le cnam Master Réseaux Informatiques d'Entreprise
RIE07 2012 – 2014

Grenoble INP FORMATION CONTINUE

Mémoire

présenté et soutenu le 4 juillet 2014 par
Cynthia Lopes do Sacramento

SDN et le passage au Cloud Computing

Un regard sur les aspects réseaux et les apports de SDN dans les data centres

---

Jury :	Romain Kobylanski
	François Miller
	Véronique Panne
Tuteur académique :	Jean-Luc Parouty
Tuteur :	Claude Casery
Entreprise :	Bull

Remerciements

Le présent document peut être considéré comme le résumé de mon cycle d'études « Master Réseaux Informatique d'Entreprise ».

Je tiens à remercier tous ceux qui, à l'Institut National Polytechnique de Grenoble et à l'entreprise Bull, m'ont accompagnée dans ce parcours.

À tous les intervenants pédagogiques de la formation RIE, j'adresse mes remerciements pour les connaissances transmises, spécialement à Messieurs Kobylanski et Parouty ainsi qu'à Madame Panne, pour leurs conseils et leur accompagnement.

J'exprime toute ma gratitude à mes collègues de Bull pour leur accueil et convivialité pendant ces deux ans d'alternance ; Spécialement aux membres de l'équipe OSI pour m'avoir intégrée, je témoigne sincèrement de ma reconnaissance : tout d'abord à Claude Casery, mon tuteur, pour son rôle clé dans mon développement professionnel, mais aussi à Julien et à Laure pour leur aide technique et leur disponibilité.

Merci également aux membres de l'équipe OMNIS, qui m'ont précédemment accueillie, pendant mon stage de licence, et qui sont devenus rapidement mes grands amis de France. Leur sagesse, encouragements (notamment de la part de Martine) et drôlerie m'ont beaucoup inspirée et ont contribué à l'aboutissement de cette expérience à l'étranger pour moi.

Dans l'équipe Storeway, je suis particulièrement reconnaissante envers Emmanuel de m'avoir initiée au sujet SDN, thème choisi pour ce mémoire, ainsi qu'à Renata, ma compatriote, pour sa compréhension et son aide pour l'équivalence d'un vocabulaire non évident.

J'exprime ma gratitude aussi à tous ceux qui ont relu mon document et m'ont permis de l'améliorer, mais particulièrement à Christine pour les corrections, patience et explications.

Enfin, je remercie ma famille et mes amis qui m'ont soutenue même de loin. Dans cette ouverture, un merci aussi à ceux pour lesquels j'ai cultivé une forte affection depuis mon arrivée. Tous ont contribué d'une manière ou de l'autre à la réussite de ce parcours.

Table des matières

Liste des tableaux

Table des figures

Introduction

Les centres de traitement de données évoluent aujourd'hui à un rythme intense pour accompagner l'explosion constatée dans l'utilisation de données. L'accélération de l'innovation dans l'informatique impose une rénovation constante des entreprises. La virtualisation a permis aux centres de données d'améliorer la productivité de ses serveurs, mais pour arriver à l'agilité souhaitée, les data centres doivent faire évoluer leurs réseaux pour pouvoir passer au Cloud Computing. Cette étude analyse les applications **Software-Defined Networking : Réseau Informatique Défini par Logiciel (SDN)** pour en distinguer les apports dans le contexte des data centres et habiliter le passage au Cloud Computing.

La plupart des infrastructures de **Technologie de l'Information (TI)** n'ont pas été construites pour supporter la croissance explosive de la capacité de traitement de l'information observée aujourd'hui. Plusieurs centres de données sont devenus hautement distribués et relativement fragmentés. Ils se trouvent donc limités dans leur capacité à évoluer rapidement et à supporter l'intégration des nouveaux types de technologies ou à se mettre à l'échelle selon les besoins de ses consommateurs.

Lorsqu'ils sont équipés d'infrastructures performantes, partagées et dynamiques ainsi qu'avec des outils nécessaires pour libérer les ressources de la demande traditionnelle, les **Système d'Information (SI)** peuvent alors répondre plus efficacement aux besoins métiers. Ainsi, les structures pourraient se focaliser sur l'innovation et ajuster les ressources à leurs priorités stratégiques. Cela soulagerait la prise de décisions, qui pourrait se concentrer sur l'information en temps-réel.

Alors que le coût du réseau dans un data centre est estimé à 15% [1] du total, sans être un des plus élevés, il est largement établi qu'il représente un élément clé pour la réduction des coûts et l'augmentation du retour sur investissement. Les coûts d'investissement dans les serveurs ont été évalués à 45% des coûts des data centres. Malheureusement la charge utile des serveurs est remarquablement basse, arrivant à seulement 10% d'utilisation dans

certains exemples.

La technique de la virtualisation a permis le déplacement des processus entre machines, mais des contraintes réseau continuent à limiter l'agilité dans les data centres. L'agilité est définie par la capacité d'affecter tout service n'importe où dans le data centre, tout en assurant la sécurité, la performance et l'isolation entre tous les services. Les designs des réseaux conventionnels dans un data centre empêchent cette agilité ; par nature ils fragmentent à la fois les réseaux et la capacité des serveurs, limitant et réduisant la croissance dynamique des pools de serveur. [2]

L'agilité est donc un élément clé ; certaines entreprises s'évertuent à déployer des nouvelles applications ou faire évoluer les existantes au rythme de la croissance de leur business. Selon le sondage mené par AlgoSec avec 240 professionnels de l'informatique, 25% des organisations participantes doivent attendre plus de 11 semaines pour qu'une nouvelle application soit mise en ligne (et dans 14%, ce temps dépasse 5 mois). Les résultats révèlent également que 59% des entreprises nécessitent plus de huit heures pour réaliser un changement de connectivité dans une application. [3]

Cependant, lors du passage au Cloud, les entreprises réalisent que la virtualisation des serveurs est considérablement limitée par les designs Ethernet classiques et les contrôles de sécurité réseau traditionnels. Avec l'augmentation de la virtualisation au sein des data centres, quatre tâches critiques deviennent contraignantes :

— Prévention de la congestion du trafic ;
— Réduction de la complexité des politiques réseau et maintien du niveau de service ;
— Élimination des points aveugles qui conduisent à des pannes ;
— Scellement des failles de sécurité pour protéger les données. [4]

Cette étude a pour but de démontrer comment SDN peut être appliqué aux data centres pour libérer le Cloud Computing et dépasser ses limites. Dans le premier chapitre, le contexte des data centres sera défini. Ensuite, les problématiques dans l'aspect réseau seront exposées. Enfin, le chapitre suivant présentera SDN et démontrera ses apports dans ce cadre.

Chapitre 1

Les évolutions du business modèle des Data Centres

Ce chapitre a pour but de définir un data centre d'en analyser les problématiques, enjeux et solutions possibles, en vue de comprendre sa situation actuelle et ses limites par rapport aux nouveaux besoins et défis business. Les éléments les plus importants de la conception et de l'architecture du data centre seront présentés ainsi que les difficultés qui ont amené faire à évoluer le mode de livraison vers une approche Cloud Computing.

1.1 Data centres et leurs objectifs

Un data centre (aussi nommé « ferme de serveurs ») est un répertoire centralisé pour le stockage, le management et la distribution de données et d'informations. Typiquement, un data centre est une installation utilisée pour loger des systèmes informatiques et ses composants associés, tels que systèmes de télécommunication et stockage.

Les data centres traditionnels hébergent historiquement de nombreuses applications relativement petites ou moyennes, chacune s'exécutant dans une infrastructure matérielle dédiée qui est isolée et protégée des autres systèmes dans la même installation. Ces data centres accueillent du matériel et du logiciel pour multiples unités organisationnelles ou même diverses entreprises. Différents systèmes informatiques au sein d'un tel data centre ont souvent très peu d'éléments en commun en termes de matériel, logiciel ou infrastructure de maintenance, et en général ne communiquent pas entre eux.

Les tendances de l'informatique vers une approche "serveur" et l'explosion en popularité des services sur internet ont changé ce scénario. Des infrastructures data centre entières ont été dédiées à un seul acteur pour faire fonctionner ses services offerts. Dans ce cadre, un data centre appartient à une seule organisation et utilise des matériels et plateformes logicielles relativement homogènes qui partagent une couche commune de systèmes de management. Ces data centres dédiés exécutent un nombre réduit d'applications (ou services internet) beaucoup plus importantes en taille ; l'infrastructure commune de management permet alors une meilleure flexibilité de déploiement.

Ces infrastructures sont montées pour gérer la taille des applications déployées et la haute disponibilité exigée pour ces services, visant en général 99,99% de durée de fonctionnement (une heure au maximum de temps d'arrêt par an). Il est difficile d'atteindre un fonctionnement libre des failles dans un regroupement de systèmes matériel et cela devient encore plus complexe avec le grand nombre de serveurs impliqués.

Les infrastructures de ces data centres doivent être dimensionnées précisément en fonction de la charge des applications supportées. Par conséquent, de nouvelles approches ont été proposées pour la construction et l'opération de ces systèmes qui doivent être conçus pour tolérer un nombre important de failles avec très peu ou aucun impact sur la performance et disponibilité des services offerts. [5] [6]

1.2 Organisation d'un data centre et difficultés

Un data centre est en général organisé en lignes de racks où chaque rack contient des dispositifs modulaires tels que serveurs, switches, briques de stockages ou instruments spécialisés. Des composants essentiels de l'infrastructure, branchés aux racks des data centres d'entreprises tels que compute, stockage et réseau, sont la base sur laquelle les applications business sont construites. Un châssis se présente avec ses propres ventilateurs, source d'alimentation, panier d'interconnexion et module de management. Pour réduire l'espace occupé, des serveurs peuvent être compartimentés dans un châssis qui est glissé dans le rack. Un châssis fournit des slots de taille standard où il est possible d'insérer des élément actifs modulaires (aussi connus en tant que « blades »). Un seul châssis peut contenir 16 serveurs 1 U ; étant donné que les racks supportent 6 châssis, ils ont une capacité théorique de 96 éléments modulaires.

