PUJOLLE

LES RÉSEAUX

9e ÉDITION

L'ère des réseaux cloud et de la 5G

EYROLLES

LA RÉFÉRENCE DES ÉTUDIANTS ET DES PROFESSIONNELS EN RÉSEAUX ET TÉLÉCOMS

Avec plus de 100 000 exemplaires vendus, *Les Réseaux* de Guy Pujolle s'est imposé comme la référence en langue française auprès des étudiants comme des professionnels en réseaux et télécoms.
Très largement refondue et mise à jour, cette neuvième édition témoigne des évolutions rapides des technologies et des usages. Alors que certaines technologies comme la téléphonie sur IP ou la 4G sont arrivées à maturité et sont largement déployées, le monde des réseaux vit de nouveaux bouleversements :

– généralisation du Cloud et du Fog Networking, avec le remplacement des boîtiers de type routeur ou commutateur par des machines virtuelles s'exécutant dans des datacenters ;
– montée en puissance de l'architecture SDN qui va à l'encontre de la philosophie Internet en (re)centralisant les fonctions de routage ;
– succès croissant des logiciels open source au détriment des solutions propriétaires des grands équipementiers ;
– transition de la 4G vers la 5G, un des grands chantiers de ces prochaines années.

Au sommaire

Éléments de base. Introduction aux réseaux • Les composants des réseaux • Réseaux virtuels et Cloud • L'intelligence dans les réseaux. **Les protocoles réseau.** Niveau physique • Niveau trame • Niveaux paquet et message. **Les solutions réseau.** Réseaux optiques • Ethernet • Réseaux IP • MPLS et GMPLS • Réseaux SDN • Cloud Networking • Réseaux open source (OPNFV, OpenStack…). Réseaux d'accès. Réseaux d'accès terrestres (fibre optique, ADSL…) • Réseaux d'accès hertziens • Small cells et réseaux multisaut. **Réseaux de mobiles et sans fil.** Réseaux 1G à 5G • Réseaux personnels : Bluetooth, UWB, ZigBee, LiFi… • Réseaux Wi-Fi (IEEE 802.11n, 802.11ac, 802.11af…) • Internet des objets. **Contrôle, gestion, sécurité et énergie.** VLAN et VPN • Gestion et contrôle • Sécurité et identité • Réseaux Green (stratégies de réduction de la consommation énergétique). **Générations futures** (réseaux participatifs, concrétisation, réseaux morphware, pilotage automatique, blockchain).

En complément sur www.editions-eyrolles.com

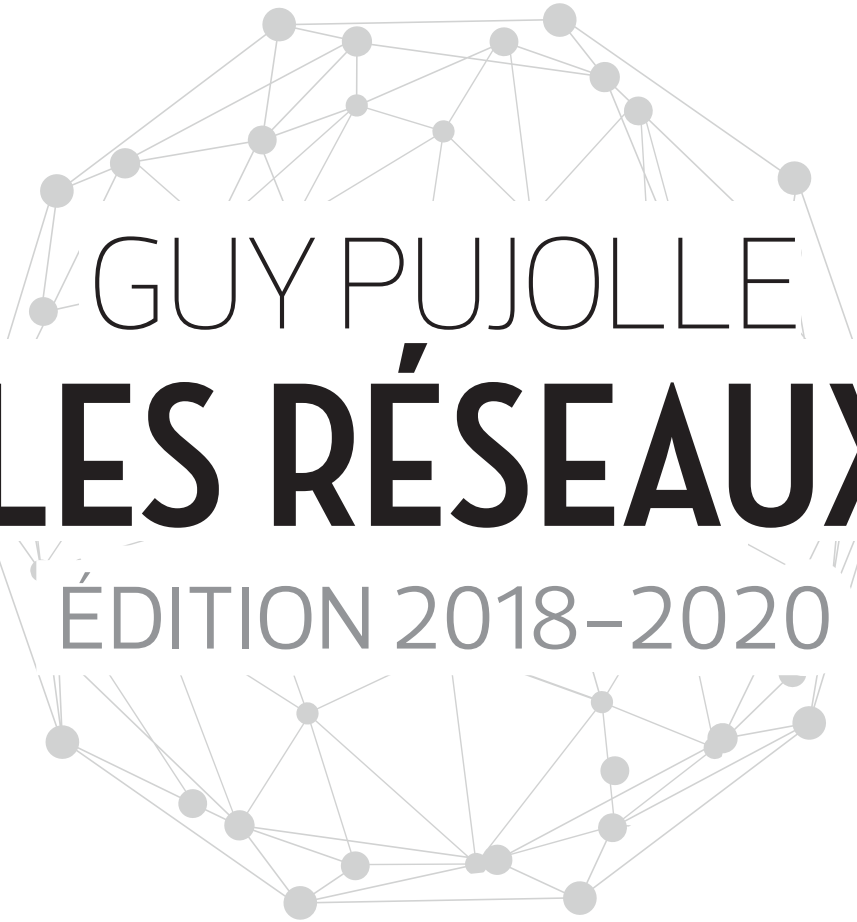
Plus de 450 pages d'annexes à télécharger : bases de traitement du signal, modèles théoriques, technologies en perte de vitesse (X.25, relais de trame, ATM, WiMAX, gestion par politiques…), compléments techniques (IEEE 802.11e, VPN IP, protocoles EAP…), bibliographie mise à jour.

