Réseau du futur – Architectures agiles

Virtualisation des réseaux

Introduction

Un réseau de communications électroniques est composé de nombreux éléments distincts ayant une fonction spécifique : les routeurs permettent l'acheminement du trafic, les pare-feux permettent la mise en place d'un cloisonnement entre les différentes parties d'un réseau, etc. Historiquement, chacune de ces fonctions était assurée par des équipements physiques différents. Le concept de virtualisation qui consiste à séparer le logiciel du matériel, déjà très éprouvé dans le monde de l'informatique classique, engendre aujourd'hui deux révolutions dans le monde des télécoms :

- la capacité de dissocier le matériel du logiciel pour les équipements réseaux : plusieurs fonctions réseau peuvent par exemple s'exécuter de manière indépendante sur un même matériel générique. Les fonctions réseau peuvent également migrer d'un matériel à un autre. On parle de NFV (pour « *Network Function Virtualization*») ;
- la capacité de configurer les équipements réseau à la volée en fonction des besoins de l'application/service au moyen d'un « contrôleur de réseau ». On parle de SDN (« *Software Defined Networks* »).

Ainsi, NFV vise à rendre polyvalents les équipements physiques utilisés en leur permettant de multiplier les fonctions qu'ils peuvent remplir (chaque fonction devenant un logiciel plutôt qu'un équipement physique propre) ; SDN vise pour sa part à rendre programmables l'acheminement et le traitement de flux. Ces deux concepts sont disjoints mais se développent concomitamment, la disponibilité de fonctions réseau virtualisé offrant une grande souplesse en matière de configuration du réseau et d'orchestration.

Il est aisé de concevoir le gain en termes d'efficacité de gestion que l'adoption de ces deux concepts peut engendrer pour un exploitant de réseau. Ce dernier peut par ailleurs espérer réduire ses coûts fixes en s'approvisionnant, en lieu et place d'équipements spécifiques, avec des équipements génériques sur lesquels s'exécuteront des fonctions logicielles. Ces apports potentiels sont toutefois à tempérer par le fait que de nouveaux coûts sont à considérer ; récurrents ou ponctuels, ceux-ci sont liés à l'exploitation de licences logicielles et leur intégration, ou à la requalification du personnel exploitant ces nouvelles technologies.

Il est enfin indéniable que ces technologies auront un effet sur les modèles économiques des opérateurs (du côté des coûts par exemple, en réduisant ceux d'investissement et en augmentant ceux d'exploitation) et des équipementiers télécoms (en augmentant par symétrie la proportion de revenus récurrents, et en favorisant la commercialisation par ces derniers de nouveaux services ou *a contrario* en les forçant à partager leurs marchés traditionnels avec d'autres acteurs du monde l'informatique). De nouvelles offres pourraient également voir le jour : un opérateur pourrait ainsi proposer à des tiers (opérateurs ou clients entreprise) l'hébergement de fonctions propres sur son réseau, voire un réseau virtualisé complet, cœur de réseau compris, clé en main. Le recours aux technologies logicielles et aux composants pourrait par ailleurs favoriser l'entrée de nouveaux acteurs sur toute la chaîne de valeur (nouveaux opérateurs, nouveaux équipementiers, nouveaux types d'acteurs *pure players* du logiciel etc.) et favoriser un repositionnement des acteurs établis dans la chaîne de valeur. L'apparition de ces technologies présente de nombreux défis et interroge la façon dont sont conçus, opérés, et réglementés les réseaux aujourd'hui :

- comment exploiter au mieux le potentiel de ces technologies au bénéfice de l'innovation et de la concurrence, tout en préservant les capacités industrielles nationales?

- comment assurer un niveau de sécurité adéquat alors que des fonctions historiquement disjointes sont amenées à être co-localisées au sein d'un même équipement ?
- comment assurer le respect des principes liés à la neutralité du net au sein d'un réseau à la capacité de reconfiguration quasi-infinie en temps réel ?
- la réglementation actuelle (notamment les obligations légales des opérateurs) est-elle *future-proof* ou au contraire doit-elle être adaptée pour tenir compte de ces évolutions ?
- les efforts actuels en matière de standardisation sont-ils suffisants pour garantir que l'intégration de ces nouvelles technologies ne conduise pas à une certaine forme d'enfermement technologique ?

La présente note, fruit d'un premier cycle d'auditions, détaille ces questions afin de permettre l'identification des enjeux qui devront faire l'objet d'une analyse plus approfondie.

1 La virtualisation des réseaux (NFV) et les réseaux logiciels (SDN)

1.1 Présentation des technologies et des possibilités offertes

1.1.1 La virtualisation des réseaux (NFV) : la polyvalence des équipements physiques

Un réseau de communications électroniques est constitué de plusieurs éléments ayant chacun une fonction bien particulière, parmi lesquels se trouvent des équipements en charge du contrôle d'accès au réseau, des pare-feux, des routeurs, des passerelles qui permettent l'interfaçage entre domaines distincts, des plateformes de service, des bases de données etc[1]. Pour la plupart et historiquement, ces fonctions sont intrinsèquement indissociables de l'équipement (*hardware*) sur lequel elles sont exécutées ; ce couplage fait que l'équipement et sa fonction sont vendus comme un unique produit intégré par les équipementiers. La virtualisation des fonctions des réseaux (« Network Function Virtualisation » ou NFV) brise ce couplage, en s'appuyant sur des solutions matures originaires du monde de l'informatique (technologies de l'IT) depuis la démocratisation du Cloud Computing. L'analogie peut être faite avec les smartphones qui regroupent les fonctions de plusieurs équipements : un seul objet peut remplir différentes fonctions telles que celles d'un téléphone, d'un appareil photo, d'une console de jeux, ou d'un podomètre, car elles sont réalisées par des logiciels[2]. En découplant les fonctions (logicielles) de l'équipement de son support matériel (hardware), la virtualisation permet d'acquérir indépendamment ces logiciels et de les installer sur des serveurs informatiques banalisés. Ces serveurs de grande capacité sont répartis sur quelques points de présence de l'opérateur[3] (« data-centers »).
Le concept du NFV a été introduit en 2012 dans un Livre Blanc co-signé par 13 opérateurs, synthétisant les avantages de la virtualisation et invitant l'industrie à le développer pour le cadre des opérateurs télécoms. L'ETSI (European Telecommunications Standards Institute), à travers un groupe de travail dédié, a publié les spécifications d'un cadre commun permettant la mise en œuvre de la virtualisation des réseaux (cf. annexe 1 pour plus de détails sur la structure du NFV) dans un environnement multi-vendeurs[4].