La figure 1.1 montre l'organisation des racks dans un data centre. Un serveur occupant

FIGURE 1.1 – Organisation de racks. [6]

1 U du rack est visualisé à gauche. Au centre on peut voir un rack et à droite un cluster de racks avec un swtich/routeur de niveau cluster. En général un ensemble de serveurs 1U est monté dans un rack et inter-connecté à un commutateur Ethernet local. Ces switches au niveau des racks, qui peuvent utiliser des liens de 1 à 10 Gbps, ont un nombre de connexions montantes vers un ou plus switches de niveau cluster (data centre).

Le stockage dans les data centres peut être proposé de diverses manières. Souvent le stockage de haute performance est logé dans des « tours de stockage » qui permettent un accès distant transparent au stockage, indépendamment du nombre et des types des dispositifs de stockage physiques installés. Le stockage peut également être fourni dans une « brique de stockage » plus petite, localisée dans le rack ou slot de châssis ainsi que directement intégrée aux serveurs. Dans tous les cas, un accès réseau efficace au stockage est crucial.

Le problème le plus important dans cette structure est l'éventuelle insuffisance de bande passante. En général, les connexions montantes sont conçues pour supporter un certain taux de demandes excédentaires puisque la fourniture d'une bande passante entière n'est pas toujours possible. Par exemple, pour 20 serveurs à 1Gbps, chacun doit partager un lien Ethernet montant unique de 10Gps à un taux de demande excédentaire de 2. Cette situation peut être problématique si la charge réseau non locale monte considérablement. Comme le stockage est traditionnellement fourni dans une tour séparée, tout le trafic de stockage traverse le lien montant dans le réseau stockage. Par exemple, l'archivage d'un gros volume peut consommer une importante bande passante. À mesure que les data centres augmentent en taille, une architecture réseau plus extensible devient essentielle.

La consommation d'énergie est également une des préoccupations de la conception des data centres, car les coûts liés sont devenus une part importante de la totalité des coûts pour cette classe de systèmes. Actuellement les CPUs ne sont plus le seul élément cible d'amélioration de l'efficacité énergétique, car ils ne dominent plus la majorité de la consommation. Des problématiques de ventilation et surconsommation d'énergie sont des facteurs de plus en plus critiques dans la conception de data centres.[6] [7]

1.3 Virtualisation et partage de ressources

Le besoin d'augmenter l'efficacité dans l'utilisation des ressources a conduit à une conception d'infrastructures avec partage de ressources et virtualisation. La virtualisation fait référence à l'abstraction des ressources logiques de leurs couches physiques pour améliorer l'agilité, la flexibilité et la réduction des coûts et ainsi privilégier le business. La virtualisation permet de consolider un ensemble de composants d'infrastructures sous-utilisés en un nombre de dispositifs plus petits et mieux utilisés, contribuant à l'économie des coûts.

La virtualisation de serveurs est une méthode pour abstraire le système d'exploitation de la plateforme matérielle. Cela permet aux multiples systèmes d'exploitation ou multiples instances du même système d'exploitation de coexister dans un ou plusieurs processeurs. L'image 1.2 illustre le partage de ressources par l'intermédiaire de la virtualisation.

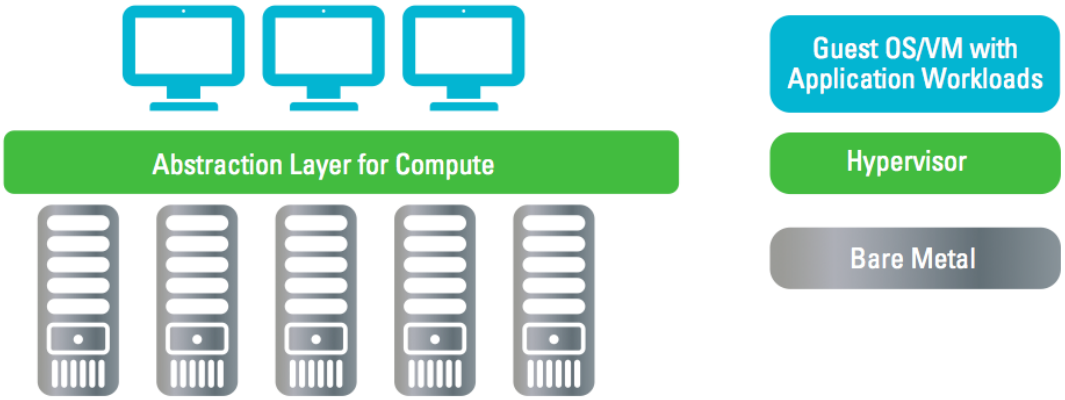

FIGURE 1.2 – Modèle d'infrastructure à ressources partagées. [8]

Un hyperviseur ou moniteur de machines virtuelles est inséré entre le système d'exploitation et le matériel pour réaliser la séparation entre le logique et le physique. Les instances de systèmes d'exploitation lancées sont appelées invités, ou systèmes d'exploitation invités. L'hyperviseur fournit l'émulation matérielle aux systèmes invités et gèrent l'allocation de ressources matérielles. Les principaux hyperviseurs disponibles sur le marché aujourd'hui sont : VMware ESXi, KVM basé sur Linux et supporté par Red Hat, Citrix XEN et Microsoft Hyper-V.

Ce modèle apporte des avantages pour l'efficacité dans l'utilisation de ressources avec des charges applicatives idéales. Cependant, quand une application commence à consommer plus de ressources que l'estimé, il peut arriver des scénarios où les systèmes d'exploitation invités n'ont pas assez de ressources, impactant ainsi la qualité du service business offert.

Cette approche a apporté une maitrise globale de management, monitoring et outillage. Elle a aussi mis en évidence que le composant « compute » de l'infrastructure améliore nettement l'utilisation et l'automatisation des ressources serveurs. Cette amélioration a été possible grâce à la programmation du contrôle de ressources fournies aux instances invitées. Toutefois, le développement de nouvelles solutions pour gérer la charge dynamique de certaines application faisait toujours défaut. [8] [9]

1.4 Le besoin d'un modèle plus dynamique

Traditionnellement, les data centres d'entreprises sont conçus pour durer pour toujours et atteindre les objectives déterminés de l'économie. Cela veut dire que les éléments sous-jacents sont dimensionnés et construits pour supporter le pic de charge projeté en termes de performance, disponibilité et sécurité. Quand la croissance volumétrique projetée ne correspond pas à la réalité, cette méthode de dimensionnement peut conduire à une situation de sous-dimensionnement ou sur-dimensionnement. Ce qui apporte un effet négatif pour les investissements et les effort de réduction de coûts.

En général, pour atteindre une meilleure disponibilité, les infrastructures sont amenées à une sous-utilisation des ressources. Comme la charge des applications varient continuellement dans les applications sur internet, il reste deux choix : soit sous-dimensionner la provision et perdre des clients ou alors sur-dimensionner et gaspiller les ressources.

Dans tous les cas, un plan détaillé de capacité est fait pour spécifier une série d'investissements importants en matériel et logiciel, dont la charge maximale est déterminée. L'image suivante illustre cette planification et les situations de problèmes de dimensionnement.

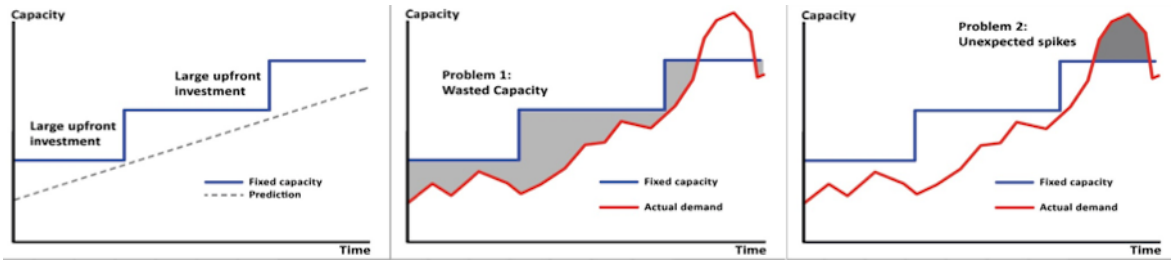

FIGURE 1.3 – Capacité fixe de ressources vs charge prévisionnelle. [10]

Face à cette problématique, un nouveau mode de livraison a été proposé pour aborder les défis du traitement des demandes pour la variation dynamique des charges applicatives. Avec la nouvelle tendance du Cloud Computing et l'**Infrastructure as a Service, Infrastructure en tant que service (IaaS)**, la conception de **clusters** hautement disponibles et des solutions extensibles peut être architecturée avec des requis non-fonctionnels comme base.

Avec sa nature extensible, le modèle de livraison cloud permet aux ressources d'être étendues et réduites dynamiquement en fonction de la consommation. Une couche logicielle d'abstraction, implémentée par les hyperviseurs, virtualise le traitement des ressources physiques, permettant ainsi au processeur, à la mémoire et aux disques durs de s'adapter aux variations des demandes. [8] [10]

1.5 Cloud Computing

Le Cloud Computing peut être défini comme un nouveau modèle de consommation et livraison de ressources et services de **TI**, et est principalement caractérisé par :

- Libre service à la demande ;
- Service réseau très accessible ;
- Location indépendante de services en commun ;
- Extensibilité et approvisionnement rapides ;
- Paiement à la consommation.

