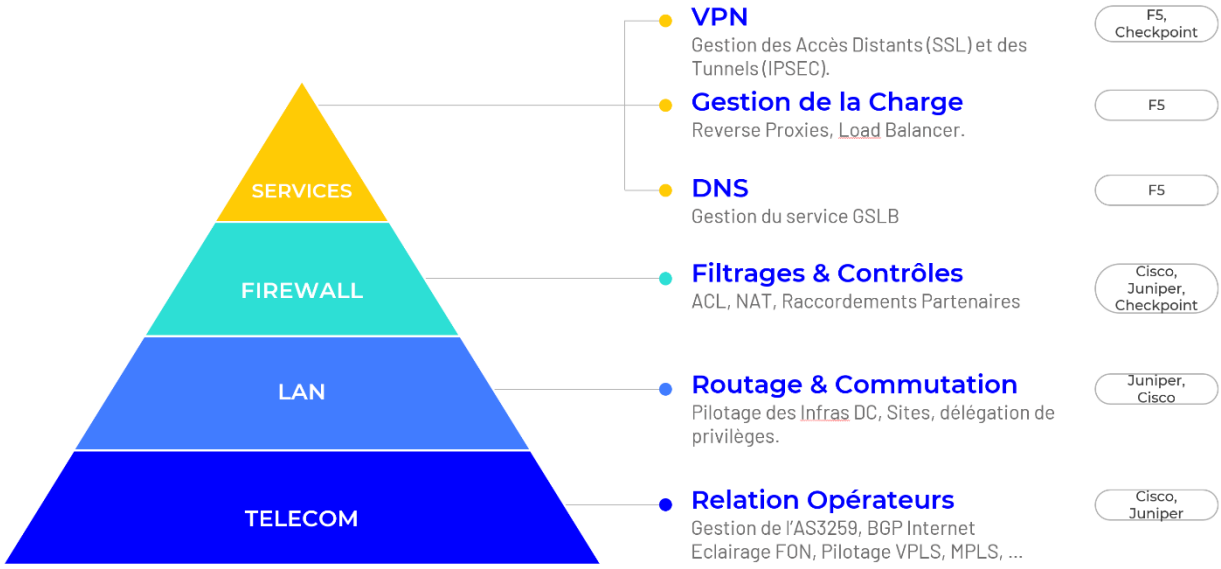

Fig. Missions & Périmètres de l'équipe d'Administration Réseau

Constituée de 9 personnes, elle assure aussi le support (niveau 3) aux exploitants de production et peut être amenée à échanger avec les clients finaux pour des diagnostics avancés.

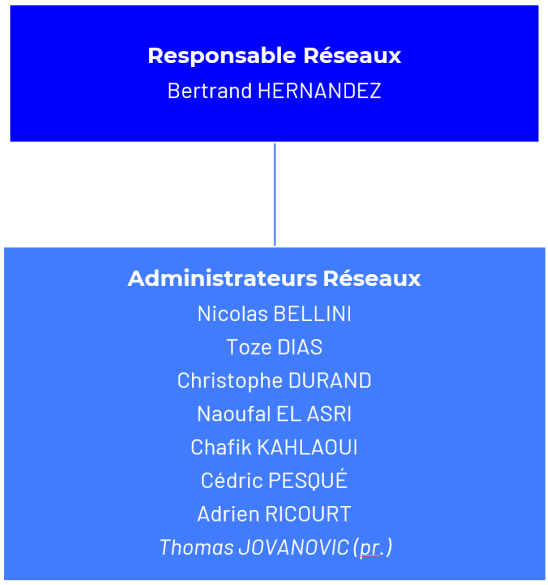

Fig. Constitution de l'équipe d'Administration Réseau

2 L'intégration dans l'équipe

Pour mon intégration au sein de l'équipe, j'ai été mis en immersion avec les différents membres pour pouvoir bien appréhender l'infrastructure réseau et sa gestion.
Cela m'a permis de voir les différents Datacenter localisés dans le sud de la France (Aix en Provence et Marseille) et les différentes actions à réaliser à l'intérieur de ceux-ci.
Par ailleurs, j'ai pu voir aussi le quotidien de l'équipe sur d'autres aspects comme le traitement des demandes de travaux, ou des incidents de production.

2.1 Le quotidien de l'équipe

L'une des tâches quotidiennes de l'équipe est le traitement de demandes et d'incidents. Ils reçoivent les demandes à travers un logiciel de gestion des services (HP Service Manager) qui les répartit selon le service concerné. Il peut y avoir des demandes pour l'équipe réseau, l'équipe système, l'équipe de sécurité… Ensuite, les demandes sont catégorisées en fonction de leur contenu.

L'équipe réseau va traiter de multiples types de demandes comme :

- Ouverture de flux firewall
- Remplacement de certificats SSL (configuration de Reverse Proxies)
- Redirection d'URL (configuration de Reverse Proxies)
- Ouverture de flux VPN

Ce sont des actions quotidiennes demandées par les autres services de la DSI mais également par les propriétaires des projets métiers.

Les différents membres m'ont appris à répondre à deux types de demandes :

- Les ouvertures de flux firewalls
- Le marquage de VLAN

2.1.1 Les ouvertures de flux firewalls.

Un firewall permet de contrôler le trafic entre différentes zones, en surveillant/filtrant les flux qui y transitent. Habituellement, ces zones, dites de confiance comprennent Internet (zone dont le niveau de confiance est faible), et au moins un réseau interne (une zone dont la confiance est plus importante). Ils existent plusieurs types de firewall qui vont correspondre à certaines couches du modèle OSI. Dans le cas de l'entreprise DOCAPOSTE, les pare-feu réseaux « à états » (statefull) utilisés (niveau OSI 4) lors de l'emploi du mot firewall.

Tous les réseaux DOCAPOSTE sont protégés par un firewall. Ces derniers utilisent des listes d'accès (ACL) afin de définir les règles de passage et de refus d'un flux TCP.

Les firewalls doivent garantir quels composants ont le droit de discuter avec quels autres composants grâce à l'ACL correspondant au flux.

Lors de la réalisation de l'ouverture, l'équipe va avoir un fichier Excel ou une demande qui indique la machine source et celle de destination avec leur adresse IP. Une adresse IP est un identifiant donné à un périphérique informatique qui est relié à un réseau. Cette adresse est la base de l'échange de donnée sur Internet et entre différents réseaux.

Ainsi, notre ACL va être placé le plus proche possible de la source. Pour repérer celle-ci, nous allons utiliser l'outil OpsUI qui va nous permettre de trouver sur quel firewall est située notre machine de destination. OpsUI est un outil interne à l'entreprise DOCAPOSTE permettant entre autres à partir d'une adresse IP pouvoir déduire sur quel firewall et interface, la machine de destination est située.