---

[1] Dans les réseaux non-virtualisés actuels, un seul équipement peut parfois supporter plusieurs fonctions distinctes : par exemple, un CPE (« Customer-Premises Equipement ») est un routeur placé chez l'utilisateur (par exemple une entreprise) qui embarque également une fonction de pare-feu et des fonctions de qualité de service. Toutefois, la configuration demeure spécifique, rigide et difficilement reconfigurable à la volée.

[2] Dans certains cas, il a néanmoins été nécessaire d'ajouter de nouveaux composants au smartphone pour qu'il remplisse cette fonction (par exemple, un capteur photo).

[3] L'architecture typique fait apparaitre généralement un grand site principal (dans un rôle centralisateur) interconnecté en très haut débit à quelques sites secondaires plus excentrés.

[4] L'adoption d'un cadre commun vise à s'affranchir des spécificités du modèle de chaque fournisseur et à permettre à l'utilisateur de cette technologie (ici les opérateurs) de s'outiller auprès de plusieurs vendeurs sur la même plateforme.

1.1.2 Les réseaux logiciels (SDN) : la programmation de l'acheminement du trafic

L'architecture d'un réseau est constituée d'un ensemble de liens et de nœuds interconnectés au moyen de routeurs distribués. Pour réaliser l'acheminement d'un flux de trafic entre deux points du réseau, les routeurs exécutent deux fonctions distinctes : signalisation (activation des algorithmes de routage) et transport (acheminement du trafic ou « forwarding »).

- La fonction de routage a pour objet de calculer, de sélectionner, d'établir et de maintenir le ou les chemins (également appelées routes) permettant d'acheminer le trafic entre des points du réseau. Elle mobilise un effort de de calcul important afin d'établir la topologie du réseau et de calculer à chaque instant la route optimale au regard de critère(s) (appelé métrique de coût) tel que la minimisation du nombre de routeurs traversés ou le délai d'acheminement (appelé latence).
- La fonction de transport (« forwarding ») a pour objet l'acheminement effectif des flux de trafic en aiguillant, au niveau de chaque nœud du réseau, les données (appelée paquets) reçues via les interfaces d'entrée du routeur vers les interfaces de sortie appropriées du routeur, conformément à une table, dite table d'acheminement, alimentée par la fonction de routage.

Parallèlement au développement de la virtualisation des réseaux, se développent les réseaux programmés par logiciel (« Software-Defined Networks » ou « SDN ») qui permettent de relâcher, voire de s'affranchir de ces contraintes en programmant et en personnalisant par voie logicielle les règles d'acheminement de trafic (cf. annexe 2 pour plus de détails). Il y a donc séparation de la signalisation (intelligence) et de l'acheminement du trafic. En centralisant ainsi le pilotage du réseau (i.e. le calcul des routes, le réajustement des routes, l'instruction de règles de traitement spécifique selon les exigences du service) au niveau d'une intelligence de calcul logiquement centralisée (appelé le « contrôleur SDN ») et en distribuant l'intelligence (notamment, la connaissance topologique du voisinage), il devient possible de déployer une infrastructure composée de routeurs qui deviennent essentiellement des exécutants en charge d'acheminer le trafic. Ainsi le paradigme d'un réseau SDN se rapproche du concept de réseaux superposés (« overlay networks »).

Le pilotage en SDN étant centralisé, les administrateurs réseau peuvent répondre rapidement à l'évolution des besoins grâce à la remontée d'information (qui elle est décentralisée), en simplifiant l'allocation des ressources en fonction de la demande ; ils peuvent aussi facilement réorganiser le réseau (par exemple pour créer des réseaux privés virtuels, ou pour modifier automatiquement les politiques de routage en fonction du service utilisé). Cette centralisation de la prise de décision couplée à la décentralisation de l'intelligence rend la conception et le fonctionnement du réseau plus flexible et à terme moins coûteux.

1.2 Vers une « informatisation » du modèle technique traditionnel des télécoms

1.2.1 Combiner SDN et NFV permettrait une fertilisation croisée entre les deux technologies

Les technologies NFV et SDN se sont développées en parallèle et font partie d'une même transformation générale de l'industrie des télécommunications s'inspirant des mutations du domaine de l'informatique. NFV vise à rendre polyvalents les équipements physiques utilisés en leur permettant de multiplier les fonctions qu'ils peuvent remplir (chaque fonction devenant un logiciel plutôt qu'un équipement physique propre) ; SDN vise pour sa part à rendre programmables l'acheminement et le traitement de flux. Les deux technologies confèrent ainsi davantage de flexibilité et d'agilité opérationnelle et permettent aux opérateurs d'aller encore plus facilement au-delà de la simple fourniture de connectivité, en développant la fourniture de services. Au-delà des apports spécifiques de chacune de ces technologies, leur combinaison ouvre le champ à un enrichissement mutuel. En effet, une mise en œuvre efficace des principes du NFV suppose l'établissement automatique et flexible de réseaux virtuels reliant les différentes fonctions

virtualisées, ce qui peut être fourni par un contrôleur SDN[5]. Inversement, établir les règles d'acheminement des flux via un contrôleur SDN nécessite des fonctions de réseau dont la réalisation sous une forme virtualisée pourrait apporter des avantages indéniables en termes de disponibilité, de flexibilité et de tenue en charge. Ainsi il est attendu qu'utilisateurs et développeurs de ces deux technologies cherchent à promouvoir leur combinaison.