Les avancements importants dans la virtualisation, réseau, approvisionnement et architectures multi-tenantes ont permis de faire évoluer radicalement les infrastructures de data centres. Le plus grand impact du Cloud Computing vient de l'instauration de nouveaux modèles de consommation et de livraison de services qui supportent l'innovation du business.

L'évolution des data centres a permis de satisfaire une plus grande variété de besoins dans le monde du travail, ce qui implique la prise en compte de plusieurs facteurs lors de la conception selon différents objectifs. Le Cloud Computing est donc né en tant que nouveau paradigme pour les architectures data centre.

Le Cloud Computing livre dynamiquement des services sur des réseaux à partir d'un ensemble abstrait de ressources. Ces ressources se retrouvent quelque part dans le « nuage » (symbole qui fait allusion à la représentation d'internet dans les topologies réseau) disponibles immédiatement à la demande. Les types de ressources ainsi que leur localisation sont transparents aux utilisateurs finaux. Ces utilisateurs ont pour principal souci que leurs applications, données et contenus soient sécurisés et disponibles, avec un niveau de qualité spécifié.

Du point de vue de l'infrastructure, le Cloud Computing fait des fortes demandes aux ressources mutualisées dans une variété de technologies (de compute, de stockage, de réseau) pour leur allocation dynamique. Tout ceci dans un environnement automatisé, orchestré et logiquement diversifié, en conciliant une variété d'applications. L'orchestration permet de mutualiser les ressources à travers multiples data centres pour une réponse dynamique aux besoins clients.

La virtualisation de serveurs a représenté un premier et important pas pour la viabilité de l'approche Cloud Computing. Toutefois, les autres deux éléments de base de l'infrastructure data centre doivent accompagner ces changements pour permettre un accès complet aux services offerts par le Cloud. Les hyperviseurs ont permis la séparation des systèmes logiques des serveurs physiques dans le cas de la virtualisation de serveurs ; cette abstraction doit être également appliquée aux matériels réseaux et de stockage. Cela permettra la définition d'un data centre entièrement piloté par un logiciel qui gère les ressources physiques, en les activant dynamiquement selon la charge applicative.

L'image suivante illustre une vue conceptuelle d'un data centre basé sur ces trois éléments avec des couches d'abstraction permettant de sécuriser, orchestrer et livrer ses ressources aux consommateurs.

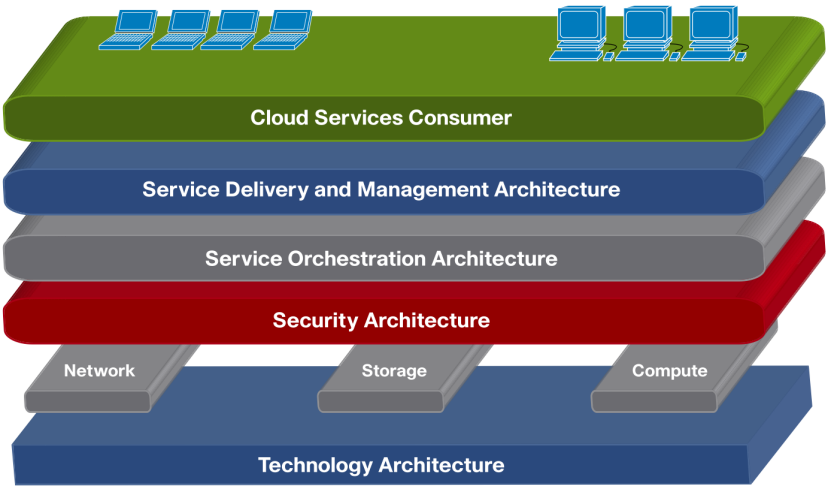

FIGURE 1.4 – Vue conceptuelle d'un data centre. [11]

L'abstraction de ces trois composants matériels est essentielle pour achever le mode de livraison Cloud au sein des data centres. L'adoption de la virtualisation des serveurs a déjà atteint son public ; en 2009 un sondage avait révélé que 77% des répondants déployaient au moins un système virtualisé dans leur data centre [12]. On observe que beaucoup de travaux se déroulent actuellement en recherche et développement se déroulent pour acquérir un niveau équivalent de maturité pour les dispositifs réseau et stockage.

L'abstraction du stockage signifie la capacité à mutualiser les dispositifs physiques de stockage pour pouvoir les utiliser en tant que volumes de stockage logiques. Cela caractérise la virtualisation du stockage ou le **Software Defined-Storage, Stockage Défini par Logiciel (SDS)**. Pour l'aspect stockage, il est reconnu que des solutions **SDS** se trouvent disponibles sur le marché, telles que EMC ViPR, HP StoreVirtual, IBM SmartCloud Virtual Storage Center entre autres.

De manière similaire, il se développe pour les réseaux une technologie fournissant une couche d'abstraction pour divers dispositifs réseau afin de permettre l'isolation logique et l'indépendance du matériel. Il se trouve que **SDN** est une des approches proposées pour traiter la problématique de l'abstraction réseau et fait donc l'objet de cette étude. Le chapitre suivant démontrera en quoi les réseaux traditionnels ne sont pas adaptés aux exigences du Cloud Computing et analysera des exemples sur divers problèmes rencontrés. L'approche SDN et ses apports seront détaillés en dernière partie. [13] [14] [8] [11]

Chapitre 2

L'aspect bloquant du réseau

Dans ce chapitre, les principales problématiques data centre dans un aspect réseau seront présentées et analysées. Seront abordés quelques questionnements sur les réseaux classiques pour tenter de répondre aux nouveaux besoins data centres. Le chapitre présentera comment divers scénarios sont traités aujourd'hui et quels sont les limites.

2.1 Le rôle du réseau dans les projets de TI

Lors du développement de projets pour l'optimisation en **TI** tels que la consolidation de data centres et la virtualisation de serveurs, une attention spéciale doit être donnée au rôle critique des réseaux dans la planification, exécution et succès en général du projet. Il est souvent admis que des planifications supplémentaires par rapport aux réseaux auraient pu contribuer au succès de plusieurs projets.

Les principaux types de modifications dans ces projets incluent l'implémentation d'équipement réseau supplémentaire pour augmenter ou améliorer la redondance, la capacité du réseau, la sécurité réseau et/ou la bande passante. Cependant, plusieurs requis associés à ces changements ne sont pas, en général, identifiés au tout début du projet. Très souvent ils ne sont détectés qu'après les étapes initiales du projet, imposant un supplément de travail et l'ajout de coûts non anticipés.

Les aspects réseau d'un projet peuvent être difficiles à gérer, et des critiques sur le fonctionnement général des réseaux sont fréquemment entendues. Des défis importants incluent la réalisation d'analyses des causes précises et opportunes, la compréhension de

la réactivité au niveau applicatif et la révélation des origines de problèmes de performance. Le simple achat d'équipement réseau n'aborde pas nécessairement ou proprement les requis réels.

Pour supporter la virtualisation complète d'une infrastructure de **TI** et continuer à optimiser le réseau, des décisions sur l'architecture doivent être faites dans le contexte de l'infrastructure existante, de la stratégie et des objectifs larges du business. Sans le développement d'un plan réseau et la conception fonctionnelle associée, les transitions réseau peuvent être risquées et conduire à un contrôle réduit des services livrés, coûts potentiellement élevés contre des résultats insuffisants et des problèmes inattendus de performance ou disponibilité.

Traditionnellement un plan et conception fonctionnelle solides suffisaient pour augmenter le succès des projets avec un réseau réactif, optimisé, moins cher et répondant mieux aux engagements des services applicatifs. Alors que ce plan reste essentiel, il est difficile dans le contexte d'utilisation actuel de maitriser complètement à l'avance la charge, dimension et tout autre requis qui doivent être assurés par les réseaux.

En face à ses difficultés et aux critiques reçues, il est facile de finir par interpréter les réseaux comme un élément bloquant pour le succès des projets. Même si sa gestion et planification peuvent être complexes, les réseaux représentent un moyen naturel pour le management et renforcement des politiques liées aux risques, performance et coûts. Seulement le réseau voit toutes les données, ressources connectées et interactions des utilisateurs à travers le Cloud. Le réseau est donc positionné de manière unique pour surveiller et mesurer l'usage et la performance des services distribués et de l'infrastructure. Les réseaux ont également un rôle central pour favoriser l'extensibilité et disponibilité. Par exemple avec sa vue unique bout-en-bout, les réseaux peuvent détecter la charge et dynamiquement la rediriger selon les politiques de contrôle.

Afin d'atteindre ce niveau de management et orchestration des ressources, on cherche à concevoir des architectures réseaux qui puissent s'étendre ou se rétracter ainsi que supporter des nouveaux services dynamiquement et rapidement en fonction des besoins immédiats. [15] [16] [17]

2.2 L'architecture réseau d'un data centre typique

La majorité des data centres d'aujourd'hui ont une structure réseau hiérarchique à trois niveaux : couche d'accès, agrégation/distribution et cœur (figure 2.1). La couche d'accès inter-connecte toutes les ressources partagées telles que serveurs, dispositifs de stockage et applications. Les réseaux d'agrégation (ou distribution) doivent fournir une haute bande passante pour la communication entre multiples réseaux d'accès. Le cœur du réseau est l'interface vers l'extérieur du réseau, qui peut être le lien avec des réseaux WAN, mobiles, VPNs ou autres types d'accès internet.

