Les réseaux virtualisés : promesses et enjeux

Par Fabrice GUILLEMIN
Orange

Les technologies de virtualisation ont révolutionné ces dernières années les réseaux de télécommunications. Au-delà des avancées techniques et de la très grande flexibilité apportée, cette rupture dans la conception des réseaux pose de nombreux défis, en particulier vis-à-vis des infrastructures sous-jacentes, le *cloud* notamment, et l'exploitation des réseaux. Cet article vise à faire le point sur des sujets sensibles pour les opérateurs de réseaux et à identifier des solutions possibles.

Virtualisation des réseaux

Les technologies de virtualisation des systèmes informatiques ont révolutionné l'architecture des réseaux de télécommunications en dissociant le *software* du *hardware* d'hébergement. Cette transformation permet de rendre les réseaux programmables, avec des versions logicielles mises à jour en continu. Les fonctions réseau sont particulièrement adaptées à cette approche, donnant naissance au concept de virtualisation des fonctions réseau (Network Function Virtualisation, NFV), initialement développé par l'ETSI [1]. L'application de NFV à l'ensemble des fonctions réseau (contrôle, transfert, routage, commutation) a mené à l'émergence des réseaux définis par le logiciel. Le concept de SDN (*Software Defined Networks*) se concentre sur la programmation du plan de transfert *via* le protocole *OpenFlow* [2].

L'approche NFV s'applique à des fonctions aussi variées que les *firewalls* ou les cœurs de réseau mobile, qui comportent eux-mêmes de nombreux composants logiciels interagissant entre eux, comme le cœur de réseau 5G. Pour augmenter la flexibilité de l'approche NFV, il est possible de décomposer les fonctions ou leurs composants en des entités plus petites, chacune réalisant une tâche élémentaire. Cette méthode, empruntée au monde informatique et correspondant à l'approche dite par microservices, est particulièrement pertinente pour les réseaux.

Dans ce contexte de NFV, les microservices sont généralement hébergés par des conteneurs, dans des infrastructures *cloud* gérées par des outils spécialisés. Kubernetes (K8S) [3] est couramment utilisé pour gérer des conteneurs, bien que des méthodes manuelles (comme Docker Compose) soient aussi possibles. L'avantage de Kubernetes réside dans son ensemble d'outils facilitant l'automatisation du déploiement de conteneurs sur des *clusters* de serveurs. Il permet en outre le redimensionnement automatique des conteneurs selon l'activité des microservices (*autoscaling*).

La combinaison de la virtualisation des fonctions réseau et de la décomposition en microservices hébergés dans des conteneurs gérés par Kubernetes représente l'approche *cloud* native, qui semble actuellement la mieux adaptée aux réseaux. Développée notamment par Google, cette approche permet de déployer et modifier les microservices en continu grâce à une chaîne d'intégration et de développement continu (CI/CD). Les projets logiciels développant les fonctions réseau archivent majoritairement le code sur des réper-

toires Git et ceux-ci peuvent être utilisés pour déployer automatiquement les fonctions *via* GitOps [4]. Ce dernier forme un cadre opérationnel basé sur les bonnes pratiques de DevOps en étendant l'approche *Infrastructure/Network as Code* (I/NaC), qui automatise le déploiement des infrastructures IT à partir de fichiers de configuration.

Ces différentes approches visent à rendre les réseaux plus flexibles et dynamiques, automatisant le déploiement et la mise à jour des fonctions réseau virtualisées, tout en permettant une gestion autonome des microservices et la reconfiguration des réseaux. Toutefois, elles bouleversent les pratiques traditionnelles des opérateurs, qui privilégient des mises à jour par paliers fonctionnels, une validation avant déploiement et une gestion majoritairement manuelle. Les constructeurs traditionnels, qui développent des fonctions réseau optimisées sur du *hardware* spécifique, doivent également s'adapter pour rendre les fonctions agnostiques au *hardware*. Cela soulève des défis opérationnels, de compétences et de conception, nécessitant une attention particulière à l'infrastructure *cloud* qui supporte ces nouvelles technologies.