1.2.2 Les effets de la virtualisation sur la qualité de service dans le cadre des télécoms

Le concept NFV tel que développé par l'ETSI définit un cadre architectural pour penser la virtualisation des fonctions de réseau ; néanmoins, il n'a pas vocation à spécifier les moyens techniques sollicités pour le mettre en œuvre.

La mise en œuvre de ces fonctions réseaux virtualisées[6] peut être fait selon deux principales modalités techniques de virtualisation informatique, détaillées en annexe 1, chacune d'entre elles présentant des avantages et des inconvénients.

Dans un cas, une certaine latence est introduite, qui peut s'avérer incompatible avec des fonctions réseau ayant des contraintes strictes en latence, empêchant donc l'exploitation de ces fonctions à la volée.

Dans l'autre cas, la latence sera plus faiblement impactée, mais ce sont cette fois des risques liés à la volatilité qui sont susceptibles d'apparaitre, c'est-à-dire une traçabilité plus complexe, un risque de défaillance plus distribué, une difficulté à orchestrer l'ensemble, etc.

Toutefois, quelle que soit la méthode de mise en œuvre de virtualisation retenue, le réseau pourra bénéficier d'un certain gain de fiabilité dans la mesure où le remplacement d'une fonction par une autre sera rendu relativement plus simple pour l'administrateur dans un modèle virtualisé, puisque, grâce à l'orchestrateur[7], les équipements défaillants sont presque immédiatement remplacés par d'autres équipements virtualisés en tous points identiques.

2 Ecosystème et chaîne de valeur

La virtualisation est susceptible d'avoir des effets importants sur les modèles d'affaire des équipementiers et des opérateurs.

2.1 Impact sur le marché des équipementiers

Pour les équipementiers, trois développements majeurs sont à anticiper du fait de la virtualisation : la modification des compétences métier, le changement de modèle économique (glissement vers des recettes variables plutôt que fixes), et l'importance croissante que le service après-vente est susceptible de prendre.

- De nombreux logiciels utilisés pour la virtualisation sont disponibles en *open-source* sous forme de composants logiciels qu'il est nécessaire d'assembler pour créer un équipement réseau virtualisé complet. Cependant, l'assemblage de ces composants, qui ne sont pas nécessairement optimisés pour fonctionner ensemble, requiert des compétences particulières.

[5] Cette piste est notamment explorée par l'ETSI. Cf. ETSI GS NFV-EVE 005 V1.1.1 (2015-12): Network Functions Virtualization (NFV) Ecosystem; Report on SDN Usage in NFV Architectural Framework.

[6] « Virtual Network Function » ou VNF.

[7] Cf. annexe 1

- Certains équipementiers disposent de l'expertise nécessaire pour réaliser un tel assemblage et proposent des licences payantes « tout-en-un », permettant de déployer facilement des équipements réseau virtualisés sur du matériel générique. Ces licences doivent le plus souvent être périodiquement renouvelées. Cette approche impacte directement le modèle d'affaire des équipementiers et leur profil de revenu avec une diminution prévisible des revenus fixes et une augmentation des revenus variables.
- Que ce soit dans le cadre des offres « tout-en-un » ou des offres centrées sur les seuls équipements physique supports de la virtualisation, les équipementiers peuvent par ailleurs se démarquer en proposant de réaliser eux-mêmes l'intégration des différents équipements virtualisés et en fournissant des garanties (support et maintenance) avec une valeur ajoutée plus importante par rapport à ce qu'ils font actuellement avec leurs équipements dédiés du fait de l'accroissement de l'enjeu de l'intégration que pose l'éclatement et la multiplicité des fonctions virtualisées. À ce titre, certains acteurs du monde de l'informatique disposent d'une expertise dans ce domaine et sont susceptibles d'entrer en concurrence avec les équipementiers traditionnels. Ainsi, certains spécialistes de la virtualisation (comme VMWare) ont développé des versions « premium » et optimisées de leurs logiciels pour bénéficier des avantages de la virtualisation (flexibilité, mutualisation) tout en atténuant les inconvénients (diminution des performances, fiabilité amoindrie) qui y sont inhérentes (cf.1.2.2). Par ailleurs, les fournisseurs de cloud, disposent eux aussi d'une expertise en virtualisation et des ressources informatiques importantes et disposent aussi des compétences réseaux nécessaires au transport de larges volumes de données en un temps réduit.

2.2 Impact sur les opérateurs télécom

2.2.1 Impacts financiers

La virtualisation des réseaux permettra probablement de réaliser des gains financiers à terme. Toutefois l'ampleur et l'horizon de ces gains restent incertains et dépendants des situations propres et des scenarii retenus.

Les fournisseurs de solutions virtualisées estiment que la virtualisation permettra des gains considérables. Ainsi, selon une étude ACG de 2015[8], la virtualisation pourrait permettre à un opérateur de réduire jusqu'à 2/3 de ses coûts d'investissement et d'exploitation liés aux équipements réseaux.

Cette estimation semble cependant maximaliste ; il convient de relativiser ces chiffres, étant donné que la partie virtualisable des réseaux ne représenterait, selon certains experts, que 25% du CAPEX annuel d'un opérateur mobile, les autres 75% concernant principalement des coûts provenant de l'investissement dans les sites radio et du foncier.