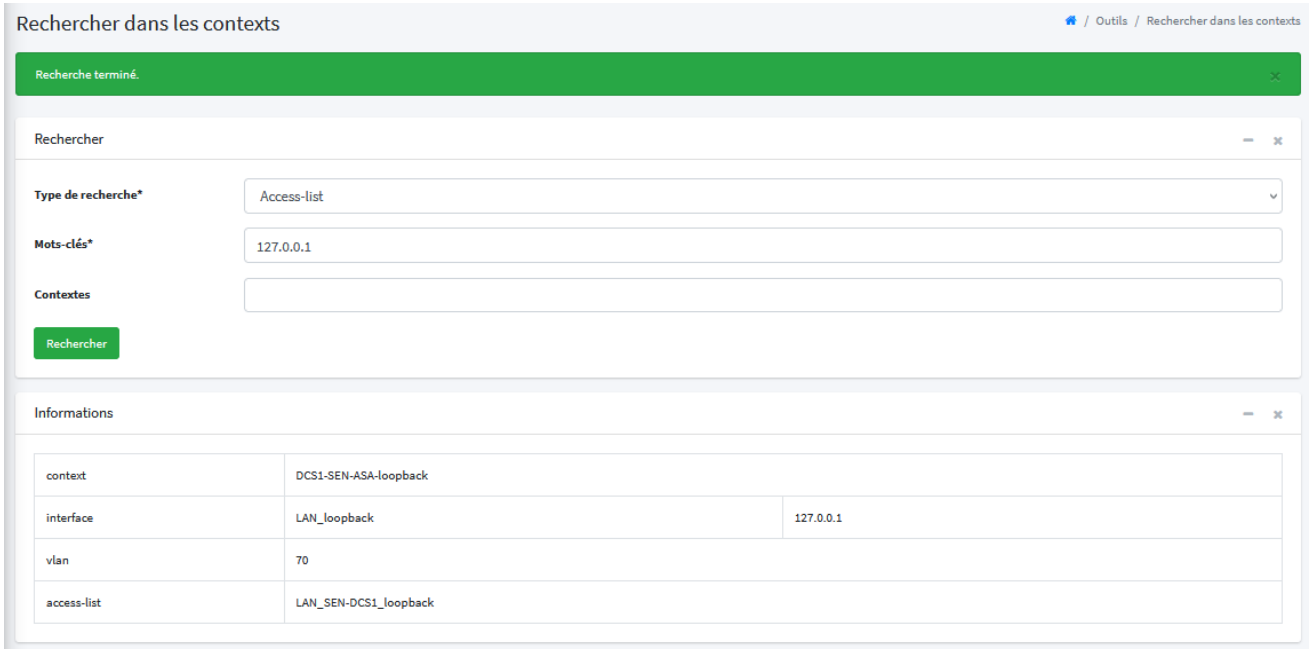

FIg. de l'application web OpsUI pour repérer le firewall et l'interface en fonction de l'adresse IP.

Ensuite, nous allons utiliser un second outil : WebSVN
Cet outil dispose des diverses configurations des firewalls DOCAPOSTE permettant ainsi à l'équipe d'avoir les sauvegardes de ceux-ci et de revenir en arrière en cas de problèmes lors de modification.

Il permet aussi de voir la configuration d'un firewall. À partir de la configuration d'un pare-feu, on peut donc situer les objets et les ouvertures de flux présents sur celui-ci et donc de créer des objets et les ouvertures s'ils sont manquants : C'est ainsi que nous allons vérifier l'existence de notre objet.

2.1.2 Le Marquage de VLAN

Le marquage de vlan consiste à mettre un vlan sur un port d'un switch. Un VLAN permet au sein d'un réseau physique commun (LAN), sur lequel sont connectés des équipements (serveurs), de les isoler les uns des autres de manière logique. Quant à un switch ou commutateur, c'est un équipement disposant de plusieurs ports permettant l'échange de données de plusieurs équipements informatiques au sein d'un réseau local.

Tout équipement situé dans un même LAN ou VLAN peut communiquer entre eux. L'avantage d'utilisé des VLANs permet d'éviter les problèmes physiques.

Ce taggage ou marquage d'une interface va être effectué à la suite de la demande de différents pôles pour qu'une machine située sur une interface d'un commutateur puisse accéder à un réseau spécifique comme un réseau de sauvegardes.

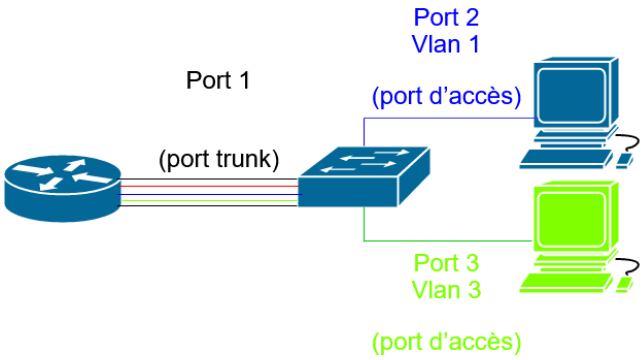

Fig. de la configuration habituelle d'un vlan

Dans la mise en place de vlan, on compte deux types de ports :

- Les ports dit d'Accès sont généralement les interfaces utilisées pour l'accès à un périphérique final.
- Les ports trunk sont des ports utilisés pour l'interconnexion avec d'autres commutateurs ou routeurs permettant le transport de différents VLAN au sein d'un même lien évitant ainsi la multiplication de lien pour les échanges avec les autres équipements. Ce type de lien dispense de la restriction géographique en offrant la possibilité de l'échange entre différents périphériques situés sur le même VLAN, mais pas sur le même commutateur.

2.2 Les actions au sein du Datacenter

2.2.1 Problème de SFP

Sur le centre de donnée d'Aix, il y a eu d'importants problèmes de débit et d'erreur sur différentes interfaces de périphéries réseau. La première hypothèse était celle de problème au niveau des SFP (Small form-factor pluggable). Un SFP est un connecteur qu'on branche à un périphérique réseau et sur lequel on relie un câble qu'on appelle une jarretière et qui est composée de deux fibres optiques protégées par une gaine et équipées à chaque extrémité d'un connecteur optique.

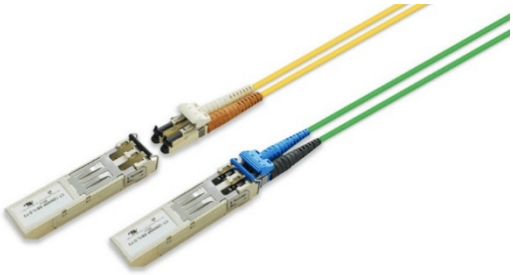

Fig. de deux SFP relié à des jarretières de fibre

Pour pouvoir confirmer cette hypothèse, Différents membres de l'équipe ont mis en place un protocole pour isoler la cause du problème. Les différentes causes du problème pouvant être :

- Un dysfonctionnement au niveau du port
- Un problème de SFP
- Problème du côté de la jarretière de fibre

Le protocole suivant a donc été mise en place :

- Arrêt (shut) du port problématique.
- Débranchement de la fibre et du SFP.
- Allumage (ou no shut) du port sans fibre branchée.
- Observation des niveaux "à vide" (sans fibre branchée) pour regarder la montée d'erreur et donc déduire si c'est un problème de port.
- S'il n'y a aucune erreur constatée, le port est éteint et la vérification passe coté SFP en rebranchant celui-ci.
- Le port est allumé avec aucune fibre raccordée au SFP.
- Une observation des niveaux "à vide" y est effectuée (sans fibre branchée) pour constater la montée d'erreur ou non et alors prouver si c'est le SFP, le coupable.
- Puis la vérification est effectuée côté fibre en éteignant celle-ci et en raccordant la jarretière de fibre au SFP.
- Un « no shut » est réalisé sur le port.
- Une observation et analyse sont effectuées des 2 côtés.
- Si on constate toujours des erreurs ou alarmes, on va effectuer la série d'opérations sur l'équipement qui est censé communiquer sur ce port.

Les remontées d'erreurs ont été constatées lors de la remise en place des SFP permettant de confirmer la première hypothèse qui était un problème dues aux SFP.

2.2.2 La mise en place de nouveaux éléments

L'une de mes premières actions a été de participer à la mise en place d'équipements dans une baie dans le Datacenter d'Aix. Une baie est une armoire permettant de stocker des équipements informatiques à l'aide de rails permettant d'y fixer les équipements. Cela permet d'optimiser l'encombrement, le câblage et de mutualiser l'alimentation et le refroidissement de ceux-ci.