L'AUTEUR

Guy Pujolle est professeur à Sorbonne Université et responsable de nombreux grands projets de recherche français et européens. Il a été professeur invité à NCSU, Stanford, Rutgers, UQAM, Postech et UFRJ. Ses recherches portent actuellement sur la conception et le développement des réseaux des années 2020.
Il est cofondateur de la société QoSMOS, spécialisée dans la qualité de service, de la société Ucopia qui commercialise un logiciel de marketing intelligent, d'EtherTrust qui propose de la haute sécurité par carte à puce et de Green Communications qui divise par deux à dix la consommation électrique des réseaux d'accès sans fil.

LES RÉSEAUX

ÉDITION 2018–2020



GUY PUJOLLE

LES RÉSEAUX

ÉDITION 2018-2020

9e édition

Avec la collaboration de Olivier Salvatori

EYROLLES

Groupe Eyrolles
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

ISBN : 978-2-212-67535-1

Préface à la 9e édition

Les réseaux composent la structure de base du septième continent qui se forme sous nos yeux. Par l'immense séisme que ce continent supplémentaire engendre en cette première partie du siècle, la planète entre dans une ère nouvelle. Ce continent est celui de la communication. Constitué de réseaux se parcourant à la vitesse de la lumière, il représente une rupture analogue à l'apparition de l'écriture ou à la grande révolution industrielle.

Ces réseaux, qui innervent aujourd'hui complètement la planète, s'appuient sur la fibre optique, les ondes hertziennes et divers équipements qui permettent d'atteindre de très hauts débits. Internet incarne la principale architecture de ces communications.

Les réseaux forment un domaine tellement complexe qu'il est impossible d'en rendre compte de façon exhaustive, et ce livre pas plus que les autres, n'en a la prétention. Simplement, il vise à faire comprendre, de manière à la fois technique et pédagogique, les fondements des réseaux en en dressant un panorama aussi complet que possible.

Les refontes apportées à cette neuvième édition sont encore plus importantes que les précédentes. La raison en est simple : le monde des réseaux connaît une révolution étonnante de prime abord. Au lieu de continuer son évolution vers un système de plus en plus distribué, il tend à se recentraliser. Mais ce système, dont la tendance actuelle est au regroupement autour de contrôleurs virtuels dans de très grands datacenters, devrait redevenir distribué d'ici à quelques années, ce que nous verrons plus clairement dans la prochaine édition de ce livre.

Parmi les autres changements importants détaillés dans la présente édition, la 5G qui se profile sera capable de prendre en charge des missions critiques telles que le contrôle des véhicules autonomes, la connexion de milliards d'objets, l'introduction des très hauts débits en mobilité et, bien sûr, le SDN (Software-Defined Networking), qui apporte la centralisation permettant d'introduire beaucoup plus d'intelligence dans les réseaux.

Un autre axe de développement important introduit dans cette édition concerne les logiciels libres, puisque les réseaux devraient avoir rejoint le monde de l'open source vers les années 2020.

Les annexes de cette édition disponibles sur le Web représentent un volume d'informations presque aussi important que l'édition elle-même.

Au total, près d'un tiers du livre est constitué d'éléments totalement neufs, tandis qu'un autre bon quart a été fortement remanié.

Nous recommandons au lecteur d'effectuer la lecture des vingt-six chapitres qui suivent en continuité. Sa construction en six parties permet toutefois de le parcourir aussi par centre d'intérêt.