En outre, si le coût d'achat de l'équipement physique devrait diminuer significativement grâce à la virtualisation, le coût du logiciel utilisé pour mettre en œuvre la virtualisation est susceptible de varier fortement. Certains opérateurs pourraient intégrer les solutions *open-source* directement, mais ceux ne disposant pas des compétences ou de la ressource suffisante pour gérer l'intégration et l'adaptation de ces solutions, pourront préférer recourir à des licences d'équipementier afin de bénéficier de logiciels optimisés et plus facilement intégrables.

Dans les deux cas, on observerait un glissement d'un modèle de coûts fixes vers un modèle de coûts variables, qu'ils soient liés à une masse salariale plus qualifiée et chargée de traiter l'intégration et l'adaptation des briques logicielles dans le cas d'un recours à des solutions *open-source*, ou au

[8] Etude financée par VMWare, "Total Cost of Ownership Study Virtualizing the Mobile Core" https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/vmware-nfv-tco-report-acg.pdf

paiement de licences dans le cas du recours aux solutions propriétaires payantes. La question du gain financier global peut alors se poser. À titre d'exemple, dans le cas d'un routeur virtualisé, au coût classique d'entretien d'un équipement s'ajouteraient donc des licences de logiciels dont les prix publics et à l'unité (et qui peuvent donc être différents de ceux pratiquées pour les opérateurs) varieraient autour de 8 000$[9] par an[10]. À titre de comparaison, l'achat d'un équipement équivalent non virtualisé coûterait environ 35 000$[11] et ne nécessite pas de licence ; en fonction de la durée de vie relative des deux appareils, les économies de coûts d'investissement pourraient donc être compensées par le coût des licences. De plus, dans certains cas, il serait nécessaire de déployer plusieurs machines virtuelles pour fournir des performances similaires à celles d'un équipement dédié. Sur le moyen terme, les gains ne seront donc pas à la hauteur des prévisions d'ACG.

Si une voie intermédiaire serait de combiner l'intégration de logiciels *open-source* et des licences achetées aux équipementiers afin de réduire les coûts, en pratique cette approche pourrait potentiellement faire perdre aux opérateurs les garanties que les équipementiers leur offrent. Aussi, pour suivre cette voie, les opérateurs pourraient être amenés à séparer, voire isoler, les machines virtuelles fournies par les équipementiers et les autres machines virtuelles.

Plus généralement, la transition vers les réseaux virtualisés peut engendrer des coûts cachés, notamment en termes de formation ou, dans certaines configurations, de consommation énergétique, même dans le cas d'un recours à des solutions propriétaires payantes.

2.2.2 Impacts opérationnels

En termes opérationnels, la virtualisation pourrait engendrer trois principaux défis pour les opérateurs : la requalification de leurs équipes, une possible dégradation de leur qualité de service, et la redéfinition des responsabilités contractuelles en cas de panne sur le réseau.

- Dans le monde de l'informatique, un ingénieur réseau peut administrer un grand nombre de machines (par exemple en moyenne 30 000 machines chez Google), alors que, chez les opérateurs, les ingénieurs administrent actuellement une centaine de machines ; au-delà du nombre de machines à gérer, la nature de ces machines est également très différente. Les opérateurs devront donc requalifier certains de leurs effectifs en administrateurs de réseaux virtualisés ; or, plusieurs experts ont souligné le fait que la formation de ces administrateurs n'est proposée par aucun cursus en France. La virtualisation du réseau des opérateurs passera donc par une période durant laquelle les opérateurs devront monter en compétence sur cette nouvelle technologie tout en gérant le parc non virtualisé. Si les opérateurs parviennent à acquérir les compétences nécessaires, certains pourraient chercher à développer eux-mêmes des logiciels de réseaux virtualisés afin d'être moins dépendants des équipementiers (c'est notamment une stratégie adoptée par AT&T[12]). Cela nécessiterait là encore un investissement significatif en termes de formation, mais cela leur permettrait d'une part de ne plus avoir à payer de licences, et d'autre part de développer des fonctions qui leurs seraient propres.
- De plus, la virtualisation pourrait poser question en termes d'effet sur la qualité de service des opérateurs (en termes de latence, de disponibilité ou de volatilité, selon le choix technologique retenu — cf. section 1.2.2). La question de l'ampleur de ces effets négatifs de la virtualisation sur la qualité de service est toutefois centrale pour déterminer si ceux-ci

[9] Source : ITprice.com

[10] Coûts pour un routeur 10Gbps, au-delà de ce débit, la consommation électrique serait trop importante sur les équipements virtualisés.

[11] Source : http://itprice.com/cisco-gpl/1000v?p=

[12] «Hitting the Open Road: Software-Accelerating Our Network with Open Source », http://about.att.com/innovationblog/061714hittingtheopen

seront négligeables ou s'ils pourraient avoir un véritable impact sur la gestion opérationnelle des réseaux.

- Enfin, la virtualisation pose un problème nouveau concernant les responsabilités contractuelles. En effet, auparavant, pour les équipements dédiés (*switches, firewalls*…), l'équipementier était généralement le seul responsable contractuellement en cas de problème. Avec la virtualisation des fonctions de réseau, qui deviennent donc des applications s'exécutant sur des serveurs génériques, l'identification d'un responsable en cas de panne peut s'avérer difficile : est-ce l'opérateur lui-même, l'équipementier[13], l'intégrateur, ou l'éditeur de logiciels ? Les garanties offertes par les équipementiers autoriseront-elles des configurations combinant des logiciels sous licences et des composants *open-source* directement intégrés?

2.2.3 Impacts sur la fourniture de services

Grâce à la virtualisation, il sera possible, sur un même réseau physique, de créer des tranches de réseaux cloisonnées (« *network slicing* »), par exemple pour proposer des offres différenciées en terme de QoS à ses utilisateurs.