La première action est de les racker, c'est-à-dire à les mettre sur les rails de la baie. Ensuite, la préparation de la future configuration des équipements en les raccordant avec les futurs équipements avec lesquels ils communiqueront.

Pour le raccordement, nous devions alors relier nos équipements à un châssis LEVITON.
LEVITON est un fabriquant d'infrastructures de câblage qui propose des châssis fibre. Dans notre cas, ces équipements permettent de relier les différentes baies entre elles.

Fig. D'un LEVITON

Le LEVITON est divisé en plusieurs emplacements où chaque emplacement dans notre LEVITON va correspondre à un emplacement d'un LEVITON d'une autre baie. Donc, il faut repérer précisément les différentes fibres pour savoir sur qu'elle interface où elles seront reliées. C'est pourquoi l'équipe commande des fibres pré-numérotées permettant de placer et repérer plus efficacement celles-ci.

La dernière étape consiste à configurer une adresse sur notre interface de management afin que les équipements soient accessibles à distance et ainsi finir leurs configurations à distance.

2.2.3 Mise en place d'une fabric Juniper

Lors d'une autre intervention Datacenter, j'ai dû participer à la mise en place une fabric Juniper.

La fabric Juniper ou VCF (virtual chassis Fabric) est un ensemble logique composé de plusieurs équipements réseau. Celle-ci s'appuie sur l'encapsulation des trames Ethernet (qui est une norme définissant la communication à l'intérieur d'un même réseau) dans des paquets IP (ensemble de données pouvant être routé pouvant envoyer vers d'autres réseaux). Cette méthode s'appelle le E-VPN (Ethernet VPN) et l'encapsulation des trames Ethernet dans un Paquet UDP permet de passer la limitation des 4094 VLAN passant à passant à 16 millions. UDP est un protocole permettant l'échange de donnée sans connexion.

Le fonctionnement de la fabric se base sur deux rôles :
• Les SPINES dont le rôle est le routage des informations.
• Les LEAFS qui vont transmettre les informations vers les différents équipements connectés (serveurs…).

La mise en place se fait assez simplement, il faut raccorder chaque LEAF sur les différents SPINES présents dans la fabrique et rajouter une configuration simple sur le LEAF que l'on souhaite rajouter.

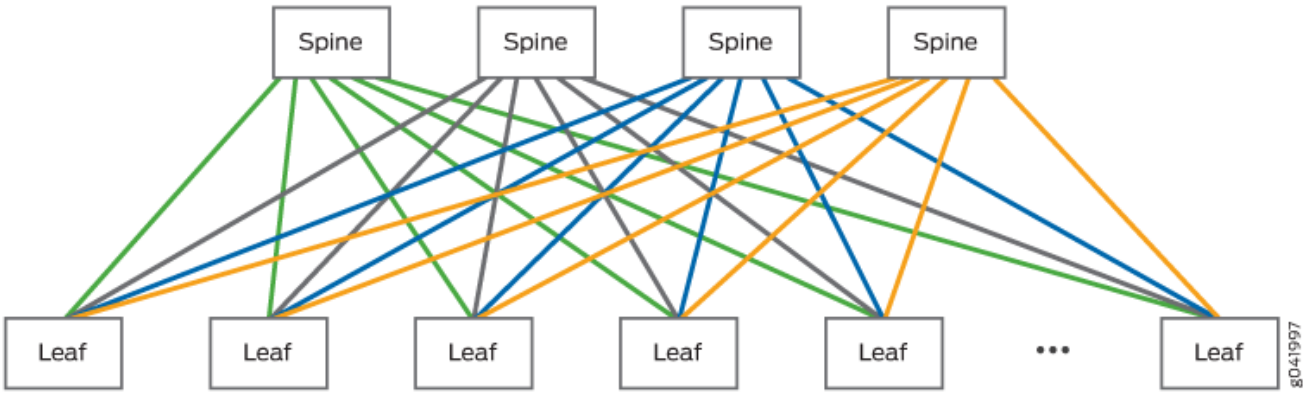

Fig. de présentation de leaf et spine.

De surcroit, la fabrique s'appuie sur l'utilisation de l'E-VPN. Et sur le protocole de routage BGP est un protocole d'échange d'informations entre différents système autonome dit AS qui sont composé de routeurs internes disposant d'une politique commune. L'utilisation de BGP et de son extension l'I-BGP qui permet les échanges d'informations entre les routeurs (peers) d'un même AS.

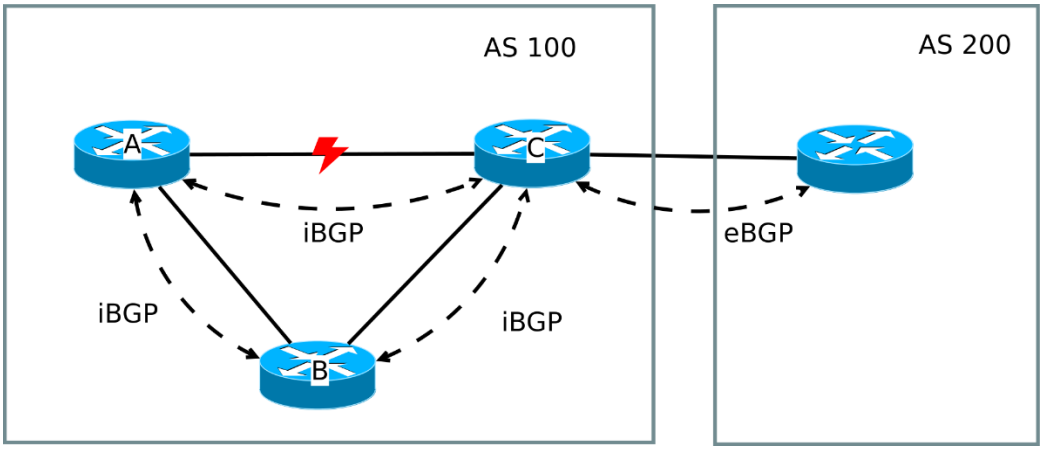

Fig. de liaisons I-BGP et E-BGP

En prenant l'exemple du schéma ci-dessus, le fait d'utiliser le protocole BGP et plus particulièrement son extension l'I-BGP est si la liaison entre le routeur A et C est coupé, la communication ne le sera pas, car il passera alors par B. D'autre part, l'EVPN va nous permettre de partager les adresses MAC (adresse qui sont exploité lors d'échanges de trames) et IP des différentes périphéries raccordé à nos différents routeurs.

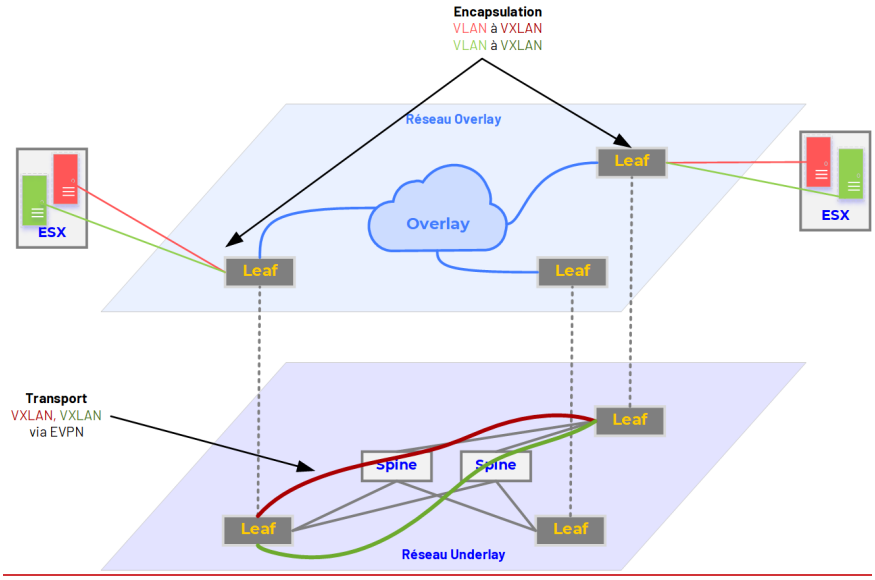

Fig. Représentation Simplifiée des strates Underlay et Overlay, exemple d'encapsulation VLAN → VXLAN.