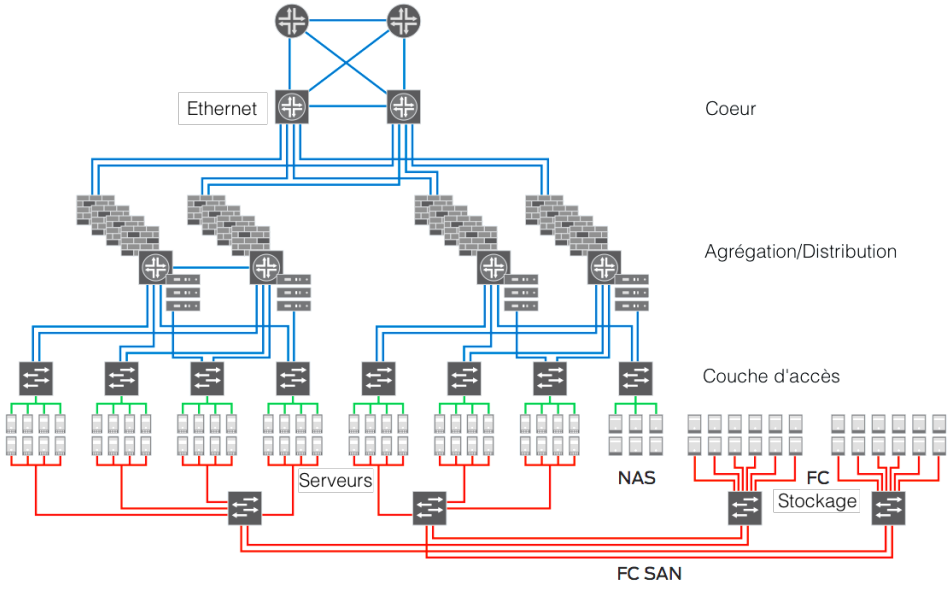

FIGURE 2.1 – Architecture réseau typique à trois niveaux. [18]

Cette architecture a été conçue pour les applications client-serveurs dans des serveurs applicatifs dédiés. Dans cette conception, le flux du trafic se fait essentiellement à partir des serveurs en direction du cœur du réseau et ensuite en dehors vers internet ou autre (flux Nord/Sud).

Ce modèle d'architecture a été la principale référence de topologie réseau pour les data centres. Cependant, il devient complexe à le maintenir dans le contexte du Cloud Computing lorsque les applications actuelles commencent à être plus distribuées, avec plusieurs couches et orientées livraison de services. Ces changements dans les applications ont impacté les réseaux pour ce qui concerne le volume et les flux du trafic.

Le trafic réseau interne a augmenté avec la croissance du nombre d'applications et services déployés ; l'utilisation de systèmes de fichiers distribués avec des données stockées séparément a eu pour conséquence une charge réseau plus importante à travers le data centre. De ce fait, on constate une forte tendance de communications inter-serveurs ou inter-VMs, impliquant un flux Est/Oust plutôt que Nord/Sud. L'industrie estime même que 80% du trafic des applications Cloud Computing constitue des flux Est/Ouest.

Cette architecture révèle une série d'interfaces de connexions des serveurs à divers type de réseaux tels que réseaux locaux, de stockage, communication entre processus. Cette disposition ajoute de la complexité et des coûts sous forme de câblage, nombre de ports, extensibilité, énergie, refroidissement etc.

Les data centres d'aujourd'hui exigent des réseaux qui sont agiles et flexibles pour pouvoir réagir rapidement aux changements et garantir une livraison efficace de services. Par exemple, des serveurs virtuels peuvent être déplacés de part et d'autre avec une simple commande en fonction de la demande. Par conséquent, les réseaux doivent s'adapter rapidement à ces changements pour éviter des perturbations du service. Cela suppose que les dispositifs semblent être connectés au même réseau local, indépendamment de leur proximité physique. Il manque à cette architecture la flexibilité nécessaire pour effectuer ces types de changements, ce qui impacte défavorablement l'efficacité opérationnelle de tout le data centre.

Afin de mieux visualiser ces difficultés, quelques scénarios critiques pour les réseaux traditionnels seront étudiés en détail. Ces scénarios supposent des infrastructures basées sur cette architecture à trois niveaux (présentée précédemment) et avec l'objectif de fonctionner en mode Cloud Computing. [19] [20] [18] [21]

2.3 La transformation des applications et exemples de scénarios critiques

Avec de multiples VMs s'exécutant chez le même hôte, partageant une carte réseau unique au moyen d'un switch logiciel (ou virtuel), les applications ont donc moins de ressources réseau que lorsqu'un un serveur physique leur est dédié. Cela peut conduire à des problèmes de performance réseau comme une bande passante réduite et un temps de latence augmenté et même à d'autres difficultés mineures comme la disponibilité

de plages d'adresses IP ; les applications peuvent ne pas être en mesure de traiter ces questions.

Les plateformes typiques d'infrastructure virtuelle fournissent des logiciels pour faire migrer les instances de VMs actives d'un dispositif physique à l'autre ; VMware Distributed Resource Scheduler (DRS) et VMotion sont des exemples de ce type de solutions. Ces solutions ne connaissent pas l'état des applications ou du réseau. Par exemple, une VM peut être migrée au milieu d'une transaction bancaire sans prendre en compte l'état de persistance de l'opération, le nombre des connexions ou la charge réseau que la VM est en train de traiter. Cela peut causer des transactions non réussies, avec perte de données et problèmes plus graves pour les utilisateurs. Par ailleurs, ces technologies permettent de migrer une VM vers un serveur physique avec plus de charge CPU disponible, mais elles n'ont pas d'informations sur la capacité réseau dans ce serveur.

Le déplacement dynamique de charges exige également que les VMs restent dans un VLAN commun, dans le même réseau au niveau 2. Pour pouvoir déplacer un réseau en dehors de son domaine niveau 2, il est nécessaire d'utiliser des procédures manuelles comme l'attribution d'adresses IP et mise à jour des entrées DNS pour les services déplacés. Pour maximiser cette flexibilité, des technologies émergent pour élargir le domaine des réseaux au niveau 2.

De nouveaux moyens tels que **Virtual eXtensible LAN (VXLAN)** et **Network Virtualization using Generic Routing Encapsulation (NVGRE)** étendent les réseaux couche 2 avec des réseaux couche 3. Même si cette capacité devient possible avec ces technologies, le trafic local aura toujours une meilleure performance et une latence inférieure s'ils restent dans un réseau niveau 2 plus grand.

2.3.1 Aspect multi-tenant

Cet exemple traite l'aspect multi-tenant des infrastructures Cloud. Pour simplifier, on assume une configuration avec deux réseaux : une pour le groupe d'ingénieurs et l'autre pour les ventes.

Pour réaliser cela avec les technologies réseaux traditionnelles, on utilise le concept de **Virtual Local Area Network, Virtual LAN (VLAN)**. Par exemple, le réseau d'ingénieurs peut être affecté au VLAN-1 et le réseau des ventes au VLAN-2. Cette attribution doit être réalisée par le système de gestion des switches virtuels dans l'hy-

perviseur. Ensuite, la configuration doit être réalisée dans tous les switches du réseau data centre et dans le switch physique auquel le routeur est connecté. Quand le VLAN est déjà utilisé, l'interconnexion n'est pas possible, cela veut dire qu'une administration continue des VLANs attribués doit être mise en place. Tout cela est fait de manière fastidieuse et manuelle par l'opérateur du réseau.

Chaque réseau est connecté à un routeur, qui doit être configuré pour prendre en compte ces VLANs. Cela veut dire que le trafic doit toujours monter et descendre pour passer par ce router (réseau accès et de distribution), ce qui n'est pas très performant. La capacité du routeur peut limiter les communication inter-départements.

Pour fournir des adresses IP automatiquement aux applications clients, un serveur DHCP doit être attribué à chaque réseau. L'équipe d'opération réseau met en place un serveur DHCP pour chaque réseau en accord avec les configurations dans les routeurs.

Le routeur doit implémenter les règles de sécurité pour permettre le trafic d'applications business entre les deux départements et l'accès internet. Les responsables de la sécurité doivent appliquer les politiques définies dans les interfaces du routeur pour assurer que seuls les flux de trafic permis sont transférés.

Cet exemple illustre la complexité opérationnelle de la configuration d'un réseau pour supporter une application. L'intervention exige un haut niveau de manipulation manuelle et concerne différents éléments de l'architecture. La totalité de la procédure est complexe et susceptible de provoquer diverses erreurs. Tout changement associé, comme le déplacement d'un serveur, l'extension d'un des réseaux, la modification de la configuration des tenants, implique quasiment la répétition complète du procédé et de la validation.

Dans le cas où la situation décrite doit être réalisée simultanément pour multiples consommateurs, il y aura clairement un grand délai d'implémentation. Dans un contexte Cloud, le traitement de demandes réseau durant plusieurs jours ou semaines devient critique et inacceptable.

2.3.2 Interconnexion WAN

Ce scénario illustre la connexion des réseaux tenants au WAN pour l'accès aux sites distants. Dans l'approche traditionnelle, un VLAN doit être créé entre le routeur du

data centre et le routeur WAN.

Un protocole de routage doit être défini pour fournir une résilience en cas de failles de communication. La configuration doit être appliquée dans les deux routeurs impliqués. Pour offrir des mécanismes anti-failles aux niveaux 2 et 3 dans le WAN, plusieurs points VPNs doivent être déployés et configurés, ce qui ajoute de la complexité dans l'opération.

Traditionnellement, les réseaux du data centre et du WAN sont gérés par des responsables distincts. Cela implique la coordination entre les deux personnels réseaux, en général via une structure formelle de projet et procédures manuelles. Par ailleurs, avec les demandes de divers tenants, ce modèle introduit des délais ainsi que des problèmes d'extensibilités supplémentaires lorsqu'ils requièrent des VLANs ou protocoles de routage dédiés.

2.3.3 Monitoring dans un data centre

Historiquement, les systèmes de monitoring se sont appuyés sur une variété de protocoles et une série fragmentée d'outils. Ces outils incluent le monitoring de la performance du réseau, des applications et des analyses de sécurité, tels que **Intrusion Detection System, Système de Détection d'Intrusion (IDS)** et **Intrusion Prevention System, Système de Prévention d'Intrusion (IPS)**. En complément l'inspection des paquets, ces outils utilisent plusieurs meta protocoles pour fournir des données sur les réseaux, tels que SNMP. NetFlow et sFlow.