Il est important de noter que les références bibliographiques, les annexes et toutes sortes d'informations qui viendraient à enrichir le contenu de l'ouvrage sont désormais accessibles sur la page dédiée au livre du site des Éditions Eyrolles (*www.editions-eyrolles.com*). L'avantage de cette solution est de permettre la mise à jour en continu des références bibliographiques, qui jouent un rôle important dans un monde aussi vivant. De même, si certaines annexes n'ont que peu de raisons de changer, de nouvelles annexes devraient apparaître régulièrement pour informer les lecteurs des grandes directions du monde des réseaux.

Cette neuvième édition n'aurait pu exister sans les huit premières et sans l'aide précieuse, depuis 1995, de collègues et de plusieurs générations d'étudiants. Je suis heureux de remercier ici un grand nombre d'entre eux ayant terminé leur thèse depuis plus ou moins longtemps pour leur aide précieuse sur des sujets arides et des collègues plus expérimentés pour leurs apports de qualité.

Table des matières

PARTIE II

PARTIE III

CHAPITRE 10

CHAPITRE 11

Partie VI

Partie I

Les éléments de base des réseaux

Les réseaux ont pour fonction de transporter des informations afin de réaliser des services pouvant se trouver n'importe où sur le globe. Une série d'équipements matériels et de processus logiciels sont mis en œuvre pour assurer ce transport, depuis les câbles terrestres ou les ondes radio dans lesquels circulent les données jusqu'aux protocoles et règles permettant de les traiter.

Cette première partie de l'ouvrage rappelle les principes de fonctionnement des réseaux et présente en détail les matériels, logiciels et architectures protocolaires sur lesquels ils se fondent.

1

Introduction aux réseaux

Les réseaux sont nés du besoin de transporter des données d'un ordinateur à un autre ordinateur. Ces données étant mises sous la forme de fichiers, l'application de base des réseaux s'est appelée le transfert de fichiers. Un peu plus tard, le « transactionnel » est apparu pour permettre à un utilisateur de réaliser des transactions avec un ordinateur distant, par exemple pour réserver une place d'avion. On a appelé session l'ensemble des transactions d'un même utilisateur pour réaliser une tâche donnée.

Avec le développement du Web, le service transactionnel s'est diversifié afin de permettre la recherche d'informations par le biais de liens. Ces applications se sont appelées client-serveur, c'est-à-dire qu'un client s'adresse à un serveur pour obtenir de l'information.

L'étape suivante des réseaux a été caractérisée par le pair-à-pair, ou P2P (*peer-to-peer*), dans lequel tous les éléments connectés au réseau sont équivalents et peuvent être distribués dans le réseau. Les applications sous-jacentes sont en fait très nombreuses, allant de la téléphonie à la recherche d'informations diverses et variées, telles les fichiers audio ou vidéo sur Internet.

Sans supplanter les applications de transfert de fichiers, qu'elles soient client-serveur ou pair-à-pair, le nouveau service Internet qui se développe depuis les années 2010 est le *Cloud*, ou « nuage ». Jusqu'à l'arrivée des Clouds, Internet avait pour objectif de transporter des données pour réaliser un service à distance. Les entreprises permettaient par exemple aux employés itinérants de se connecter à leurs serveurs par le biais d'Internet. Elles possédaient pour cela tous les éléments nécessaires, comme la messagerie électronique, les applications métier ou les serveurs d'archivage, ainsi que la puissance de calcul requise. Aujourd'hui, il est possible de réaliser dans le Cloud ce qui se faisait auparavant au sein de l'entreprise : calcul, stockage, application métier, messagerie, téléphonie, etc. Les avantages sont nombreux : le client peut accéder à ces services de n'importe où ; ceux-ci peuvent être sécurisés par de la redondance ; il est possible d'ajouter instantanément de

nouveaux services, de la puissance de calcul, de l'espace de stockage, etc., en fonction des besoins et en ne payant que ce qui est utilisé.

Cette nouvelle génération met en œuvre le concept de virtualisation, par lequel les ressources dont l'entreprise ou le particulier a besoin peuvent se trouver n'importe où, voire se déplacer en fonction du coût des serveurs.

Avant de détailler plus avant ces nouvelles générations de réseaux, les sections qui suivent rappellent quelques éléments clés de l'évolution des réseaux et des architectures actuelles.