3 La préparation d'un site

L'équipe réseau administre aussi les sites de l'entreprise DOCAPOSTE et leurs liaisons. Ils doivent lors du déménagement ou de l'installation de nouveaux sites y aller pour mettre en place le réseau et le relier aux autres sites. Pour des raisons d'efficacité et gain de temps lors de leurs installations sur site, le matériel réseau est configuré avant leurs mises en place sur sites.

Lors de mon arrivée au sein de DOCAPOSTE, l'équipe avait à configurer des firewalls et commutateurs pour un nouveau site situé à Villeneuve-d'Ascq et m'ont laissé faire leurs configurations.

3.1 Le site de Villeneuve-d'Ascq

Le site de Villeneuve-d'Ascq est un nouveau site résultant du déménagement du site de Marcq-en-Barœul vers un site plus grand. Ce site dépend de DOCAPOSTE BPO qui assure entre-autres, les prestations de numérisation et d'archivage de DOCAPOSTE.

3.2 Les équipements choisis et leur configurations

La présentation des équipements et de leurs configurations va suivre le modèle OSI qui est une structure en sept couches organisant les activités réseau. Les sept couches sont organisées de la façon suivante :

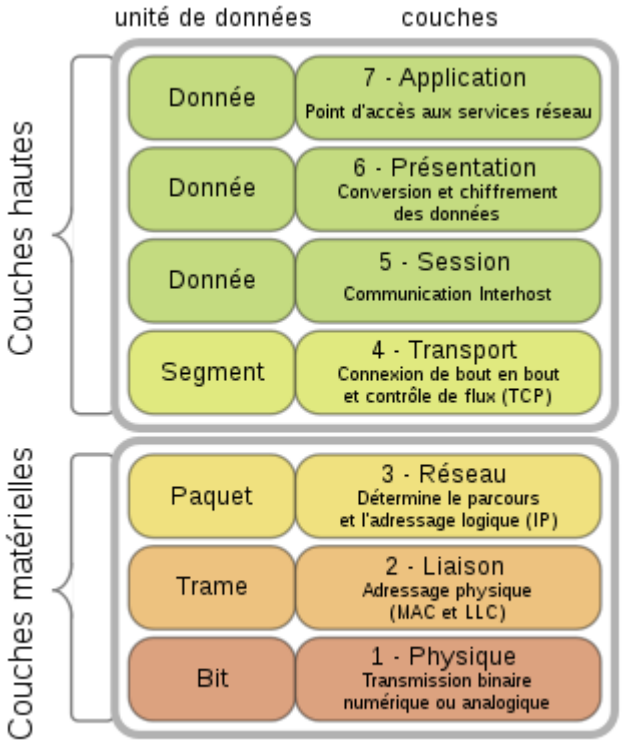

Fig. représentant le modèle OSI et l'application sur chaque couche.

3.2.1 La couches 1 et 2

Les couches 1 et 2 du modèle OSI vont correspondre à la partie commutations et câblage de notre plan. Pour la partie commutation, l'équipe va s'appuyer sur l'utilisation des commutateurs suivants, 2 Cisco Nexus 5548UP et de 14 Cisco Nexus 2248TP que l'on va nommer respectivement N5K et N2K dans la suite de la présentation.

De plus, la partie commutation va être organisée comme ci-dessous :

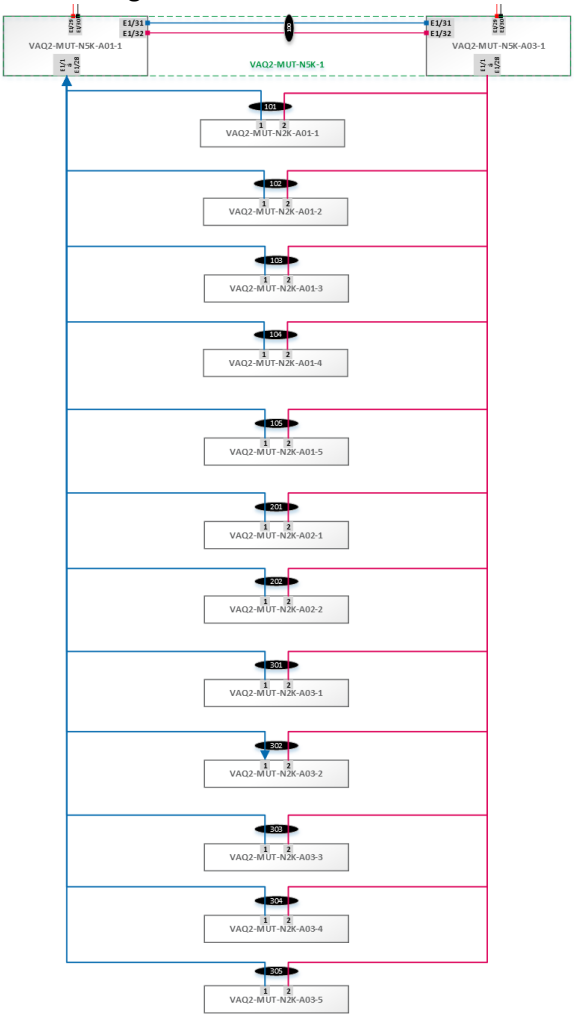

Fig. de la partie commutation.

Sur le schéma ci-dessus, nos 14 N2K vont être rattachés sur les 2 N5K pour s'assurer d'une disponibilité et d'une résilience maximale en cas de panne d'un composant.
C'est ce que l'on appelle la redondance. La redondance est le fait de prévoir de multiples ressources pour un même rôle. Cela permet d'augmenter sa fiabilité, notamment en cas de panne.

Notre couche de distribution s'appuie sur la philosophie d'une fabric Cisco. Elle s'appuie sur l'utilisation de différentes solutions afin de rendre un Datacenter/centre plus modulables et convergent. L'utilisation des Commutateurs Nexus 5K et 2K va nous permettre de mettre en place à cette idée.

Les N2K sont ce que l'on appelle des FEX pour Fabric EXtender. Les FEX sont des compagnons des commutateurs N5K. Lorsqu'ils y sont connectés, les FEX deviennent ainsi une partie logique des commutateurs parents.

Un Cisco FEX n'a pas d'intelligence, il n'exécute/gère rien et s'appuie sur ses parents, ici des N5K. Comme son nom l'indique, Cisco FEX « étend » la structure vers les périphériques qui nécessitent une connectivité réseau.

L'avantage d'utiliser des FEX est la simplicité de configuration. En effet, le FEX va être relié au N5k qui va lui injecter la configuration (versions…) et le considère comme un Linecard, une extension de son châssis.

Afin que les N2K puissent communiquer avec les deux N5k simultanément, il faut utiliser des VPC (Virtual port Channel).

Un VPC est un lien logique composé de deux liens physiques raccordant nos deux commutateurs N5K à un troisième périphérique, un N2K qui lui va considérer qu'il communique à un seul équipement. La notion de VPC s'appuie sur celle de port channel qui est une agrégation (réunion) de liaison au sein d'une interface logique basée sur le protocole LACP (IEEE 802.3ad).