La virtualisation permet également aux opérateurs de partager avec des tiers (autre opérateur, utilisateur, entreprise, verticaux etc.) l'accès à leurs infrastructures réseau (cf. section 1.2.2) pour héberger des fonctions virtualisés, ces fonctions pouvant être fournies par l'opérateur (sous forme de catalogue) ou par les utilisateurs eux-mêmes comme par exemple des fonctions de pilotage ou monitoring de machines nécessaires à certaines industries ou cas d'usage pour verticaux (voiture connectée, smart city etc.).

Dans un scénario d'ouverture plus avancée, l'opérateur pourrait également techniquement offrir la possibilité à ses clients d'opérer leurs propres réseaux virtuels sur sa plateforme, soit en conservant une certaine maîtrise de l'intelligence de la plateforme (orchestration, contrôle, vision de bout-en-bout…), soit en se désengageant complètement de l'intelligence et en se confinant à un rôle d'opérateur d'infrastructure. Un fabriquant de terminal (par exemple un constructeur de voitures connectées) pourrait ainsi gérer son propre réseau virtuel et y fournir les services associés.

Plusieurs opérateurs prévoient déjà de monétiser l'accès à certains équipements de leurs réseaux.

2.2.4 Impacts concurrentiels

La virtualisation pourrait permettre à de nouveaux opérateurs de lancer leur activité en s'appuyant sur un réseau entièrement virtualisé sans détenir d'infrastructures physiques en propre. Ces nouveaux opérateurs pourraient avoir des positionnements différents (marchés de niche ou marchés de masse) et des périmètres d'activités différents (opérateurs locaux, nationaux ou transnationaux).

En effet, un nouvel opérateur pourrait minimiser son investissement d'entrée en recourant à des solutions de cloud, ce qui réduirait son coût d'investissement. De plus, la gestion d'un réseau virtualisé nécessite des équipements différents et des effectifs humains avec une formation particulière. Les nouveaux entrants, qui pourraient directement recruter les profils et déployer les équipements les plus adéquats, pourraient donc bénéficier d'un avantage comparatif.

L'entrée sur les marchés des télécommunications pourrait donc être facilitée, notamment pour des acteurs disposant d'une expertise dans la virtualisation et le cloud, qui ne sont actuellement pas des acteurs présents sur ce marché ; ainsi, le paysage concurrentiel des télécommunications pourrait être profondément modifié.

[13] Par exemple, en 2008, l'opérateur danois TDC a signé un partenariat stratégique avec l'équipementier Ericsson pour opérer et gérer son réseau afin d'accélérer la commercialisation de la 4G. Il n'est pas exclu qu'avec la virtualisation et les impacts opérationnels sur le métier de l'opérateur, de tels types de partenariats deviennent de plus en plus courants.

Toutefois, si la virtualisation permet de simuler un réseau physique sans avoir besoin d'en être propriétaire, la nécessité d'obtenir un accord d'accès auprès de détenteurs d'infrastructures physiques demeure. Le degré d'accessibilité et la souplesse offerte par les détenteurs d'infrastructures physiques pourrait constituer un frein à ce développement. L'émergence de nouvelles offres grâce à la virtualisation, notamment d'offres transnationales, dépendra également du niveau d'homogénéisation des modalités d'accès.

3 Identification des problématiques et des enjeux pouvant mériter un focus dédié

3.1 Interopérabilité

Les technologies SDN et NFV permettent des architectures réseau fonctionnant grâce à plusieurs briques logicielles indépendantes et personnalisables. Ces briques peuvent être disponibles en *open-source*, ou développées en interne par certains des acteurs évoqués en section 2. Il serait souhaitable que ces « briques » puissent être utilisées sur la majorité des environnements, des infrastructures, et pouvoir communiquer entre elles : il s'agit d'une problématique d'interopérabilité.

Cet enjeu d'interopérabilité peut être appréhendé à deux niveaux : d'une part à l'intérieur d'un même réseau, et d'un autre part à la frontière de réseaux distincts (interconnexion).

- Au niveau d'un même réseau, l'interopérabilité entre les différentes composantes d'une architecture réseau reposant sur le SDN et la virtualisation permettrait d'éviter des inefficacités (par exemple, le fait de devoir « personnaliser » une application réseau pour chaque socle de virtualisation). Ainsi, assurer cette interopérabilité, permettrait aux opérateurs d'acquérir des fonctions réseaux et les déployer dans leur infrastructure avec un minimum d'adaptation, ce qui leur permettra d'en réduire le délai et les coûts de mise en œuvre.
- Au niveau de la frontière entre réseaux distincts, l'interopérabilité sera nécessaire pour assurer une interconnexion de ces réseaux et garantir ainsi une qualité de service de bout en bout. Un point de vigilance concerne l'interopérabilité entre différents domaines SDN, notamment en ce qui concerne l'interopérabilité des différents orchestrateurs, qui ne fait pour l'instant objet d'aucune normalisation.

La programmabilité du réseau via des APIs et l'orchestration des fonctions virtualisées nécessitent la modélisation des configurations des équipements et des services réseaux virtualisés[14]. Cela a des conséquences pour les architectes réseaux qui doivent désormais modéliser ces services.

Des travaux de standardisation, menés notamment par l'industrie – par exemple au sein de l'ETSI ou d'organisations/consortiums ad-hoc[15] – et le monde de l'open-source pourraient aider à répondre, techniquement parlant, à cette problématique d'interopérabilité. Pour garantir cette interopérabilité, il conviendra que les différentes organisations convergent, autant que possible, vers des standards communs ou, *a minima*, compatibles.