L'ajout de ces outils à l'opération du réseau est le premier pas vers une visibilité opérationnel, permettant de détecter et solutionner les problèmes plus rapidement. La difficulté qui reste est d'alimenter ces outils avec la redirection du trafic vers leurs capteurs, pour qu'ils puissent superviser et gérer la massive quantité de données passantes d'une manière flexible et efficace.

La localisation des pannes considérablement simplifié si les données des paquets sont filtrées et rendues disponibles aux administrateurs du réseau. Précédemment, les flux de données circulaient principalement en direction Nord/Sud, le placement de la capture ou redirection du trafic était évidente : dans les points d'entrée / sorties du réseau. Toutefois, avec les tendances actuelles de flux plutôt Est/Ouest, de mobilité des hôtes et de demandes plus importantes pour performance, la supervision est devenue plus difficile et couteuse dans les data centres modernes.

Les approches initiales pour la résolution de ces problèmes étaient l'agrégation du trafic drainé à des systèmes haute performance et envoyé aux outils de monitoring. Dispositifs comme les **Network Packet Brokers (NPBs)** offrent des fonctionnalités additionnelles telles que manipulation ou enregistrement de la charge utile.

Le déploiement de ces outils pour chaque tranche réseau des tenants n'est pas efficace, particulièrement quand plusieurs instances des outils sont requises pour supporter le traitement du trafic excessivement important pour être traité par une seule instance. En outre, l'ajout d'instances et outils exige des attentes répétitives pour la maintenance et implique diverses étapes pour le routage du trafic, connexion de systèmes de drainage et ensuite réversion à la configuration de routage initiale. Tout cela effectué manuellement par l'administrateur réseau. Une fois déployés, ces solutions fixent le trafic statiquement un ensemble d'outils, ce qui conduit au cloisonnement des informations et difficultés à les partager entre tenants.

2.4 Aspects de sécurité

Comme développé précédemment, on exige de nos jours que les applications livrent immédiatement des informations et services spécifiques au contexte, à une latence réduite et à une haute performance. Parallèlement, le Cloud Computing et les applications orientées services introduisent des demandes plus strictes au niveau service. La mutualisation de ressources et les infrastructures multi-tenantes ont apporté de nouvelles préoccupations pour la sécurité qui n'existaient pas précédemment et qui ne sont donc pas traitées dans l'architecture traditionnelle. Cette section a pour but d'aborder quelques menaces et questions de sécurité introduites par la virtualisation et le Cloud Computing.

Points invisibles de la communication

Les applications de sécurité réseaux traditionnelles ne voient pas la communication entre VMs au sein du même hyperviseur, à moins que toutes leurs communications ne soient routées à l'extérieur de la machine hôte vers l'application de sécurité et re-routées à l'intérieur. Cette manière de traiter la problématique introduit un ralentissement considérable du réseau.

Dans le Cloud Computing, le moyen de traiter ces deux problèmes est d'intégrer des modules de sécurité dans chaque VM pour qu'elles puissent s'auto-protéger. Cette

solution oblige la re-configuration de tous les systèmes en cas de mise à jour des politiques de sécurité. Il manque dans l'architecture actuelle un contrôleur central qui pourrait diffuser les politiques dans tous les nœuds.

Attaques entre VMs et exposition de l'hyperviseur

Les serveurs virtualisés utilisent les même systèmes d'exploitation et applications que le serveurs physiques. Les vulnérabilités retrouvées alors représentent donc des menaces pour les systèmes physiques ainsi que pour les environnements virtuels. De cette manière, quand un élément de l'environnement virtuel est compromis, l'ensemble du système est en risque dès lors qu'un système de sécurité conscient de la virtualisation n'est pas en place.

Dans ce scénario, un hacker peut attaquer un système invité, qui peut ensuite infecter d'autres VMs. Le risque augmente avec le nombre de VMs hébergées. Une protection capable de détecter des activités malveillantes au niveau des VMs doit être mise en place, indépendamment de la localisation des VMs dans l'environnement virtuel.

Un autre mode d'attaque concerne l'hyperviseur qui devient une cible d'attaque en raison de son rôle et ses responsabilités. Certaines attaques vont essayer de traverser l'espace d'isolation des VMs pour compromettre l'hyperviseur. Sécuriser l'hyperviseur est donc indispensable, malgré la complexité de réalisation.

VMs à niveaux de confiance mixtes

Les VMs qui contiennent des données sensibles peuvent finir par résider dans le même hôte qu'une autre VM moins critique, ce qui entraine différents niveaux de confiance dans un groupement de VMs. Il serait possible de séparer les VMs selon leurs niveaux de sécurité, mais ce principe contredit l'intention de la virtulisation de faire une meilleure utilisation des ressources. Cette problématique implique un système de protection par VM, malgré la complexité déjà évoquée à synchroniser les politiques entre tous les systèmes.

Lacunes sur les instantanées

La virtualisation et le Cloud Computing apportent des fonctionnalités telles que : approvisionnement, clonage, migration et désaffectation à la demande. Il en résulte que les VMs sont activées et inactivées à cycles rapides et il peut être difficile d'assurer une sécurité efficace de ces systèmes tout en les gardant à jour.

Après une période d'inactivité, l'écart des VMs par rapport à la base de sécurité peut être tellement important que la simple mise sous tension peut introduire des vulnérabilités considérables. Par ailleurs, même les VMs inactives peuvent être compromises. De cette manière, de nouvelles VMs peuvent être clonées à partir de templates avec une sécurité obsolète et être mises en ligne.

Quand ces VMs sont réactivées ou clonées, elles représentent une vulnérabilité instantanée à partir du moment où elles sont connectées au réseau. Une solution serait l'installation, pour chaque hôte, d'une VM dédiée pour la mise à jour des applications de sécurité des autres VMs qui sont lancées, ce qui permettrait de profiter des bénéfices de la virtualisation en toute sécurité.

Blocage de ressources

Quand des opérations gourmandes en ressources sont appliquées aux VMs, elle peuvent rapidement surcharger le système. Par exemple, quand les balayages ou mise-à-jour des antivirus sont réalisés simultanément sur plusieurs VMs dans un même serveur physique, le système peut ne pas supporter la consommation intensive des ressources (mémoire, CPU, réseau, stockage). Cela peut impacter la performance globale des applications en exécution.

Dans les systèmes physiques, des anti-virus installés dans chaque système d'exploitation consomment une mémoire additionnelle importante. L'application de cette architecture aux systèmes virtuels signifie une perte indésirable d'efficacité sur l'utilisation des ressources. Les produits qui ignorent la virtualisation proposent la randomisation ou le regroupement pour éviter la charge intensive des opération simultanées.

Malheureusement, la randomisation ne permet pas d'éviter les longues périodes de haute consommation du système pour les cycles complets de balayage. Le groupement ne contribue pas à la nature mobile de la virtualisation et exige une reconfiguration lors de la migration ou du clonage de VMs.

Chapitre 3

Applications SDN et leurs apports aux data centres

Ce chapitre définira SDN et présentera ses réponses aux problématiques réseau rencontrées en général dans les data centres, qui ont été débattues dans le chapitre précédent. Le chapitre démontrera également les apports de SDN au sein des data centres par rapport à ces problématiques présentées précédemment.

3.1 Définition de SDN

Les requis réseaux des applications devraient être articulés dans un langage simple, utilisé pour demander les comportements réseau souhaités. La programmation des réseaux est aujourd'hui très limitée, introduisant un malheureux compromis : le développement d'applications contraint par un paramétrage réseau excessivement détaillé, ou l'ignorance de ces détails par le traitement du réseau comme une boîte noire. Aucune de ces solutions n'est convenable ; la première implique des applications spécifiques à chaque type de réseau alors que dans la deuxième, le contrôle nécessaire à l'extraction de fonctionnalités réseau n'est pas présent.

Un niveau approprié d'abstraction des capacités réseaux est nécessaire pour les rendre programmables et améliorer l'utilisation des ressources. L'instanciation de services réseau doit pouvoir se faire instantanément, de manière alignée aux besoins des applications. Le réseau doit permettre l'établissement de connectivité interne et entre data centres, tout en gardant la cohérence avec les politiques définies par le prestataire cloud et ses tenants.

Aujourd'hui, tout cela se fait lentement, manuellement avec un risque élevé d'erreurs, comptant sur les ordres de travail pour établir une multitude de configurations selon le fournisseur de chaque équipement.

Les principes **SDN** sont plus adaptés à ce scénario, l'approche propose une couche d'abstraction pour permettre la programmation du réseau et autoriser le contrôle dynamique de services. SDN est un nouveau **paradigme** réseau défini comme une architecture qui a pour but de centraliser sur un contrôleur l'intelligence du réseau. Cette intelligence étant traditionnellement distribuée parmi plusieurs équipements réseaux réalisant une fonction spécifique dans l'infrastructure.

Ces dispositifs ont en général une fonctionnalité de commutation de paquets (**plan de données**) et une partie pour traiter ses données appliquant une logique spécifique selon les états et la configuration enregistrés (**plan de contrôle**). SDN propose de dissocier ces deux fonctions dans les dispositifs et d'agréger dans un contrôleur commun l'activité de traitement. L'imagine ci-dessous permet de visualiser les différences entre les architectures traditionnelles et SDN.