Ces notions vont aussi permettre d'améliorer la bande passante puisque la bande passante de l'interface logique va correspondre à l'addition de la bande des différentes interfaces présentes dans ce lien. Par ailleurs, l'utilisation d'agrégation de lien permet aussi de se protéger d'une panne de l'une des interfaces, car le lien sera composé des autres interfaces.

3.2.2 La couches 3

La couche 3 du modèle OSI va correspondre à la partie Réseau. C'est ici qu'on va mettre en place le routage, l'adressage IP de nos VLANs et la connexion avec nos différents sites.

3.2.2.1 Le mise sous grappes des srx 340

Pour la partie routage vont être utilisés 2 firewalls Juniper SRX340 qui vont être groupés au sein d'une même entité logique pour être configuré comme un seul équipement, on appelle cela un cluster ou grappe.

L'avantage de la structure en cluster avec les 2 SRX340, c'est que l'un des équipements va être celui qui gère l'entité logique (le nœud primaire) et le second quant à lui est en assistance (nœud secondaire) et prendre la main si le nœud primaire ne répond pas. Cela va permettre d'améliorer la disponibilité des 2 équipements et la redondance de ceux-ci.

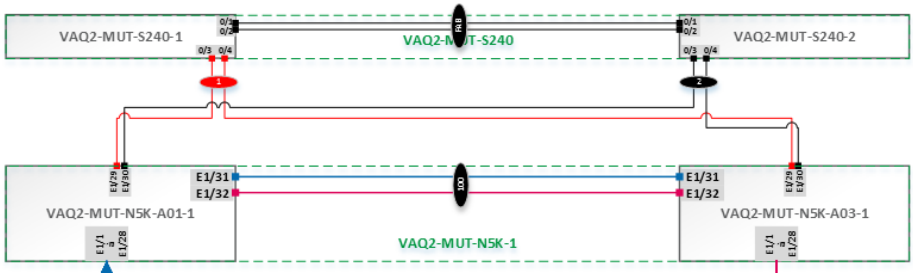

Fig. de la partie routage.

Ci-dessus, on peut voir que chacun des nœuds du cluster dispose d'une liaison vers les nexus 5K relié avec les SRX en liaison VPC présenté dans un point précédent. Cette disposition nous assure une protection contre l'indisponibilité d'un des deux nœuds.

Ces deux liens vont utiliser une solution Juniper, la redundant Ethernet (Ethernet redondant) qui va créer une interface logique qui comprend des interfaces physiques de chaque nœud d'un cluster.

Par ailleurs, notre routeur va effectuer à l'aide de ces liaisons le routage inter-vlan, car du coté N5K, les interfaces vont être configurées en mode Trunk.

3.2.2.2 La liaison inter-sites

Sur interconnecter les différents sites, DOCAPOSTE s'appuie sur la solution opérateur VPLS. Ce protocole permet d'interconnecter les LAN (Niveau 2) de différents sites entre eux. Celui-ci est construit sous la forme de liaisons point à multipoints : les sites peuvent se parler les uns aux autres sans que les flux ne transitent par les portes de collectes situées en Datacenter.

L'interconnexion des sites VPLS de DOCAPOSTE va s'appuyer sur l'utilisation de deux liaisons fournies par deux opérateurs différents pour chaque site afin de disposer d'une redondance lors de la panne de l'une des deux liaisons.

Ainsi, comme pour une fabric de Datacenter, l'interconnexion des sites utilise un réseau I-BGP pour établir des communications entre les différents équipements de routage, et donc les différents sites.

L'infrastructure VPLS va s'appuyer sur le même principe puisque la création d'un premier réseau est nécessaire afin d'établir la communication inter-sites, c'est que l'on appelle le réseau Underlay puis d'un second réseau s'appuyant sur l'Underlay afin d'échanger les différentes informations, cette couche d'échange se nomme l'Overlay.

Pour l'underlay, l'utilisation d'une interface avec une adresse qu'on va ensuite chercher à diffuser à tous les voisins. Pour cette diffusion, le protocole de routage OSPF (Open Short Path First) va être utilisé afin d'échanger sur chaque segment VPLS connu par le site.

Les routeurs exécutant le protocole de routage OSPF doivent établir des relations de voisinage (neighbor adjacency) avant d'échanger des routes. Comme OSPF est un protocole de routage d'état de liaison (Link State), les voisins n'échangent pas de tables de routage.

Grâce à cela, ils échangent des informations sur la topologie du réseau. Chaque routeur OSPF exécute ensuite l'algorithme SPF (Shortest Path First – Chemin le plus court) pour calculer les meilleures routes et les ajoute à la table de routage. Étant donné que chaque routeur connaît la topologie complète d'un réseau, la probabilité d'une boucle de routage est minime.

Après avoir réalisé l'échange des adresses de bouclage à l'aide d'OSPF, nous allons interconnecter nos sites (réseau overlay) à l'aide du protocole de routage BGP et plus particulièrement de l'I-BGP qui a été décrit dans un point précédent.

L'utilisation de BGP et D'I-BGP en tant que telle serait inexploitable puisque pour permettre l'échange de route à l'intérieur d'un système autonome, il faut disposer d'un maillage complet, c'est-à-dire que chacun des routeurs doit relier à tous les autres et ainsi modifié l'ensemble des liaisons lors de la mise en place d'un nouveau site. Ce qui rendrait l'utilisation de BGP inexploitable pour la connexion de plusieurs dizaines de sites entre eux.

C'est pour cela, il nécessaires d'utiliser des Route Reflector. Un Route Reflector est un routeur qui est relié à tous les routeurs internes à notre A.S et qui va redistribuer toutes les routes aux différents peers. Voici la différence de maillage sans et avec l'utilisation d'un Route Reflector :

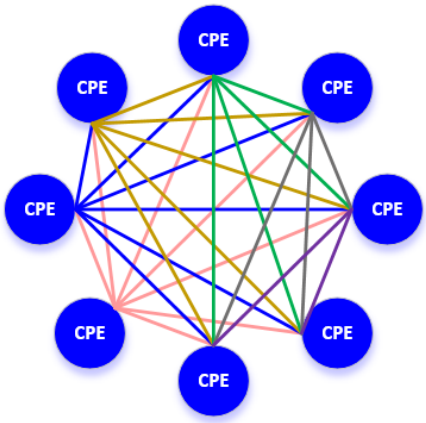

Fig. représentant le maillage BGP sans l'utilisation d'un R.R

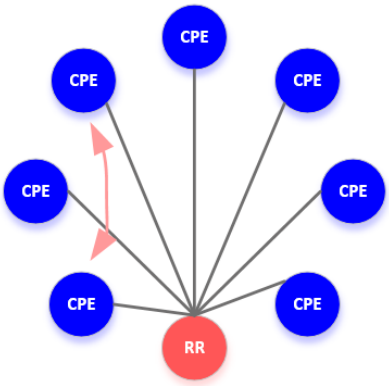

Fig. représentant le maillage BGP avec l'utilisation d'un R.R

3.2.2.3 La configuration partie firewaling

Les SRX 340 sont des firewalls donc par défaut ils n'autorisent pas d'échange avec l'extérieur. Ainsi, il est nécessaire de configurer les différents échanges d'information avec l'extérieur à l'aide de listes d'accès (ACL).

Nous devons alors configurer plusieurs listes d'accès basique pour permettre les échanges de flux entre les différents sites puisque par défaut l'échange entre différentes zones est interdit. Les règles de sécurité plus complexes notamment pour l'accès à Internet seront réalisées avec des équipements spécifiques au sein des différents centres de données de DOCAPOSTE.
Ces différentes listes d'accès simples sont notamment :

- La permission d'échange de flux OSPF permettant ainsi l'échange d'informations OSPF avec les autres routeurs permettant la mise en place du réseau Underlay.
- La permission d'échange de flux BGP permettant ainsi l'échange d'informations BGP avec les autres routeurs permettant la mise en place du réseau Overlay.
- La permission d'échange de flux de site qui va autoriser l'envoi de tous les flux d'un site vers sa destination.
- L'échange entre les différents vlans devra être aussi autorisé.