Le paquet

L'entité de base des réseaux est le paquet. Celui-ci rassemble des éléments binaires, suites de 0 et de 1 correspondant à des données provenant de différents types d'informations, comme la parole et la vidéo, ou bien de stockages, de calculs et d'applications. Les paquets contiennent en général entre quelques octets (8 bits) de ces éléments binaires et 1 500 octets.

L'objectif des réseaux est de transporter les paquets provenant d'un utilisateur, d'une machine, d'un objet ou de tout ce qui peut produire de l'information. En d'autres termes, un émetteur crée des paquets et les envoie jusqu'à un récepteur. Comme il n'y a que peu de chance qu'il existe une ligne directe entre l'émetteur et le récepteur, les paquets traversent des nœuds intermédiaires qui les transfèrent vers le nœud suivant et ainsi de suite jusqu'au récepteur.

Ce livre détaille les différentes façons d'effectuer le transport des paquets d'un émetteur à un récepteur, telles que suivre toujours un même chemin, représenté par une succession de nœuds intermédiaires, ou emprunter des routes différentes en fonction de la nature des paquets à transporter.

La première solution consiste à marquer un chemin (*path*) et à y envoyer les paquets. Les paquets se suivent et arrivent dans l'ordre de leur émission. Dans ce cas, même s'il s'avère qu'un autre chemin est plus court ou demande moins de temps, les paquets restent sur le chemin qui a été ouvert tant que celui-ci satisfait à la qualité de service exigée par l'émetteur. Cette solution de chemin a donné naissance à la technique dite de commutation (*switching*), dans laquelle les nœuds s'appellent des commutateurs (*switches*).

La seconde grande solution est celle du routage (*routing*), dans laquelle les paquets sont routés vers un nœud qui peut changer dans le temps en fonction de l'état du réseau et en essayant à tout instant de prendre la route la plus courte. Le nœud qui effectue l'aiguillage est appelé un routeur. Il possède pour cela une table de routage. Dans ce cas, les paquets peuvent arriver dans le désordre au récepteur.

Les nœuds qui transfèrent les paquets d'une ligne d'entrée vers une ligne de sortie sont appelés des nœuds de transfert (*forwarding nodes*). Ils ont longtemps été constitués d'éléments matériels, avec peu de logiciel à l'intérieur pour gérer le passage des paquets et détecter, par exemple, des anomalies. Dans la nouvelle génération de nœuds de transfert qui est en phase d'installation, les nœuds physiques sont remplacés par des nœuds logiciels, aussi appelés nœuds virtuels.

Passer d'une architecture matérielle à une architecture logicielle est assez simple. Il suffit d'écrire un code dans un langage déterminé afin de décrire et réaliser ce que fait une machine matérielle. Ce code est appelé machine virtuelle, ou VM (Virtual Machine).

Pour exécuter des machines virtuelles, une infrastructure matérielle est évidemment nécessaire. Celle-ci doit disposer de suffisamment de puissance de calcul pour offrir le même rendement qu'un nœud de transfert matériel. Une telle puissance n'est disponible que dans des datacenters, ou centres de données, qui regroupent un grand nombre de serveurs.

La nouvelle génération de réseaux qui se met en place aujourd'hui se caractérise par l'ensemble de ces éléments : des datacenters qui intègrent des nœuds de transfert et qui sont interconnectés par des liaisons à très haut débit, en général en fibre optique. La suite du chapitre décrit les environnements qui se déploient dans ces datacenters : le Cloud pour les plus gros d'entre eux, le MEC (Mobile Edge Computing) pour ceux de taille moyenne, le Fog pour les petits et le Skin pour les très petits.

Cloud, MEC, Fog et Skin

Un Cloud est rendu possible par l'exploitation par un réseau de la puissance de calcul et de stockage d'un datacenter. En d'autres termes, c'est l'ensemble des machines virtuelles déployées dans un ou plusieurs datacenters en vue de répondre aux besoins des utilisateurs. Les machines virtuelles, ou VM, peuvent être rangées dans trois grandes catégories : les VM de stockage, les VM de calcul et les VM réseau. On peut leur ajouter deux nouveaux types de machines apparues sur le marché en 2017 : les VM de sécurité et les VM de gestion et de contrôle.