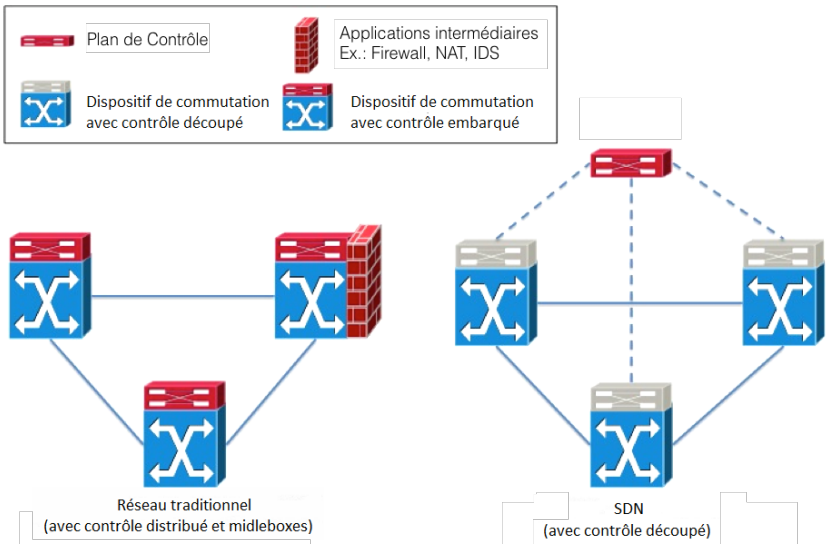

FIGURE 3.1 – Architecture réseau traditionnel et SDN. [22]

L'expérience saisie lors de la construction des grands réseaux IP/MPLS a montré que l'intelligence doit être poussé vers les bords pour autoriser l'extension des réseaux. Le principe doit être appliqué afin de promouvoir un cœur du réseau data centre simplifié et efficace. L'approche sépare les services réseaux de l'infrastructure permettant l'innovation parallèle dans les deux domaines.

Des leçons acquises dans la conception des réseaux mobiles ont apporté la technique d'optimisation pour la mobilité et d'automatisation opérationnelle à large échelle. Cela permet la création d'un modèle auto-instancié et dirigé par des politiques qui minimise les coûts et délais de livraison.

Cette solution apporte le comme bénéfice d'avoir, l'introduction d'une interface commune de management, permettant la mise en place dynamique de services, indépendante de la marque/modèle des dispositifs réseau. Avec SDN, l'administration réseau devient plus agile car un seul élément (le contrôleur) est à maîtriser au lieu d'avoir à configurer l'ensemble des équipements du système, accélérant considérablement le temps de convergence du réseau pour l'accommodation de nouvelles applications déployées.

3.2 Virtualisation des fonctions réseau, NFV

Un concept qui est très souvent discuté en conjonction avec **SDN** est **Network Functions Virtualization, Virtualisation des fonctions réseau (NFV)**. **NFV** pousse les technologies de virtualisation à consolider les applications réseau sur des serveurs, switches et baies de stockage standards de l'industrie. La virtuliasation des fonctions réseau no seulement réduit les dépenses en équipements, mais aussi apporte d'autres bénéfices tels que l'extension agile d'applications, l'innovation à une vitesse plus rapide, une plus haute disponibilité et une meilleure utilisation de ressources.

Toutefois, pour se bénéficier des apports, il est nécessaire que l'infrastructure réseau sous-jacente s'adapte rapidement et automatiquement. Par exemple, pour migrer une fonction réseau dans un nouveau matériel, les politiques et les configurations associées à ce service doivent être provisionnés dans un nombre d'équipements et d'autres fonctions réseau. La complexité de configurer les réseaux dans un environnement si dynamique augmente énormément avec l'introduction de nouveaux éléments réseaux.

Bien que le développement de SDN et NFV puissent procéder indépendamment, l'association des deux principes est de plus fort intérêt pour le progrès des solutions cloud. SDN peut être employé en tant que technologie facilitatrice de la virtualisation des fonctions réseau, favorisant la consolidation des applications réseau dans des dispositifs industriels standards.

3.3 SDN, NFV et le Cloud Computing

Les approches Cloud permettent aux opérateurs réseau d'assurer une création et un déploiement de services plus rapides. Elles répondent également aux attentes croissantes sur la qualité et la performance des solutions, tout en traitant les charges trafics de plus en plus importantes.

Afin de supprimer les contraintes des réseaux dans les data centres, une plateforme innovante pour l'abstraction des fonctionnalités réseau et pour l'instanciation automatisée de services est proposée. Avec SDN, les fournisseurs de services cloud, opérateurs à l'échelle web et grandes entreprises technologiques peuvent construire une infrastructure réseau multi-tenante, robuste et extensible pour livrer des espaces virtuels de compute, stockage et réseau prêts à l'usage pour des milliers de tenants et groupes d'utilisateurs.

Le **plan de contrôle** dans SDN fonctionne en lien avec le système de management cloud afin de configurer dynamiquement des éléments réseaux pour s'adapter aux décisions des systèmes d'orchestration pour le changement d'utilisations des ressources. SDN fourni l'infrastructure nécessaire pour réaliser cette capacité de NFV.

However, fully realizing the potential of this technology in today's service provider networks means doing more than just separating the forwarding and control planes. This expanded definition of Service Provider SDN includes :

> Integrated network control – this unified control layer controls the data center and network as an integrated entity, in order to deliver the best user experience. > Orchestrated network and cloud management – a unified approach that includes legacy network management and new cloud management systems. It is this end-to-end orchestration that enables flexible service creation, which in turn makes the network dynamic, adaptive and agile. This cuts introduction and modification cycles for services and removes barriers to innovation. > Service exposure – the SDN architecture provides network awareness to the application layer through service exposure application programming interfaces (APIs). These APIs not only provide raw network data, but are instead composed APIs that deliver actionable information at the application level.

The service control layer of the Service Provider SDN architecture brings elastic, real-time allocation of resources for networking services. It enables these services to be defined and provisioned through self-service portals in a matter of minutes, rather than the days, weeks or even months that are traditionally required.

This demands a platform with integrated control across networking domains that exposes “composed APIs” for new revenue generation. An end-to-end network management system across IP and transport infrastructure provides further efficiencies, develops greater responsiveness, and enables more reliable planning, provisioning, activation, adaptation and control of new service connections.

The goal is to couple cloud management to a programmable network, via SDN controllers, to achieve full integration of the cloud and network, where cloud resources are no longer confined to a single data center, but are spread throughout the network.

Using common orchestration for end-to-end service management as well as for operations, administration and maintenance reduces operating costs in areas such as provisioning, monitoring and faultfinding. More importantly, end-to-end orchestration enables flexible service creation, which makes the network dynamic, adaptive and agile.

3.4 Scénarios d'utilisation

Un système cloud qui s'intègre de façon transparente et dynamique avec un réseau programmable (grâce à SDN) peut fournir une importante plus-value à ses opérateurs et à leurs abonnés (consommateurs finaux et entreprises). Aujourd'hui la connectivité seule ne suffit pas, les utilisateurs réclament une variété de services hébergés dans le cloud, et cela exige des réseaux la capacité de fournir la connectivité correcte à l'application souhaitée. C'est dans ce cadre que la réelle valeur d'un cloud à réseau dynamiquement programmable devient visible.

Cette capacité permet de découper le réseau en tranches et offrir aux clients leurs morceaux dédiées et personnalisés. Il y a une variété de scénarios imaginables à partir de ce concept de diviser le réseau pour convenir à différents applications et besoins.

Un des cas d'utilisation est l'infrastructure virtuelle d'entreprise, dans laquelle un portail basé sur SDN peut être étendu selon les particularité de l'organisation. La solution associe la coordination riche d'un contrôleur cloud et d'un contrôleur SDN. Cela permet l'instanciation, la réplication et la migration du réseau et services basés cloud dans la meilleure localisation disponible, en fonction des requis tenants, de la congestion globale du réseau et de la disponibilité de ressources. Cette solution conforme à l'idéal de ne pas limiter le cloud avec les contrainte physique du data centre, implémentant un suivi de flux et un renforcement de politiques dans un niveau logique pour le cloud. Cela englobe plusieurs data centres, quelle que soit leur localisation géographique dans l'infrastructure du réseau.

Another case is the virtual home gateway. This is an example of virtualizing some of the functions of a traditional home gateway and hosting them in a Network-enabled Cloud. Virtualization reduces the complexity of the home gateway by moving most of the sophisticated functions into the network. As a result, operators can prolong the home gateway refreshment cycle, cut maintenance costs and reduce time to market for new services. The most important aspect of this solution, however, is that it gives the network visibility to all the devices that were traditionally hidden behind the home gateway. This opens up significant revenue opportunities through the ability to offer services that are personalized in a much more granular way.

Avec le cloud, SDN et NFV travaillant ensemble, on peut dynamiquement étendre les fonctions réseau au sein des data centres. Lors que la charge réseau augmente, le

contrôleur SDN peut demander au gestionnaire cloud d'instancier une nouvelle fonction réseau dans le cloud pour commencer à répartir le trafic.

Un des scénarios les plus traditionnels de l'intégration des services dynamiques avec SDN consiste à en resserrer l'interaction entre le réseau et le cloud. Pour les services "inline" tels que filtrage, modification des entêtes et **Network Address Translation, Traduction d'adresse réseau (NAT)**, les opérateurs utilisent diverses "appliances", ou d'autres services pour gérer le trafic utilisateur. Ces services sont hébergés dans du matériel physique ou en machines virtuelles. L'enchaînement de services est nécessaire pour router le trafic client à travers ces services. Les solutions traditionnelles sont soit statiques ou très limitées en flexibilité et extension.

3.5 Complexité

3.6 Agilité

3.7 Sécurité

Conclusion

Même avec le succès incontestable de l'architecture d'internet, l'état de l'industrie réseau et l'essence de son infrastructure se trouvent en phase critique. Il est généralement admis que les réseaux courants sont excessivement chers, compliqués à gérer, sujets aux blocages des fournisseurs et difficiles à faire évoluer.