3.2.3 La configuration de la partie management

Autres points importants ne figurant pas directement dans le modèle OSI, c'est la configuration de la partie management qui constitue un point d'orgue dans la configuration des équipements réseau. Cette partie porte sur 5 points et requiert un maximum d'attention pour sa mise en place :

- La configuration des OOB
- La mise en place sur la plateforme SNMP
- La configuration radius
- Mise en place du syslog
- Mise à jour des équipements à leur version recommandé

3.2.3.1 Configuration de l'OOB

L'OOB (out of band) est l'utilisation d'un réseau exclusivement réservé pour le management des équipements. L'utilisation d'un OOB permet une meilleure disponibilité des équipements en cas de panne du réseau principal et permet aussi une meilleure sécurité.

Sur les nexus 5K et SR340 destinées à Villeneuve-D'ascq. Le raccordement à l'OOB de DOCAPOSTE va s'appuyer sur l'utilisation des interfaces de Management des équipements.

Pour la configuration OOB cotée n5K, il est essentiel de mettre en place une route par défaut sur la VRF de management dont dépend l'interface de management, c'est dire que tous les paquets IP seront envoyés vers une destination précise.
Coté de la grappe de SRX340, l'utilisation de l'interface logique de management FPX localisé sur la première interface de chaque SRX et d'une route par défaut va nous permettre son management. Les flux utilisateur et production passeront par une VRF dédiée.

Un VRF (Virtual routing and forwarding) est une technologie qui permet de segmenter un routeur physique en plusieurs routeurs virtuels. Le VRF permet une segmentation des routeurs au niveau 3, un peu comme les VLANs permettent une segmentation des commutateurs au niveau 2.

3.2.3.2 Configuration sur la plateforme SNMP

SNMP est l'abréviation de Simple Network Management Protocol, en français « protocole simple de gestion de réseau » qui est un protocole de communications permettant l'administration et la supervision des équipements réseau.

Au sein de l'entreprise DOCAPOSTE, il y est utilisé différentes plateformes. La première, Librenms est une plateforme gérée par l'équipe réseau pour surveiller les différents équipements réseau. Puis, une seconde destinée quant à elle pour l'alerting qui est le fait d'envoyer des alarmes lors de problèmes, est quant à elle gérer par une équipe de l'entreprise avec l'outil de supervision Zabbix.

Par ailleurs, les traps snmp sont aussi configurés pour être envoyés vers un serveur spécifique. Les traps snmp sont l'envoie par un périphérique réseau d'une alerte lors d'une action spécifique (port éteint...).

3.2.3.3 Configuration du client radius

Radius est un protocole normalisant les communications serveur-clients pour la mise en place d'une gestion d'authentifications unifié. Sur chacun des équipements sous la gestion de l'équipe réseau, un client radius est configuré.

Lorsqu'un utilisateur va essayer de se connecter sur un équipement, celui-ci va alors envoyer une requête avec les informations d'authentifications, c'est-à-dire le login et le mot de passe. Puis, le serveur radius va alors vérifier dans la base de données, si les authentifications sont valides. Ainsi, le serveur va envoyer une requête confirmant son existence permettant à l'utilisateur de s'y connecter. Sinon, le serveur envoie une requête demandant à l'utilisateur de retaper ses identifiants d'authentifications et les précédentes étapes seront répétées.

La configuration du client radius est divisée en deux étapes :

- La configuration coté client où il faut indiquer l'adresse du serveur et la clé d'authentification pour pouvoir s'y connecter.
- La configuration coté serveur, là il faudrait mettre en place l'équipement dans une base de données avec des informations comme l'adresse du serveur, la clé d'authentification (mot de passe chiffré) de celui-ci.

3.2.3.4 Mise en place d'un client syslog

Le syslog est l'envoie d'un journal normalisé à partir d'un client, ici d'équipements réseau, vers un serveur qui va les stocker permettant d'avoir ainsi une traçabilité des différentes actions/problèmes sur les équipements.

La configuration coté SRX et n5K va s'effectué d'une façon similaire et va consister à indiquer le serveur syslog de destinations avec un niveau de priorité à choisir. Ici, on va choisir le niveau correspondant au débogage permettant en cas de problème sur les équipements pourvoir retrouver la source du problème plus facilement car toutes actions ou modifications seront indiqués dans le log.

Puis du coté serveur, il est alors nécessaire de rajouter dans un fichier où les informations comme l'adresse IP, le nom d'hôte ou le port permettant au serveur de récupérer les logs des différentes machines et de les envoyer dans les endroits spécifiques selon les hôtes.

3.3 Préparation et envoi du matériel vers le site

On m'a délégué la mise sous cartons des différents équipements et éléments telle que des jarretières de fibre, SFP ou des câbles rj45. Pour cela, j'ai dû vérifier le poids des nexus 5K et 2K pour savoir comment les disposer pour que cela puisse correspondre aux conditions posées par le groupe de transport T.N.T. La dernière étape a consisté à téléphoner à T.N.T pour organiser l'envoi des cartons (22 cartons) vers le site de destinations en donnant les différentes informations nécessaires à l'envoi.

4 Le nommage des équipements

Le nommage d'un équipement est critique pour l'administré puisque c'est avec son nom que l'on va pouvoir savoir son rôle et sa position au sein de l'infrastructure. Cela permet aussi une automatisation simple à l'aide de script.

4.1 La situation actuelle

Les différents équipements disposent d'un nommage dépendant de leur ancienneté. En effet, l'entreprise dispose de deux normes de nommage, l'historique et la nouvelle.

4.1.1 L'ancienne norme de nommages

La première plus ancienne était organisée en trois parties séparées par des tirets. La première partie était composée du rôle de l'équipement dans la topologique du réseau. Il y avait 5 rôles possibles :

- SW pour switch (commutateur) représentant les équipements de la couche 2 de notre réseau.
- FW pour firewall (pare-feu) est qui était attribué principalement au firewall des différents sites de l'entreprise et ceux permettant l'accès vers l'extérieur.
- RT étant l'abréviation de routeur, attribué plus particulièrement au routeur de l'entreprise.
- Lb pour load-balancer dont leur rôle est de répartir les paquets reçus par des clients extérieurs sur un ou plusieurs serveurs qui exécutent la même tâche. On parle de reverse proxy lorsque la connexion s'effectue à partir de l'extérieur du réseau à destination de l'intérieur du réseau.
- CTX pour contexte firewall qui est le firewall le plus présent au sein de DOCAPOSTE. C'est un firewall multi-contextes qui offre la possibilité de virtualiser plusieurs firewalls dans un seul équipement.

La seconde partie correspond à l'abréviation du nom du site ou du Datacenter. Par exemple, pour le nouveau site de Villeneuve-D'Ascq, nous aurons l'abréviation VAQ.

Enfin, la dernière partie est quant à elle un commentaire libre ou le numéro du modèle, s'il était plusieurs au sein d'un même site ou la position d'une baie.

Par exemple pour un srx 340 du site de Villeneuve-D'Ascq, on aurait l'exemple suivant :
Fw-vaq-n1

La croissance et la diversification de l'entreprise dans différents domaines telle que la santé et le cloud à compliqué le repérage et rôles des différents équipements réseau au sein de l'infrastructure. C'est pourquoi il a été nécessaire que les équipements soient renommés pour permettre un meilleur repérage.