[14] Le langage de modélisation de données YANG (« Yet Another Next Generation », crée par un groupe de travail de l'IETF) est un exemple de langage de modélisation de ces configurations permettant de spécifier un modèle de service (en décrivant ses composants, ses interactions internes et externes, ses exigences et ses capacités) qui sera utilisé par l'orchestrateur/le contrôleur SDN mais également vis-à-vis à des tiers (exposition de ce service via des APIs).

[15] Par exemple TIP (Telecommunication Infrastructure Project) consortium initié par Facebook, ou ONF (Open Network Foundation) consortium non lucratif initié par les opérateurs, des académiques et des acteurs OTT.

3.2 Accès des tiers aux infrastructures physiques : enjeux d'innovation, de concurrence et de préservation des capacités industrielles

Comme vu en section 2.2.3, la virtualisation offre un spectre de possibilités techniques pour les tiers sur les infrastructures ou plateformes des opérateurs.

Le degré d'exploitation de ce potentiel technique dépendra in fine du degré d'ouverture de l'opérateur vis-à-vis des tiers, qui peut aller de la simple proposition de catalogue de services virtualisés instanciés par l'opérateur lui-même jusqu'au cas où l'opérateur permet aux tiers qui le souhaitent l'instanciation et l'orchestration de leurs fonctions virtualisées.

Se pose donc la question des règles d'accès aux infrastructures physiques et du degré d'exposition des interfaces de programmation applicatives (API ou « Application Programming Interface ») aux tiers afin qu'ils puissent héberger leurs fonctions virtualisées ou paramétrer leur réseau virtualisé. Par ailleurs, la question des API pose une problématique concurrentielle dans le cas où un protocole ou une API seraient favorisés par des acteurs, de manière à exclure ceux qui ne les utiliseraient pas.

Plus largement, la modification (ou non) des règles d'accès pourrait avoir des effets sur la dynamique concurrentielle et sur l'incitation à l'innovation. La question de la préservation des capacités industrielles des acteurs nationaux pourra également se poser.

3.3 Neutralité de l'Internet et qualité de service différenciée

Comme vu précédemment, la virtualisation permet de mettre en œuvre le *network slicing*. Pour chaque *slice*, il est possible de configurer spécifiquement plusieurs paramètres de qualité de service dont bénéficieront les flux transportés. En outre, dans un réseau, le recours au SDN centralise et simplifie le paramétrage de la qualité de service pour chaque réseau, ce qui pourrait permettre de définir plus facilement des traitements spécifiques par type de flux.

Se pose alors la question de la conformité de ces fonctions au cadre réglementaire relatif à la neutralité de l'internet, ainsi que les modalités de contrôle du respect de cette obligation.

Dans ce contexte, le BEREC n'identifie pas à ce jour[16] le *network slicing* comme une atteinte à la neutralité du net en tant que tel, dès lors qu'il est utilisé conformément aux possibilités de différenciation de qualité de service autorisées par le règlement européen sur l'internet ouvert (pour des services dits « spécialisés » par exemple, ou pour des pratiques de gestion de trafic raisonnables)[17]. Le BEREC précise par ailleurs qu'il revient aux autorités de régulation de déterminer au cas par cas si un service répond aux dispositions de l'article 3(5) du règlement internet ouvert, qui précise dans quelles conditions il est possible de proposer des optimisations pour les services spécialisés avec un niveau de qualité spécifique.

Pour contrôler les politiques de qualité de service implémentées au sein d'un réseau ayant recours au SDN, une première piste, relativement complexe à mettre en œuvre, pourrait être la consultation des fichiers de configuration au niveau du contrôleur et de l'orchestrateur, ainsi que la consultation des journaux d'événements réseau. Plus largement, se pose une problématique d'accès aux informations relatives au réseau pour des fins de contrôle du respect des obligations.

[16] Un groupe de travail concernant la mise à jour des lignes directrices du BEREC sur la neutralité du net a été mis en place pour l'année 2019.

[17] « According to BEREC's current understanding and analysis, the Regulation seems to be leaving considerable room for the implementation of 5G technologies, such as network slicing, 5QI and Mobile Edge Computing. To date, BEREC is not aware of any concrete example given by stakeholders where the implementation of 5G technology as such would be impeded by the Regulation.» https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/8317-berec-opinion-for-the-evaluation-of-the-application-of-regulation-eu-20152120-and-the-berec-net-neutrality-guidelines

3.4 Sécurité

Les technologies SDN et NFV soulèvent quatre problématiques en termes de sécurité : création d'un point unique de défaillance due à la centralisation du contrôle des fonctions de réseau (« single point of failure », SPOF), nécessité de garantir l'étanchéité entre applications, augmentation des surfaces d'attaques, hétérogénéité des configurations.

- La centralisation du contrôle des fonctions de réseau constitue une vulnérabilité pour toute l'architecture : si cet élément est rendu indisponible ou dysfonctionnel, il n'est plus possible de gérer les réseaux dépendants de ce contrôleur (configuration, politique de routage…). Pour limiter le risque lié à la centralisation, il est possible de redonder les éléments critiques du réseau de manière à le rendre plus robuste. La virtualisation facilite le déploiement d'équipements redondés. Il s'agit plus particulièrement d'une problématique de robustesse et de fiabilité du réseau.
- La mutualisation des infrastructures permise par la virtualisation permet d'exécuter en parallèle des applications différentes sur une même machine physique : si les conditions de sécurité permettant de garantir l'étanchéité entre les applications s'exécutant simultanément ne sont pas réunies, alors l'effectivité de la mutualisation et les gains attendus pourraient être limités par la nécessité de n'exécuter chacune des fonctions réseaux les plus critiques qu'isolément.
- Ces architectures se composent de plusieurs briques logicielles indépendantes, qui peuvent devoir communiquer entre elles : la multiplication des canaux de communication peut constituer une augmentation de la surface d'attaque et aboutir à d'éventuelles vulnérabilités supplémentaires.
- Les architectures NFV entraînent une très grande liberté dans la configuration des briques qui constituent le réseau. Cette liberté engendre d'une part une multiplication des sources d'erreurs potentielles et d'autre part une grande hétérogénéité des configurations, et donc une complexification de l'analyse de sécurité. Le nombre d'intervenants impliqués dans la configuration du réseau peut par ailleurs engendrer une dilution des responsabilités.