On constate donc un réel besoin de faire évoluer cette architecture mais des résistances s'opposent à cette évolution en raison de la complexité et la possible saturation du système. En réponse, les réseaux programmables ont été un objet intensif de recherche par la communauté. Les travaux dans ce domaine s'orientent vers l'offre SDN, un nouveau paradigme transformant cette architecture.

L'approche SDN sépare le plan de contrôle et le plan de données, offrant un contrôle et une vision centralisés du réseau. Cela peut apporter certains bénéfices comme le contrôle directement programmable, la simplification du hardware réseau et la simplification de l'ingénierie du trafic. En revanche, des défis d'implémentation sont à surmonter tels que la concentration des risques dans un contrôle physiquement centralisé, l'équilibre entre flexibilité et performance et les conditions d'interopérabilité.

La flexibilité apportée par SDN est telle que de nombreuses possibilités d'applications sont à imaginer. Essentiellement pour l'administration de data centers, le contrôle d'accès et de la mobilité pour les réseaux campus ainsi que l'ingénierie du trafic pour les réseaux WAN.

Le marché suit de près les nouveautés dans le domaine et investit sur les technologies implémentant SDN. Les stratégies ne sont pas encore assez matures et les consommateurs potentiels attendent des offres plus consolidées. Cependant, des solutions innovantes commencent à surgir et certaines sociétés assument le rôle de tête dans le marché.

On s'aperçoit que l'ampleur des possibilités SDN, même si elle présente un avantage en théorie, freine son adoption. En raison de la grande variété de concepts et produits,

les consommateur hésitent toujours à prendre une décision. En même temps, les grands fournisseurs cherchent à la fois à exploiter le nouveau marché et à protéger leurs solutions consolidées. Ces obstacles même s'ils sont confirmés, ne semblent pas être assez forts pour empêcher les échanges à long terme.

Au vu cette étude, il semblerait que dans un futur proche, les clients les plus informés et les plus disposés à innover vont commencer à déployer SDN. Leurs expériences et les résultats obtenus vont fortement impacter le choix des prochains consommateurs. Il est possible que ceux qui dessineront le futur de la technologie des réseaux informatiques pour les prochaines années seront ceux qui auront osé se lancer les premiers. Cette démarche peut éventuellement représenter un risque, mais aussi l'opportunité de tirer des bénéfices plus durables et de prendre de plus larges parts du marché.

Index

Acronymes

ACI Application Centric Infrastructure, Infrastructure centrée sur les applications

API Application Programming Interface, Interface de Programmation

ASIC Application Specific Integrated Circuit, Circuit intégré pour application spécifique

DHCP Dynamic Host Control Protocol, Protocole pour la configuration automatique d'hôte

DNS Domain Name System, Système de noms de domaine

GRE Generic Routing Encapsulation

HTTP HyperText Transfer Protcol, Protocole de transfert de hypertexte

IaaS Infrastructure as a Service, Infrastructure en tant que service

IaaS Infrastructure as a Service, Infrastructure en tant que Service

IDS Intrusion Detection System, Système de Détection d'Intrusion

IETF Internet Engineering Task Force, Détachement d'ingénierie d'internet

IP Internet Protocol, Protocole d'Internet

IPS Intrusion Prevention System, Système de Prévention d'Intrusion

IRTF Internet Research Task Force, Détachement de recherche d'internet

LAN Local Area Network, Réseau local

MPLS MultiProtocol Label Switching, Commutation multi-protocoles par étiquettes

NAT Network Address Translation, Traduction d'adresse réseau

NFV Network Functions Virtualization, Virtualisation des fonctions réseau

NOS Network Operating System, Système d'exploitation réseau

NPB Network Packet Broker

NVGRE Network Virtualization using Generic Routing Encapsulation

ONE Open Network Environment, Environnement Réseau Ouvert

ONF Open Networking Foundation

QoS Quality of Service, Qualité de service

SDN Software-Defined Networking : Réseau Informatique Défini par Logiciel

SDS Software Defined-Storage, Stockage Défini par Logiciel

SI Système d'Information

TI Technologie de l'Information

VLAN Virtual Local Area Network, Virtual LAN

VM Virtual Machine, Machine Virtuelle

VXLAN Virtual eXtensible LAN

WAN Wide Area Network, Réseau étendu

Glossaire

Abstraction En informatique, l'abstraction est un terme souvent employé pour désigner le mécanisme et la pratique qui réduisent et factorisent les détails négligeables de l'idée exprimée afin de se focaliser sur moins de concepts à la fois. C'est aussi la notion de couches d'abstraction utilisée comme moyen pour gérer la complexité des systèmes informatiques où les couches correspondent à des niveaux de détails appliqués. [23]

Big Data Big Data est un terme appliqué aux ensembles de données dont la taille (ou le format) est au-delà de la capacité des outils logiciels communs, qui ne peuvent plus les capturer, les gérer et les traiter. Une nouvelle classe de technologies et outils a été développée pour attribuer une valeur commerciale à ces données grâce à une analyse complexe. Le terme est employé en référence à ce type de données ainsi qu'aux technologies utilisées pour les stocker et les traiter. [24]

Cloud Computing Cloud Computing, ou informatique dans les nuages, est une évolution de la fourniture de services **TI** qui offre un moyen d'optimiser l'usage et le déploiement rapide de ressources. Cela se fait par des systèmes et solutions plus efficaces et **scalables**, fournissant un niveau plus haut d'automatisation. Diverses entreprises ont adopté le cloud computing et réalisent des avantages significatifs en agilité, réduction de coûts et soutien de la croissance du business. [25]

Cluster En réseaux informatiques, un cluster désigne un groupe des machines reliées entre elles à l'aide d'un réseau de communication. Cette configuration est souvent utilisée pour réaliser des calculs à haute performance. [26]

Data Center Centre de traitement de données. Il s'agit d'une installation utilisée pour héberger des systèmes informatiques et les composants associés, comme les systèmes de télécommunication et de stockage. En général, un data center inclut alimentation et connexions des données redondantes, contrôles d'environnements comme la climatisation ainsi que divers dispositifs de sécurité. [27]

Fabric En informatique, fabric (qui signifie tissu en anglais) est un synonyme de plateforme ou structure. En général, le terme fabric décrit la façon dont différents composants travaillent ensemble pour former une entité unique. Dans ces systèmes la liaison entre les composants est tellement dense qu'un schéma représentant leurs relations rassemblerait à une pièce de tissu tricotée. Sous ce terme généralement admis par l'industrie réseau, un fabric est une topologie réseau dans laquelle les composants transmettent des données l'un à l'autre à travers les switches d'interconnexion. [28] [29]

Middlebox Boîtier intermédiaire. Un middlebox est un serveur conservant des états de la communication entre deux hôtes. Ils se différencient des hôtes qui représentent les extrémités de la communication. Ils sont encore différents des routeurs qui ne gardent pas d'états concernant les sessions de communications. [30]

Open Daylight Association initiée par Linux Foundation pour l'union des géants du marché réseau dans le but de développer un contrôleur SDN open source, pour l'innover, l'encourager et pour permettre son adoption accélérée. [31]

Open Source Logiciel avec code source ouvert, qui peut donc être utilisé librement, modifié et partagé par quelqu'un. Un logiciel open source est développé par plusieurs personnes et distribué sous des licences qui se conforment à la définition d'open source. [32]

OpenFlow Le protocole OpenFlow vise à standardiser l'interface entre les applications et le contrôleur ainsi que l'interface entre le contrôleur et les éléments de commutation. [22] [33]

Paradigme Un paradigme consiste en une collection de règles, standards et exemples de pratiques scientifiques, partagés par un groupe de scientifiques. Sa genèse et poursuite en tant que tradition de recherche sont conditionnées à un fort engagement et consensus des personnes impliquées. [34] D'après Dosi [35], quand un nouveau paradigme technologique apparaît, il représente une discontinuité ou un changement dans la manière de penser. Ce changement apporté par le paradigme est souvent lié à une sorte d'innovation radicale qui implique une nouvelle technologie. Dans ce document, le terme paradigme sera employé dans ce sens d'innovation et application de nouvelle technologie.

Plan de Contrôle Intelligence du réseau, ensemble des données locales utilisées pour établir les entrées des tableaux de commutation, qui sont utilisés par le plan de données pour effectuer la transmission du trafic entre les ports d'entrée et de sortie du dispositif. [36]

Plan de Données Le plan de donnés traite les data-grammes entrants dans le média à travers une série d'opérations au niveau des liens qui collectent ces data-grammes et réalisent divers tests de cohérence basiques. Ensuite les data-grammes sont transférés en accord avec des tableaux pré-remplis par le **plan de contrôle**. [36]

Scalabilité Terme provenant de l'anglicisme *scalability* qui exprime la capacité d'être mis à échelle. En informatique cela désigne la capacité d'un système, d'un réseau ou un processus de gérer l'augmentation ou la réduction de la charge de manière à pouvoir la gérer. [37]. Le terme est souvent employé pour exprimer une extensibilité, évolutivité ou passage à l'échelle, mais il n'y «a pas d'équivalent communément admis en français ». [38]

Virtualisation Pour diverses entreprises, l'infrastructure serveur virtualisée est la base sur laquelle le **cloud** est construit. Initialement, les technologies de virtualisation ont permis aux data centers de consolider leurs infrastructures pour réduire les coûts. Avec le temps, l'intégration des technologies pour le management flexible de ressources a facilité une allocation plus dynamique. Cela a aidé à réduire les coûts et a également augmenté la flexibilité et la performance. [25]

Bibliographie

[1] Albert Greenberg et al. « The cost of a cloud: research problems in data center networks ». In : *ACM SIGCOMM Computer Communication Review* 39.1 (2008), p. 68–73.