Une VM de calcul est un ensemble matériel et logiciel agrégeant la puissance de calcul d'un ou plusieurs processeurs et de la mémoire afin de réaliser des calculs qui peuvent se révéler extrêmement importants. Une VM de stockage est essentiellement constituée d'un ensemble de mémoires permettant de stocker des données. Une VM réseau est un équipement réseau virtuel, comme un routeur ou un commutateur virtuel, qui est stocké dans la mémoire d'un datacenter et dispose ainsi de la puissance de calcul associée, laquelle peut varier dans le temps. Une VM de sécurité peut agir en tant que serveur d'authentification virtuel ou pare-feu virtuel afin de gérer la sécurité de clients, de machines ou d'objets. Enfin, une VM de gestion et de contrôle peut faire office de contrôleur ou d'orchestrateur virtuel afin de contrôler des flots de paquets ou de mettre en place un ensemble de machines virtuelles pour déployer un service.

Le Cloud bénéficie généralement de la puissance de stockage et de calcul d'un gros datacenter, possédant plusieurs centaines ou milliers de serveurs, voire jusqu'à un million de serveurs, rassemblés au même endroit. La tendance actuelle consiste toutefois à installer ces datacenters au plus près de l'utilisateur afin d'offrir le meilleur temps de réponse possible. En se rapprochant de l'utilisateur, ces datacenters desservent de moins en moins de clients et leur taille décroît. Le Cloud en résultant est alors appelé Fog, c'est-à-dire une « brume » qui entoure l'utilisateur de très près.

Deux autres environnements peuvent être définis : le Skin, ou peau, c'est-à-dire un nuage qui se trouve au contact de l'utilisateur, tout au plus à quelques mètres. On appelle les

datacenters correspondants des femto-datacenters, ou des home-datacenters, ou encore des wall-datacenters. La taille de ces datacenters n'est que de quelques serveurs, mais avec une grande puissance de stockage. La première génération de ce type de mémoires était représentée par les NAS (Network Attached Storage), qui étaient des serveurs de fichiers autonomes. Un femto-datacenter doit en outre posséder une très forte capacité de calcul ainsi qu'un système d'exploitation spécifique supportant des machines virtuelles. Le chapitre 3 décrit en détail comment se monte un tel environnement virtualisé.

Un autre environnement de Cloud de taille moyenne est le MEC (Mobile Edge Computing). Celui-ci recouvre un ensemble de services fournis par des datacenters de taille moyenne que les opérateurs placent essentiellement près du bord des réseaux, c'est-à-dire derrière les grandes antennes relais 3G/4G. Les MEC-datacenters desservent tous les clients situés derrière une antenne 3G ou 4G et bientôt 5G. L'environnement MEC est présenté au chapitre 13. Étant propres aux opérateurs de télécommunications, ces datacenters ne sont pas inclus dans la série Cloud, Fog et Skin.

Pour résumer, on peut regrouper les différentes sortes de datacenters en quatre grandes catégories, qui définissent les quatre grandes architectures de la nouvelle génération de réseaux :

- Cloud, aux puissances de calcul et de stockage très importantes, capables de gérer simultanément plus de dix mille utilisateurs et pouvant en gérer des millions.
- MEC, capables de gérer de mille à dix mille utilisateurs.
- Fog, capables de gérer de cinquante à mille utilisateurs.
- Skin, pour moins de cinquante utilisateurs.

Ces valeurs sont évidemment relatives puisque les définitions de ces différents environnements ne sont pas normalisées. Ces classes de datacenters représentent toutefois les grandes tendances des années 2020.

Les environnements de Cloud

Cloud est un mot générique désignant tous les environnements capables d'exploiter du calcul et du stockage, quelle que soit la taille des datacenters concernés.

Un Cloud peut offrir un très grand nombre de services grâce aux machines virtuelles qui le composent. Les environnements correspondants sont regroupés dans trois groupes principaux :

- IaaS (Infrastructure as a Service) ;
- PaaS (Platform as a Service) ;
- Saas (Software as a Service).

La hiérarchie de ces environnements est décrite à la figure 1.1.