Infrastructures *cloud*

Dans la transformation des réseaux en systèmes entièrement logiciels et dynamiques, l'infrastructure *cloud* joue un rôle crucial. Au début de NFV, les machines virtuelles (VM) étaient privilégiées, mais elles se sont rapidement révélées moins performantes que la technologie de conteneurisation, plus légère et plus facile à déployer. Bien que l'hébergement de *clusters* K8S dans des VM soit possible et offre une isolation supérieure comparée à une implémentation directe sur le système d'exploitation d'un serveur (solution dite *bare metal*), il est maintenant communément admis que l'infrastructure *cloud* la plus adaptée pour les réseaux logiciels devrait reposer sur des *clusters* K8S.

Pour les fonctions de contrôle qui n'ont pas d'exigences de temps réel strictes, comme les fonctions de contrôle (authentification, bases de données clients, etc.), les *clouds* centralisés suffisent. Il est courant de voir des déploiements de réseaux mobiles privés utilisant les *clouds* d'Amazon, de Microsoft ou de Google. Cependant, certaines fonctions du plan de transfert des données avec des contraintes fortes en termes de débit et de latence doivent être implantées au plus près des utilisateurs, en particulier la passerelle vers Internet. En raison du manque de standardisation entre les plans de contrôle et de données, certaines fonctions de ces derniers sont souvent colocalisées dans des implémentations commerciales ou *open source*, telles que Magma.

Outre les fonctions du cœur de réseau, celles du réseau d'accès sont également candidates à la virtualisation. L'Alliance Open RAN (ORAN) travaille à la désagrégation des unités de traitement radio (BBU) en différentes fonctions : CU (*Centralized Unit*), DU (*Distributed Unit*) et RU (*Remote Unit*) [6]. Les fonctions de contrôle radio (CU) sont clairement éligibles à la virtualisation, tandis que les DU, qui traitent le codage et le *scheduling* radio, nécessitent des capacités de calcul plus importantes. Les RU sont encore principalement implémentées sur des FPGA[1] dédiés. La virtualisation des fonctions CU et DU, regroupées dans des *clouds* communs pour des raisons énergétiques et de gestion de trafic, s'inscrit dans l'approche *cloudRAN*.

Cette tendance à virtualiser certaines fonctions du plan de transfert conduit au déploiement d'infrastructures *cloud* en bordure de réseau, appelées *edge cloud*. Ce terme est interprété différemment selon les acteurs : les GAFAM l'utilisent pour désigner des data centers régionaux à leur échelle mondiale, tandis que les opérateurs nationaux l'associent à des *data centers* régionaux au sein d'un même pays. Pour ces derniers, la

[1] *Field-programmable gate array* : matrice de portes programmables. Voir par exemple : https://www.futura-sciences.com/tech/definitions/technologie-fpga-8700/

virtualisation du réseau d'accès et de certaines fonctions du cœur de réseau nécessite le déploiement de *data centers* à travers tout un pays, notamment pour les fonctions CU et UPF, voire plus proches des antennes (à une centaine de kilomètres) pour les DU, qui peuvent nécessiter des accélérations *hardware* ou des GPUs.

La virtualisation des fonctions réseau représente donc un investissement considérable pour les opérateurs, déjà soumis à la pression des GAFAM qui maîtrisent les technologies du *cloud* et ont acquis des *start-up*s spécialisées dans les fonctions réseau. Investir massivement dans une infrastructure *cloud* distribuée pose un défi stratégique majeur pour les opérateurs. Pour rentabiliser cet investissement, ils doivent trouver des applications nécessitant un déploiement en bordure de réseau et générant des revenus substantiels. Cependant, la latence d'un réseau national, qui est de l'ordre de quelques dizaines de millisecondes, est compatible avec la plupart des applications actuelles, y compris les jeux et l'intelligence artificielle. Une politique de *peering* adéquate avec les acteurs OTT pourrait être une solution économique pour offrir des applications sensibles à la latence. Ces acteurs supporteraient les coûts d'investissement, mais bénéficieraient des revenus directs ou indirects des applications.