A contrario, il est possible que le recours au SDN permette une meilleure maîtrise des configurations et favorise la modification rapide de celles-ci. L'élaboration d'un cadre sécurisé propice au développement de la virtualisation fait partie des actions de l'ANSSI, identifiée notamment dans la revue stratégique de cybersécurité publiée en février 2018.

3.5 Souveraineté

La virtualisation des réseaux soulève deux enjeux au regard de la maitrise de la souveraineté nationale : d'une part, l'obligation pour les opérateurs de localiser sur le territoire national certaines de leur activités et, d'autre part, l'obligation de soumettre à autorisation l'exploitation de certains dispositifs techniques.

- La virtualisation permet aux opérateurs de s'affranchir des contraintes géographiques pour la réalisation de certaines fonctions relevant du cœur de réseaux, de son exploitation ou de sa supervision. Ainsi certains opérateurs français pourraient choisir de réaliser certaines de ces activités en dehors du territoire national, soit pour des raisons de coût, soit pour les mutualiser avec les activités similaires de filiales ou de sociétés sœurs exerçant dans d'autres pays. Or, la réglementation prévoit spécifiquement que certaines activités, notamment la mise en place et la mise en œuvre des moyens nécessaires aux interceptions de correspondances[18], aient lieu sur le territoire national. La délocalisation de certaines fonctions à l'étranger, facilitée par la virtualisation, peut également avoir un impact sur la capacité de l'Etat à mettre en œuvre ses

[18] Article D. 98-7 III du CPCE

capacités en matière de détection de cyberattaques ou de réaction en cas de crise. Le fait que des fonctions historiquement internalisées par les opérateurs puissent être externalisées auprès de fournisseurs externes peut également avoir des impacts en termes de souveraineté lorsque, par exemple, ces acteurs sont assujettis à des réglementations étrangères (par exemple le Cloud Act[19]).

- Dans le cadre juridique actuel[20], les dispositifs techniques de nature à permettre les interceptions sont soumis à autorisation du Premier ministre. Or, dès lors que des fonctions réseaux, soumises au régime d'autorisation susmentionné, sont virtualisées, se pose la question de savoir précisément quels éléments doivent obtenir cette autorisation. S'agit-il uniquement de la fonction virtualisée en elle-même ou faut-il également obtenir une autorisation pour l'infrastructure du cloud, machines physiques et systèmes d'exploitation, susceptible d'exécuter les fonctions virtualisées pour lesquelles une autorisation est requise ?

La prise en compte de ces contraintes régaliennes par les opérateurs, voire de leurs évolutions, sont déterminantes pour leur permettre de définir précisément la place que devra prendre la virtualisation dans leurs futurs réseaux et, par conséquent, les gains qu'ils pourront en retirer.

Là encore, ces questions de souveraineté relèvent davantage des compétences notamment du Gouvernement (ANSSI et SGDSN entre autres).

[19] https://www.congress.gov/bill/115th-congress/senate-bill/2383/text

[20] *C.f.* L'article R.226-3 du code pénal et l'arrêté du 11 août 2016 modifiant l'arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal.

Annexe 1

Spécifications historiques de la virtualisation

Le concept du NFV a été introduit en 2012 dans un Livre Blanc[21] co-signé par 13 opérateurs, synthétisant les avantages de la virtualisation et invitant l'industrie à le développer pour le cadre des opérateurs télécoms. L'ETSI (*European Telecommunications Standards Institute*), à travers un groupe de travail dédié, a publié les spécifications d'un modèle permettant la mise en œuvre de la virtualisation des réseaux dans un environnement multi-vendeurs. Dans sa version simplifiée, le modèle NFV de l'ETSI est structuré autour de 3 blocs principaux :

- l'infrastructure NFV, une infrastructure générique sous forme de serveurs, commutateurs, base de données etc. et agnostique par rapport aux applications qu'elle supporte ;
- les fonctions réseaux virtualisées (« Virtual Network Function » ou VNF), qui en s'inspirant des avancées de la mise en œuvre de la virtualisation dans le domaine de l'IT, sont instanciées à la volée sur l'infrastructure NFV ;
- l'« orchestrateur » ou « contrôleur » (« *Management and Orchestration* » ou MANO), qui prend en charge le contrôle et la gestion de ces VNF (gestion de cycle de vie, contrôle de leur élasticité, choix du serveur physique sur lequel exécuter tel ou tel VNF etc.). L'orchestrateur pilote le comportement des VNF à travers une série de descripteurs (fichiers spécifiques) fournis par le vendeur, contenant leurs caractéristiques, des instructions décrivant les ressources matérielles requises pour les déployer à travers le VIM (« Virtual Infrastructure Manager ») (type et débit de connectivité interne/externe, capacité de calcul/stockage etc.) et les conditions contraignant leur assemblage avec d'autres VNF. En somme, l'orchestrateur demeure le garant d'une composition et d'une orchestration des VNF à travers une vision du service de bout en bout.