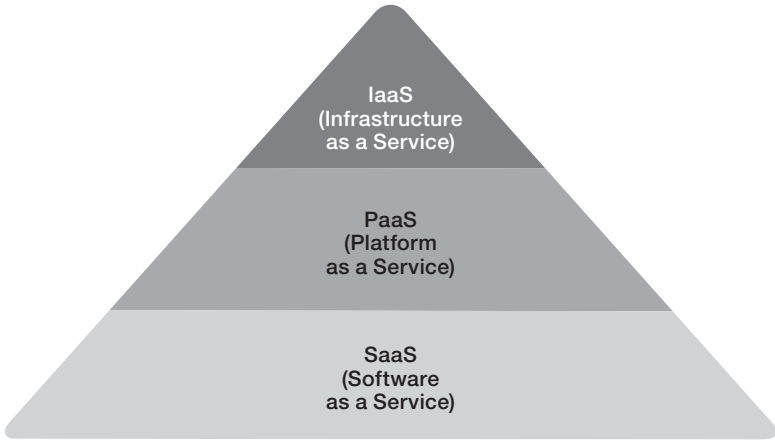


Figure 1.1

Les trois grands environnements de Cloud

Les fonctionnalités des principaux environnements de Cloud sont illustrées à la figure 1.2.

Dans le modèle classique, utilisé avant l'arrivée des Clouds, chaque entreprise utilisatrice devait gérer elle-même l'ensemble du système informatique, depuis le réseau et les applications jusqu'au stockage, en passant par les machines physiques, le système d'exploitation, les bases de données et éventuellement la virtualisation, si elle était déjà introduite dans le système.

L'IaaS permet à l'utilisateur de sous-traiter au fournisseur du Cloud la partie basse de l'environnement, c'est-à-dire le réseau, le stockage, l'infrastructure matérielle et la virtualisation. Le client conserve le système d'exploitation, la gestion des données et les applications. Dans le cas d'un PaaS, le client sous-traite un peu plus au fournisseur de Cloud, lui laissant également la charge du système d'exploitation et des données. Avec le SaaS, l'utilisateur sous-traite l'ensemble du système au fournisseur de Cloud, y compris ses applications.

Concernant ce qui intéresse ce livre, si chacun des trois environnements a recours au Cloud, l'IaaS est la version minimale permettant d'y traiter la partie réseau.

D'autres environnements, tels que SECaaS (Security as a Service), NaaS (Networking as a Service), XaaS (Anything as a Service), etc., permettent à des fournisseurs de Cloud d'offrir des services particuliers, comme de la sécurité, du réseau ou de la virtualisation totale.

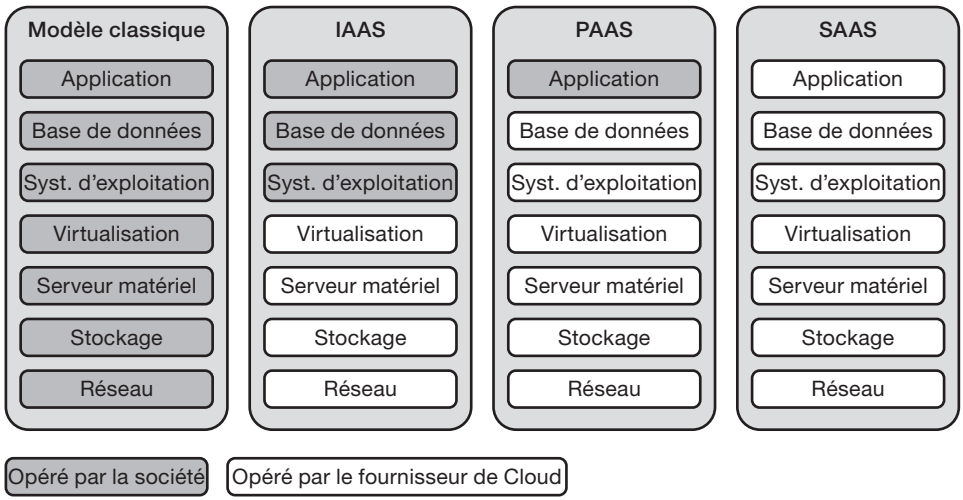


Figure 1.2

Fonctionnalités des principaux environnements des fournisseurs de Cloud

En résumé, les environnements réseau de nouvelle génération sont constitués de datacenters, grands, moyens, petits ou très petits, qui exécutent des machines virtuelles en guise de routeurs ou de commutateurs. Ces datacenters sont reliés entre eux par des canaux de communication à très haut débit, qui peuvent être de la fibre optique dans les centres importants ou des liaisons hertziennes à la périphérie.

On peut représenter cette nouvelle génération de réseaux sous la forme illustrée à la figure 1.3, où les machines qui transfèrent les paquets sont implémentées dans des datacenters et où ces datacenters sont reliés en réseau. Ceux-ci sont d'autant plus petits qu'ils se situent vers la périphérie. Ces réseaux font partie de ce que l'on appelle le Cloud Networking.