Cette situation rend la problématique du *edge cloud* complexe pour les opérateurs de réseau nationaux. Les causes de latence pour les applications sont souvent localisées dans les zones radio (cellulaires et wifi), et le déploiement de data centers très proches des utilisateurs n'améliore la latence que marginalement. Cependant, le traitement de grandes quantités de données, comme les flux vidéo de télésurveillance nécessitant des débits d'*upload* élevés, peut représenter un cas d'usage intéressant pour le *edge cloud*. Le problème est de trouver une équation économique équilibrée pour les opérateurs.

Pour conclure, la virtualisation des fonctions réseau soulève des préoccupations en matière de sécurité, notamment vis-à-vis des données sensibles des utilisateurs. L'hébergement de ces fonctions dans des *clouds* publics comme GCP ou AWS pose des problèmes de confidentialité des données (RGPD en Europe). Si ce problème peut être non critique dans un environnement privé, comme un réseau privé d'une multinationale, il devient beaucoup plus préoccupant dans le contexte des réseaux de télécommunications publics. Les recommandations actuelles de l'ANSSI n'autorisent pas ce genre de déploiement. Pour surmonter ce problème, il est nécessaire de développer une solution de *cloud* maîtrisé par l'opérateur de réseau (*cf.* le projet Sylva [7]).

Orchestration

Un défi connexe à la virtualisation des réseaux et à la capacité de créer un grand nombre de réseaux virtualisés sur un même substrat est la manière d'orchestrer ces déploiements. L'orchestration se distingue de l'automatisation, cette dernière visant à automatiser des tâches auparavant manuelles, tandis que l'orchestration coordonne et organise différents déploiements pour atteindre des objectifs globaux d'optimisation pour l'infrastructure (par exemple, taux d'occupation des serveurs, utilisation des liens de transmission) et pour les réseaux virtuels déployés (par exemple, latence, taux de perte de paquets).

Les outils d'orchestration intègrent des bibliothèques de fonctions à déployer, des interfaces de commande (interface « nord »), des inventaires, des modules de collecte de données et d'optimisation, et parfois des méthodes pour définir des règles métier permettant de déployer des boucles autonomes de contrôle. La plateforme ONAP (Open Network Automation Platform) a été conçue dans cette optique, offrant une vue holistique sur tous les segments du réseau (réseaux d'accès, de transport, de cœur et l'infrastructure *cloud*) [8]. ONAP comprend tous les modules nécessaires pour optimiser à la fois le substrat (infrastructures *cloud*, réseaux de transport et de routage sous-jacents) et les réseaux virtuels déployés. Les techniques d'intelligence artificielle se révèlent en particulier très efficaces pour résoudre les problèmes d'optimisation associés [9].

Cependant, concevoir une plateforme unique globale est difficile et conduit à des solutions lourdes à déployer et à maintenir. De plus, chaque composante du réseau tend à développer ses propres plateformes d'orchestration, en particulier les plateformes *cloud* avec K8S et l'automatisation *via* GitOps. Étant donné que les réseaux sont naturellement répartis géographiquement, par exemple avec des réseaux d'accès (RAN) et cœurs virtualisés, il est nécessaire d'avoir des versions de K8S *multi-cluster* pour déployer un réseau virtualisé de manière cohérente. Plusieurs projets, comme Nephio, travaillent sur des versions de K8S *multi-cluster*.