[2] Albert Greenberg et al. « The cost of a cloud: research problems in data center networks, section 3. Agility ». In : *ACM SIGCOMM Computer Communication Review* 39.1 (2008), p. 68–73.

[3] *Examining the Impact of Security Management on the Business*. Executive Summary. An AlgoSec Survey. 2013.

[4] *Solving Critical Challeges of the Virtualized Data Center*. Executive Summary. Market Pulse. 2011.

[5] *Understanding Data Centers and Cloud Computing, Section What Is a Data Center?* White Paper. Global Knowledge Training LLC. 2010.

[6] Luiz Andre Barroso et Urs Holzle. « The datacenter as a computer: An introduction to the design of warehouse-scale machines, Chapitre 1 : Introduction ». In : *Synthesis lectures on computer architecture* 4.1 (2009), p. 1–108.

[7] Krishna Kant. « Data center evolution: A tutorial on state of the art, issues, and challenges, section 2. Data center organization and issues ». In : *Computer Networks* 53.17 (2009), p. 2939–2965.

[8] Sandeep Raghuraman. *The Journey Toward the Software-Defined Data Center*. White Paper. Cognizant (NASDAQ: CTSH). Sept. 2013.

[9] M. Girola et al. *IBM Data Center Networking: Planning for Virtualization and Cloud Computing, chapitre 2 : Servers, storage, and software components*. IBM redbooks. IBM Redbooks, 2011. isbn : 9780738435398. url : `http://books.google.fr/books?id=EKjEAgAAQBAJ`.

[10] Harish Ganesan. *AWS Cost Saving Tip 5: How Amazon Auto Scaling can save costs*. Web Site. http://harish11g.blogspot.fr/2013/04/Amazon-Web-Services-AWS-Cost-Saving-Tips-how-Amazon-AutoScaling-can-reduce-leakage-save-costs.html. Avr. 2013.

[11] Kapil Bakshi. *Cisco Cloud Computing - Data Center Strategy, Architecture, and Solutions*. White Paper. Cisco Systems, Inc. 2009.

[12] *Virtualization & TCO: Linux vs. Microsoft*. Sondage. Gabriel Consulting Group, Inc. 2009.

[13] M. Girola et al. *IBM Data Center Networking: Planning for Virtualization and Cloud Computing, chapitre 1 : Drivers for a dynamic infrastructure*. IBM redbooks. IBM Redbooks, 2011. isbn : 9780738435398. url : `http://books.google.fr/books?id=EKjEAgAAQBAJ`.

[14] *Cloud-Ready Data Center Reference Architecture, Section : Framework*. White Paper. Juniper Networks, Inc. Mai 2010.

[15] M. Girola et al. *IBM Data Center Networking: Planning for Virtualization and Cloud Computing, chapitre 4 : The new data center design landscape*. IBM redbooks. IBM Redbooks, 2011. isbn : 9780738435398. url : `http://books.google.fr/books?id=EKjEAgAAQBAJ`.

[16] V. Josyula, M. Orr et G. Page. *Cloud Computing: Automating the Virtualized Data Center, chpaitre 3 : Data Center Architecture and Technologies*. Networking Technology. Pearson Education, 2011. isbn : 9780132604048.

[17] *Effects of virtualization and cloud computing on data center networks, Section : Introduction*. Technology Brief. Hewlett-Packard Development Company, L.P. Oct. 2011.

[18] *The Cloud-Ready Data Center Network, applying the lessons of cloud computing to vastly improve economics of networking and the user experience*. White Paper. Juniper Networks, Inc. Juin 2012.

[19] *Effects of virtualization and cloud computing on data center networks, Section : Changing business applications*. Technology Brief. Hewlett-Packard Development Company, L.P. Oct. 2011.

[20] *Cloud-Ready Data Center Reference Architecture, Section : Network Infrastructure*. White Paper. Juniper Networks, Inc. Mai 2010.

[21] P. Raj et G.C. Deka. *Handbook of Research on Cloud Infrastructures for Big Data Analytics, chapitre : The Network Infrastructures for Big Data Analytics*. Advances in data mining and database management (ADMDM) book series. IGI Global, 2014. isbn : 9781466658653. url : http://books.google.fr/books?id=m95GAwAAQBAJ.

[22] Bruno Nunes Astuto et al. *A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks*. Anglais. Section 3. SOFTWARE-DEFINED NETWORKING ARCHITECTURE. Jan. 2014.

[23] Robert M. Keller. *Computer Science: Abstraction to Implementation, Section 1.1 The Purpose of Abstraction*. Article. Harvey Mudd College. Sept. 2001.

[24] *Information Management and Big Data A Reference Architecture*. An Oracle White Paper. Fév. 2013.

[25] *Intel's Vision of Open Cloud Computing, section Speeding Agility, Reducing Costs, and Accelerating Innovation via Cloud*. White Paper. Intel IT Center. Août 2013.

[26] Qingkui Chen, Haifeng Wang et Wei Wang. « Continuance Parallel Computation Grid Composed of Multi-Clusters. » In : *Journal of Networks* 5.1 (2010).

[27] William Tschudi et al. « High-performance data centers: A research roadmap ». In : (2004).

[28] Margaret Rouse. *network fabric*. Web Site. http://searchsdn.techtarget.com/definition/network-fabric. Mar. 2014.

[29] Martin Casado et al. « Fabric: A Retrospective on Evolving SDN, section 3 Extending SDN ». In : *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*. HotSDN '12. Helsinki, Finland : ACM, 2012, p. 85–90. isbn : 978-1-4503-1477-0. doi : 10.1145/2342441.2342459. url : http://doi.acm.org/10.1145/2342441.2342459.

[30] Pamela Zave. « Internet Evolution and the Role of Software Engineering ». English. In : *The Future of Software Engineering*. Sous la dir. de Sebastian Nanz. Section 3 The Real Internet et 4 Internet trends and evolution. Springer Berlin Heidelberg, 2011, p. 152–172. isbn : 978-3-642-15186-6. doi : 10.1007/978-3-642-15187-3_12. url : http://dx.doi.org/10.1007/978-3-642-15187-3_12.

[31] *Open Daylight Project*. Web site. http://www.opendaylight.org/project. Avr. 2014.

[32] *Open Source Initiative*. Web site. http://opensource.org/. Avr. 2014.

[33] Nick McKeown et al. « OpenFlow: Enabling Innovation in Campus Networks ». In : *SIGCOMM Comput. Commun. Rev.* 38.2 (mar. 2008). Section 2. THE OPENFLOW SWITCH, p. 69–74. ISSN : 0146-4833. DOI : 10.1145/1355734.1355746. URL : http://doi.acm.org/10.1145/1355734.1355746.

[34] D. Despotovi S. Cvetanovi et I. Mladenovi. « The concept of technological paradigm and the cyclical movements of the economy ». Anglais. In : *Facta universitatis - series: Economics and Organization* 9.2 (2012), p. 149–159. ISSN : 330.342.143.

[35] G. Dosi. *Technological paradigms and technological trajectories, Research Policy.* Anglais. 1982.

[36] Thomas Nadeau D. et Ken Gray. *SDN: Software Defined Networks.* 1st. Chapitre 2 - Centralized and Distributed Control and Data Planes. O'Reilly Media, Inc., 2013. ISBN : 1449342302, 9781449342302.

[37] André B. Bondi. « Characteristics of Scalability and Their Impact on Performance ». In : *Proceedings of the 2Nd International Workshop on Software and Performance.* WOSP '00. Ottawa, Ontario, Canada : ACM, 2000, p. 195–203. ISBN : 1-58113-195-X. DOI : 10.1145/350391.350432. URL : http://doi.acm.org/10.1145/350391.350432.

[38] René J CHEVANCE. « Serveurs multiprocesseurs et SGBD parallélisés ». In : *Techniques de l'ingénieur. Informatique* H2068 (2001), H2068–1.

SDN : Software-Defined Networking

rédigé par Cynthia Lopes do Sacramento

Résumé

De récentes technologies et concepts émergent pour répondre aux nouvelles utilisations des réseaux et internet. Comme par le passé pour le Big Data, conçu pour le traitement des énormes quantités de données ou le Cloud Computing pour le management de l'hébergement de ressources. Une évolution similaire est attendue dans le domaine des réseaux informatiques. Ce qui a mobilisé la communauté dans les projets de recherche sur les réseaux programmables, dont un des sujets est l'objet de cette étude : SDN - Réseaux Informatiques Définis par Logiciel. SDN est un nouveau paradigme créé pour adapter les infrastructures courantes aux enjeux de la communication actuelle : une plus haute bande passante et les exigences des applications modernes. SDN propose une nouvelle architecture plus dynamique, facile à gérer, rentable et flexible. Cette architecture sépare le plan de contrôle (intelligence et état du réseau) du plan de données (fonctions de transmission). L'approche permet de rendre le contrôle directement programmable avec l'infrastructure sous-jacente abstraite aux applications réseaux et services.

Mots clés : SDN, Réseaux Programmables, Plan de Contrôle, Plan de Données

Abstract

New technologies and concepts appear in response to new network and internet usage requirements. Such as Big Data for massive data processing and Cloud Computing for resources hosting management. Similar evolution is expected for the computer networks. As result the research community has produced many works on programmable networks. Among them, the subject of this study : SDN - Software Defined Networking. SDN is a new paradigm designed to adapt current infrastructures to the issues of the recent communication : increasingly need for high speed and the exigences of modern applications. SDN proposes a new architecture plus dynamic, ease to manage, profitable and flexibile. This architecture decouples the control plane (network intelligence and state) from the data plane (transmission functions). This approach makes de the control directly programmable and causes the underlying infrastructure to be abstracted to network applications and services.

Keywords : SDN, Programmable Networks, Control Plane, Data Plane