4.1.2 La nouvelle norme de nommage

Les architectes réseau ont mis en place une nouvelle norme de nommage pour correspondre au mieux à l'échelle de l'entreprise DOCAPOSTE. La nouvelle norme dispose de généralement 4 champs séparés par des tirets.

Le premier correspond à l'identifiant du site.

Le second représente l'offre d'hébergements, le rôle des équipements à l'intérieur de l'infrastructure. On en compte 15 mais il y en a 5 principales :

- MUT pour la mutualisation de plusieurs offres d'hébergement.
- DIR pour les sites Bureautique.
- SEN concerne l'hébergement des données sensibles comme les données personnelles d'utilisateurs.
- HDS (hébergeurs de données de santé) étant l'hébergement des données médicales requérant des mesures spécifiques.
- CLD correspond à la partie cloud de DOCAPOSTE.
- Standard ou STD correspond à un hébergement ne requérant aucune attention particulière.

La troisième va représenter le type d'équipement. Il indique par défaut le type d'équipements physique (Cisco Nexus 5K ou SRX 340). Dans le cas où l'équipement serait logique, on le remplace par le type d'équipements logique comme VCF.

Enfin, le dernier point est la description. Il permet d'identifier de façon unique l'équipement lorsque les champs précédents sont identiques. La description peut être composée de deux façons. Ses deux façons vont dépendre de si l'équipement est en Datacenter ou non.

Si l'équipement est dans un Datacenter, il aura alors 3 champs :

- Le fonctionnement de l'équipement au sein du dc, il y a 6 choix possibles :
    - Les leafs
    - Spine
    - RP (reverse proxy)
    - LB (load balancer)
    - ADC pour application delivery controller qui est la solution constructeur F5 permettant de faire tourner différents services simultanément telle que le VPN-SN, RP…
    - OOB
- Le nom de la baie dans laquelle, il est situé.
- Enfin, un numéro pour pouvoir différencier les équipements qui est par défaut à 1.

Si l'équipement n'est pas en Datacenter, il lui disposera alors d'un espace de commentaire servant à lui attribuer généralement un numéro servant pour la différentiation.

4.2 La situation lors du stage

4.2.1 L'uniformisation du nommage des équipements réseau

La première action a été de récupérer les différents équipements réseaux au sein de la plateforme de supervision réseau LibrenMS et de l'ancienne plateforme de l'équipe Cacti. Pour cela, un membre de l'équipe a utilisé un script permettant de récupérer la liste des équipements à travers l'API des deux Plateformes. Une API (Application Programming Interface) que l'on peut traduire par interface de programmation d'application permettant à travers un langage de programmation d'accéder et modifier les paramètres d'une application.

Une fois les équipements dans un fichier de type Excel, la première passe consiste à la normalisation de tous les équipements et la mise à l'écart des différents équipements qui nécessiter des passes avec différent membres de l'équipe.

Les différents problèmes étant :
• Le manque d'informations concernant notamment la localisation ou le rôle de certains équipements dans les Datacenters.
• Le manque de rôle ou précision pour certains équipements comme notamment les F5 Big IP qui portent les fonctions de gestion de domaines, de VPN et de reverse Proxy sur des VM (machines Virtuelle) tournant sur des socles (un firewall F5) à l'aide de VCMP (Virtual Clustered Multiprocessing) qui est une plateforme permettant de créer et d'utiliser des VM à partir d'un firewall F5. Il s'est révélé nécessaire d'indiquer quels équipements sont des socles et lesquelles sont les VM.
• L'offre d'hébergements qu'il doit être utiliser sur les équipements des différents sites de DOCAPOSTE. Actuellement, il existe deux types d'offres valable DIR et MUT. Généralement, il y a différents types de flux transitant sur les différents sites comme les flux d'utilisateurs ou ceux pour la partie éditique notamment, donc la question de la pertinence de l'offre DIR a été poser.

4.2.2 Le deuxième passage sur les équipements

Une réunion a été effectué avec les différents acteurs des pole architecture et de l'administration réseau responsables de cette nouvelle norme de nommage pour présenter l'avancement concernant le nommage des équipements et les différents problématiques apparus lors de la première passe.

A la fin de la réunion, il est apparu l'utilité sur certains équipements logiques de mettre en avant le modèle des équipements notamment pour les VC (Virtuel Chassis) qui est une solution de Juniper pour la mise en grappe de switches. Un VC est mise en place qu'avec un type de modèle spécifique d'où l'utilité de mettre en avant le modèle.

De plus, l'utilisation de l'offre d'hébergement mutualisé pour les sites a été confirmer et la position manquante pour certains équipements en datacenter a été donner me permettant une seconde passe pour vérifier, corriger et terminer les modifications sur les équipements.

4.2.3 Finalisation du renommage des équipements

Après avoir terminé un deuxième passage sur le document, j'ai dû voir avec un membre de l'équipe admin réseau pour présenter le document le nommage final des équipements et le vérifier. Par ailleurs, on a constaté le manquement de certains équipement critique comme ceux servant à l'OOB dans un datacenter sud et un nord.

Il m'a donc donné une autre liste d'appareil où j'ai effectué une comparaison avec le fichier final pour récupérer les équipements manquants. Après, les avoir récupérés j'ai vérifié leur présence au sein de librenms puis indiquer s'ils étaient présents ou non.

Les principaux équipements manquants étaient :

- Des context firewall servant pour le contrôle et l'isolation des réseaux des différents clients de DOCAPOSTE.
- Des appareils servant pour l'oob des différents datacenters.
- Certains équipements réseau de site.

A la suite de cette dernière action, j'ai revérifié la liste avec les derniers éléments ajouté pour vérifier que tout est bien renommé et je réalise un dernier passe avec le membre de l'équipe responsable du renommage pour confirmer que tous les équipements respectent la nouvelle convention de nommage.

Conclusion

Durant le stage, j'ai pu acquérir de nouvelles compétences dans le domaine de l'administration et mise en place d'un réseau. A travers les différents projets que j'ai pu mener, j'ai su mettre en œuvre ce que j'ai appris durant ma formation notamment sur la partie configuration du matériel réseau.

Les premiers jours furent assez complexes, le temps de trouver mes marques. Cependant mon intégration à l'équipe fut très rapide, notamment grâce à tous les membres de l'équipe réseau qui ont su m'apporter les connaissances dont j'avais besoin. Plus tard j'ai aussi visité les deux datacenters du sud (Celui de Marseille et Marseille), les cœurs du réseau d'information de l'entreprise.

Enfin, cela m'a permis de voir les différentes missions effectuées par des administrateurs au sein d'une moyenne-grande entreprise mais aussi de répondre à mon questionnement concernant mon parcours professionnel, car j'hésitais entre l'administration réseau et système.
De part, le retour d'expérience des différentes personnes au sein des pôles architectures, administration réseau et système, j'ai décidé de poursuivre mes études et d'acquérir des compétences professionnelles pour devenir à termes Ingénieur réseau avec des compétences dans Linux pour le déploiement de services, notamment.

Remerciements

Dans un premier temps, je tiens à remercier Bertrand Hernandez et Thomas DE SIANO de m'avoir accueilli en tant que stagiaire au sein de l'équipe réseau de DOCAPOSTE ainsi que de leur disponibilité.

Je tiens également à remercier toute l'équipe d'administration réseau pour leurs disponibilités et plus particulièrement :

Messieurs Cédric PESQUE, Toze DIAS, Naoufal EL NASRI pour m'avoir maintes fois aidé et assisté à configurer les équipements pour les sites ainsi qu'apporter leur expérience personnelle.

Messieurs Thomas JOVANOVIC et Adrien RICOURT pour m'avoir montré les différentes actions au sein des Datacenters ainsi que les réalisations quotidiennes de l'équipe réseau.