En dehors des aspects relevant du *cloud*, différents segments du réseau développent également leurs propres plateformes d'orchestration. Par exemple, les RIC (*RAN Intelligent Controller*) d'ORAN (temps réel et non temps réel) visent à orchestrer et optimiser les réseaux d'accès radio. Les fonctions réseau virtualisées, comme les cœurs de réseau, sont également conçues avec leurs propres fonctions d'orchestration, même si celles-ci sont le plus souvent des plateformes d'administration propres à la fonction. L'orchestration de bout en bout se limite alors à coordonner les différents orchestrateurs pour déployer des réseaux virtuels de bout en bout, sachant que certaines tâches nécessitent de toute façon des tâches manuelles, ne serait-ce que l'installation d'antennes radio pour déployer un réseau radio. L'architecture *Open Digital Architecture* (ODA) du TM Forum [10] modélise les différentes parties d'un réseau et les tâches d'orchestration associées. Néanmoins, une orchestration cohérente de bout en bout reste encore aujourd'hui un défi majeur pour les opérateurs. Une multitude de sociétés apparaissent pour assurer l'intégration du code et opérer des outils pour orchestrer les réseaux de bout en bout.

Conclusion

Au-delà des promesses apportées par les technologies de virtualisation pour les réseaux de télécommunications, celles-ci bouleversent totalement l'écosystème et le métier des opérateurs de réseau s'en trouve totalement modifié. Après la vague d'enthousiasme soulevée à leur émergence rapide, la maîtrise opérationnelle de ces technologies reste en grande partie à consolider, surtout pour les opérateurs de réseau historiques. L'écosystème industriel est lui-même en continuelle transformation pour essayer de trouver un point d'équilibre sur ces technologies.

Sur le marché grand public, les opérateurs classiques restent les mieux placés par leur proximité avec les clients ; la virtualisation et toutes les techniques du *cloud* peuvent leur apporter beaucoup de flexibilité même si la maîtrise globale reste un défi majeur, surtout vis-à-vis de l'intégration de très gros logiciels. Sur le marché des réseaux privés cependant, la tension avec les GAFAM risque de s'accroître étant donné qu'ils se sont donné les moyens d'offrir des solutions performantes aux clients professionnels. Les opérateurs de réseau peuvent néanmoins utiliser la proximité et de l'assistance qu'ils apportent à leurs clients pour rester dans la chaîne de valeur.

Références

[1] YI B., XINGWEI W., LI K., DAS S. K. & HUANG M. (2018), "A comprehensive survey of Network Function Virtualization", *Computer Networks*, vol. 133, pp. 212-262.

[2] XIA W., WEN Y., FOH C. H., NIYATO D. & XIE H. (2015), "A Survey on Software-Defined Networking", in IEEE Communications Surveys & Tutorials, vol. 17, n°1, pp. 27-51.

[3] BURNS B., GRANT B., OPPENHEIMER D., BREWER E. & WILKES J. (2016), "Borg, Omega, and Kubernetes", *ACM Queue*, vol. 14, pp. 70-93.

[4] BEETZ F. & HARRER S. (2022), "GitOps: The evolution of DevOps?", *IEEE Software*, 39(4), IEEE Computer Society Press, https://doi.org/10.1109/MS.2021.3119106

[5] RIVERA D., MORENO J., SANZ RODRIGO M., LOPEZ D. & MOZO A. (2023), "Providing heterogeneous signaling and user traffic for 5G core network functional testing", *IEEE Access*, vol. 11, pp. 2968-2980.

[6] POLESE M., BONATI L., D'ORO S., BASAGNI S. & MELODIA T. (2023), "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges", *IEEE Communications Surveys and Tutorials*, 25(2).

[7] https://sylvaproject.org/

[8] SLIM F., GUILLEMIN F., GRAVEY A. & HADJADJ-AOUL Y. (2017), "Towards a dynamic adaptive placement of virtual network functions under ONAP", 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Berlin, Germany, pp. 210-215.

[9] ALVES ESTEVES J. J., BOUBENDIR A., GUILLEMIN F. & SENS P. (2022), "A heuristically assisted deep reinforcement learning approach for network slice placement" in *IEEE Transactions on Network and Service Management*, vol. 19, n°4, pp. 4794-4806.

[10] https://www.tmforum.org/oda/