Les premières propositions de mise en œuvre de VNF se basent sur des machines virtuelles, ou « *virtual machines* » (VM) ; il s'agit de partitions de la ressource physique (l'infrastructure) cloisonnées par une couche logicielle spécifique où chaque machine virtuelle embarque le logiciel de la fonction réseau à virtualiser. Grâce à ce partitionnement, il est possible de permettre à plusieurs opérateurs de contrôler des machines virtuelles qui sont déployées sur une même machine physique. Néanmoins, ces machines virtuelles intègrent leurs propres systèmes d'exploitation et ne permettent généralement pas un accès direct à la ressource physique. Ces contraintes font que les machines virtuelles sont légèrement moins réactives que les machines physiques qu'elles émulent. Si cette légère latence causée par la virtualisation n'est pas problématique dans l'usage d'un ordinateur classique, elle est incompatible avec certaines fonctions réseau requérant des contraintes strictes de latence et empêche donc d'exploiter ces fonctions à la volée. Ainsi des propositions alternatives plaident pour l'utilisation de « conteneurs », une variante miniature de la machine virtuelle qui s'appuie sur une isolation moins étanche entre la machine virtuelle et l'infrastructure physique. Les conteneurs sont plus réactifs que les machines virtuelles et leur usage est plus mature dans l'industrie des plateformes cloud à base de web-services[22] et de micro-services (Cloud natif), mais aussi plus volatiles[23].

---

[21] *Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action*. White Paper publié au la conférence "*SDN and Openflow World Congress*" (2012)

[22] Ce sont les briques de base constituant des applications de type Facebook, les messageries Gmail, applications Amazon etc.

[23] La volatilité est liée à la granularité d'un container. Contrairement à une machine virtuelle, le container est un micro composant, ce qui induit des risques spécifiques : traçabilité plus complexe, risque de défaillance plus distribué, complexité pour coordonner et orchestrer l'ensemble etc.

Annexe 2

SDN

Pour réaliser leurs fonctions de routage des flux de trafic, les routeurs mobilisent un effort de signalisation et un calcul important (notamment pour la découverte des équipements voisins, le calcul de la route optimale, l'exécution de certaines tâches spécifiques (comme l'inspection des paquets, le filtrage, le partage de charge etc.) intégrées aux tâches standards d'acheminement et de transfert des paquets) et requièrent souvent une programmation statique des règles de gestion de trafic. Les réseaux programmés par logiciel (SDN) permettent de relâcher voire de s'affranchir de ces contraintes en programmant et en personnalisant par voie logicielle les règles de routage et de gestion de trafic en fonction des contraintes/objectifs du service.

Cette programmation par voie logicielle est possible grâce à la dissociation de la couche de transmission/traitement de flux de données (« Data Flow ») et de la couche de contrôle/signalisation (« Controle Plane ») habituellement intégrée dans le même équipement. Cette séparation a été d'abord formulée par une recommandation de l'ITU-T puis théorisée par l'ONF[24] en 2014 à travers un modèle architectural en 3 couches distinctes qui interagissent à travers des interfaces de programmation applicative (API[25]): la couche logicielle (comprenant les applications de l'utilisateur final qui utilisent le réseau SDN), la couche de contrôle (fournissant la fonction de contrôle centralisée qui supervise et agit sur le comportement de transfert de réseau, elle se matérialise sous forme de « contrôleur SDN ») et la couche infrastructure (comprenant l'ensemble des équipements de réseau en charge d'exécuter les commandes de commutation et de transfert des paquets telles que instruites par le contrôleur SDN).

SDN permet de gérer le plan de transfert à partir d'un contrôleur logiquement centralisé, ce qui rend les opérations et la gestion du réseau très flexibles. L'architecture en couches avec des API bien documentées entre les couches fournit une indépendance par rapport aux fournisseurs, évitant ainsi de verrouiller l'opérateur de réseau dans une logique (technique et donc commerciale) spécifique à un équipementier.

[24] Open Network Foundation (ONF), SDN Architecture (06/2014)

[25] Application Programming Interface (API) qui joue le rôle de façade clairement délimitée permettant à une entité logicielle de communiquer avec une autre entité. Développées massivement dans le monde de l'informatique pour faciliter la création d'applications ou de services logiciels, les API sont mises en œuvre souvent sous forme de bibliothèques logicielles (développées en Open Source ou propriétaires) et présentent l'intérêt de masquer par l'abstraction les éléments techniques spécifiques au fonctionnement interne de l'entité et ainsi jouer un rôle clef pour favoriser l'interopérabilité.

Annexe 3

Bibliographie

- ETSI, *Network Functions Virtualisation: Introductory white paper*
  https://portal.etsi.org/nfv/nfv_white_paper.pdf
  https://www.etsi.org/technologies/nfv
- AT&T, *AT&T Vision Alignment Challenge Technology Survey, AT&T Domain 2.0 Vision White Paper*, November 13, 2013.
- Martin Taylor, *The application of Cloud Native design principles to network function virtualization*, Metaswitch.
- Bruno Chatras, *La virtualisation des fonctions de réseaux de télécommunication*, Revue Telecom n°181, mai 2017.
- 5G-PPP Software Network Working Group, *From Webscale to Telco, the Cloud Native Journey*, Cloud Native White Paper, July 2018
- Commission Européenne, *Implications of the emerging technologies Software-Defined Networking and Network Function Virtualisation on the future Telecommunications Landscape (SMART 2005/0011)*, 2016

  http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=44557
- ORECE, *Input paper on Potential Regulatory Implications of Software-Defined Networking and Network Functions Virtualisation (BoR (16) 97)*, 2016

  https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6088-input-paper-on-potential-regulatory-impl_0.pdf
- IDATE Digiworld Research, *Virtualization in Telco Networks: which markets for SDN and NFV, and what perspectives with netowork slicing for 5G?*, September 2017
- *SDN and NFV Simplified: A visual guide to understanding Software Defined Networks and Network Function Virtualization*", Jim Doherty, 2016 Pearson Education.
- Diego Kreutz, Fernando M. V. Ramos, Paulo Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky, Steve Uhlig, *Software-Defined Networking: A Comprehensive Survey,* IEEE Surveys & Tutorials on communications.