Monsieur Nicolas BELLINI pour m'avoir exposé l'urbanisation au sein d'un Datacenter et aidé lors de la convention de nommage et apporté différents conseils en programmation.

Monsieur Chafik KAHLAOUI pour la présentation de la sécurisation du réseau au sein de DOCAPOSTE.

Je souhaite par cette occasion remercier le corps enseignant de l'IUT pour m'avoir enseigné toutes les bases qui m'ont permis de réaliser ce stage dans de bonnes conditions.

Glossaire

ACL ou Liste d'accès de contrôle : Liste autorisant ou interdisant l'échange de certaines applications (Web…) à un périphérique de destination et/ou de source.

Adresse IP : Identifiant donné à un périphérique informatique qui est relié à un réseau.

BGP : BGP est un protocole d'échange d'informations entre différents système autonome dit AS qui sont composé de routeurs internes disposant d'une politique commune.

Cloud : Mise en accès de service à distance par un fournisseur pour un client.

Cluster ou Grappe : Regroupement de plusieurs équipements en un seul équipement logique afin de maximiser l'utilisation des équipements.

Commutation/commutateur : Appareil permettant de relier plusieurs périphéries réseau au sein d'un réseau local.

Couche underlay: Réseau servant pour établir une connexion permettant l'échange entre différents éléments sur laquelle une application ou autre couche va se baser.

Couche Overlay : Réseau construit sur un autre réseau, celui-ci ne connaîtra pas la construction du réseau sous-jacent.

Ctx: Firewall physique utilisé pour héberger différents firewalls (ou contexte) virtuels.

Datacenter : Lieu regroupant des périphéries informatiques chargées de stocker et d'échangé des données avec différents clients issues de réseau interne ou via internet.

DUT : Diplôme Universitaire de Technologie.

DSI : Direction des Systèmes d'Information.

l'E-VPN : Extension du protocole BGP permettant le partage des adresses MAC et IP des différentes périphéries raccordé à nos différents routeurs.

Fex: Fabric EXtender

Firewall ou pare-feu : Appareil permettant de faire appliquer une politique de sécurité au sein d'un réseau.

HDS : Hébergeur de donnée de santé est une certification nécessaire afin d'héberger des données de santé.

Linecard: Extension d'un châssis d'un périphérique réseau.

Modéle OSI : Norme définissant en 7 couches définissant la communication dans les réseaux informatiques.

OOB : Utilisation d'un réseau exclusivement réservé pour le management des équipements.

OSPF : OSPF est un protocole de routage d'état de liaison (Link State) qui échange des informations sur la topologie du réseau.

Paquets IP : Norme spécifiant l'échange à l'extérieur d'un réseau local.

Port Channel : Agrégation de plusieurs liaisons au sein d'une interface logique.

Protocole de routage : Protocole spécifiant l'échange d'information entre différents routeurs.

Radius : Protocole normalisant une communication serveur-clients pour la mise en place d'une gestion d'authentifications unifié.

Redondance : Duplication et maximisation des parties critiques de notre réseau pour augmenter la fiabilité de celui-ci.

Reth ou Redundant Ethernet : Solution Juniper regroupant plusieurs interfaces physiques de chaque nœud (équipement) d'un cluster au sein d'une interface logique.

Reverse Proxies : Appareil dont le rôle est de répartir la charge reçue par le réseau sur un ou plusieurs serveurs qui exécutent la même tâche.

Routage : Choix d'un chemin, le plus efficace possible pour parvenir à un destinataire.

Routage inter Vlan : Périphérie faisant l'échange des flux entre deux VLANs.

Route Reflector: Routeur relié à tous les routeurs internes à notre A.S et qui va redistribuer toutes les routes aux différents peers.

SNMP : Simple Network Management Protocol est un protocole de communication permettant l'administration et la supervision des équipements réseau.

SSL (Secure sockets layer) : Protocole permettant le chiffrement des données dans un échange WEB.

Syslog : Envoie d'un journal normalisé à partir d'un client vers un serveur qui va les stocker.

Trames Ethernet : Norme spécifiant l'échange d'information à l'intérieur d'un réseau.

Trunk: Interfaces servant pour transporté différents VLAN au sein d'un même lien.

TCP : Transmission Control Protocol est un protocole permettant l'échange de donnée de façon fiable de bout en bout.

UDP : User Datagram Protocol est un protocole permettant l'échange de donnée sans connexion.

VLAN ou Réseau local virtuelle : Réseau local logique permettant une isolation efficace des machines dans un réseau local spécifique.

VPC: Lien logique permettant aux liens qui sont physiquement connectés à deux commutateurs d'apparaître comme un seul Port Channel pour le troisième périphérique.

VPLS : Protocole permettant d'interconnecter les Lans (Niveau 2) de site entre eux.

VXLAN : Encapsulation des trames Ethernet dans des paquets IP.

Bibliographie

blackbox. (s.d.). *SFP, SFP+ et QSFP : Quelles sont les différences ?* Récupéré sur blackbox: https://www.blackbox.fr/fr-fr/page/45251/Information/Technique/black-box-explique/LAN/SFP-et-QSFP-Quelles-sont-les-differences

Chassis Cluster Redundant Ethernet Interfaces. (21, Mars 26). Récupéré sur Juniper: https://www.juniper.net/documentation/us/en/software/junos/chassis-cluster-security-devices/topics/topic-map/security-chassis-cluster-redundant-ethernet-interfaces.html

Cisco Adapter Fabric Extender. (2016, Janvier 11). Récupéré sur Ciso: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/data_sheet_c78-657397.html

Communauté. (s.d.). *Small form-factor pluggable* . Récupéré sur wikipedia: https://fr.wikipedia.org/wiki/Small_form-factor_pluggable

Configuring Chassis Clustering on SRX Series Devices. (21, Mars 26). Récupéré sur Juniper: https://www.juniper.net/documentation/us/en/software/junos/chassis-cluster-security-devices/topics/topic-map/security-chassis-cluster-verification.html

Devrim, B. (2012, Novembre 14). *What Is Cisco UNIFIED FABRIC? Why Should You Care?* Récupéré sur Cisco: https://blogs.cisco.com/datacenter/what-is-cisco-unified-fabric-why-should-you-even-care

Gandit, P. (2011, avril 18). *le FEX Nexus 2000 au coeur des architectures Data Center Business Advantage*. Récupéré sur Cisco France Blog: https://gblogs.cisco.com/fr/datacenter/le-fex-nexus-2000-au-coeur-des-architectures-data-center-business-advantage/

Sheldon. (2018, Juin 28). *Qu'est-ce qu'un module SFP et comment en choisir un ?* Récupéré sur FS Community: https://community.fs.com/fr/blog/sfp-module-what-is-it-and-how-to-choose-it.html

SRX Series Chassis Cluster Configuration Overview. (2021, Mars 26). Récupéré sur Juniper: https://www.juniper.net/documentation/us/en/software/junos/chassis-cluster-security-devices/topics/task/chassis-cluster-srx-series-creating.html

Understanding Virtual Chassis Fabric Components. (2021, Mars 26). Récupéré sur Juniper: https://www.juniper.net/documentation/us/en/software/junos/virtual-chassis-fabric/topics/concept/vcf-components.html

Understanding Virtual Chassis Fabric Configuration. (2021, Mars 26). Récupéré sur Juniper: Understanding Virtual Chassis Fabric Configuration

Virtual Chassis Fabric Overview. (2021, Mars 26). Récupéré sur Juniper: https://www.juniper.net/documentation/us/en/software/junos/virtual-chassis-fabric/topics/concept/vcf-overview.html

What Is a Network Fabric? (s.d.). Récupéré sur Cisco: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-a-network-fabric.html