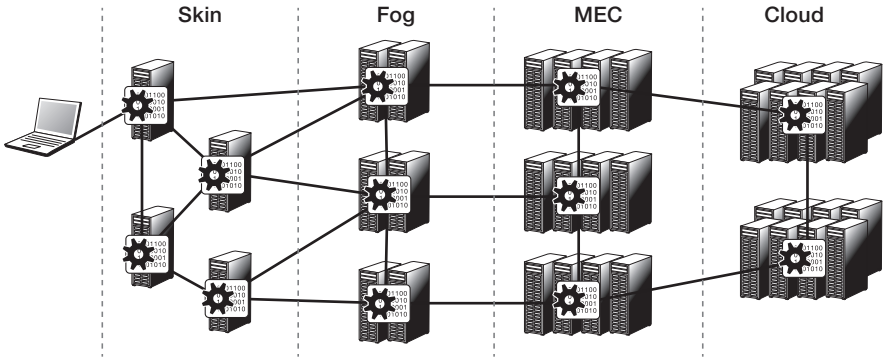


Figure 1.3

Architecture des réseaux à base de datacenters

Les nouvelles architectures réseau

À partir de l'architecture générale décrite à la figure 1.3, on peut déduire les quatre grandes architectures réseau qui se mettent en place aujourd'hui.

La première concerne les fournisseurs de Cloud (Google, Amazon, Microsoft, Apple, etc.) qui souhaitent gérer les réseaux à partir de très gros datacenters centraux.

Dans cette architecture, toute la périphérie avec les clients doit envoyer les données vers le centre, lequel traite alors l'ensemble des applications, que ce soit celles des clients ou celles associées au contrôle du réseau.

Dans ce cas, le signal émis par l'utilisateur remonte jusqu'au datacenter par l'intermédiaire d'une antenne intermédiaire ou utilise pour ce faire le réseau d'accès. Dans le premier cas, le signal remonte directement jusqu'au datacenter, et il n'est plus nécessaire de mettre les signaux en paquets. Cette solution est appelée Cloud-RAN (Radio Access Network), ou C-RAN. Elle est fortement centralisée et commence à se déployer dans les pays en développement en raison de ses coûts relativement bas puisqu'il n'y a qu'une infrastructure en étoile autour du datacenter. Toutes les machines virtuelles sont rassemblées dans le datacenter, ce qui offre la meilleure utilisation possible des ressources du datacenter.

Cette architecture est illustrée à la figure 1.4. Elle est examinée en détail au chapitre 13, dans le cadre du Cloud Networking.

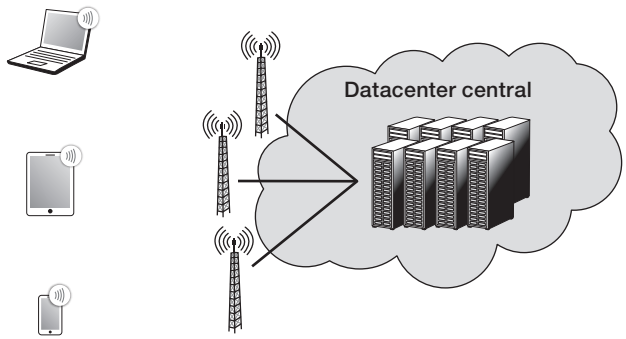


Figure 1.4

Architecture Cloud-RAN des fournisseurs de services

La deuxième architecture consiste à distribuer le datacenter central dans des datacenters MEC (mobile Edge Computing) de plus petite taille. Cette solution est illustrée à la figure 1.5.

Un datacenter MEC prend en charge de façon centralisée toute la périphérie. Dans cette solution, tous les équipements situés entre le client et le datacenter MEC sont virtualisés. Par exemple, la box Internet disparaît pour devenir une simple VM dans un serveur du datacenter MEC. L'avantage d'une telle architecture est de fournir un temps de réaction meilleur que dans le cas centralisé de l'architecture Cloud-RAN.

Cette solution à la faveur des opérateurs de télécommunications, qui espèrent ainsi contrôler et gérer toute la périphérie à partir de leurs datacenters. Ceux-ci doivent être reliés entre eux pour réaliser le réseau cœur, c'est-à-dire le réseau central permettant l'interconnexion des clients entre eux lorsqu'ils ne sont pas situés dans la zone définie par le datacenter.

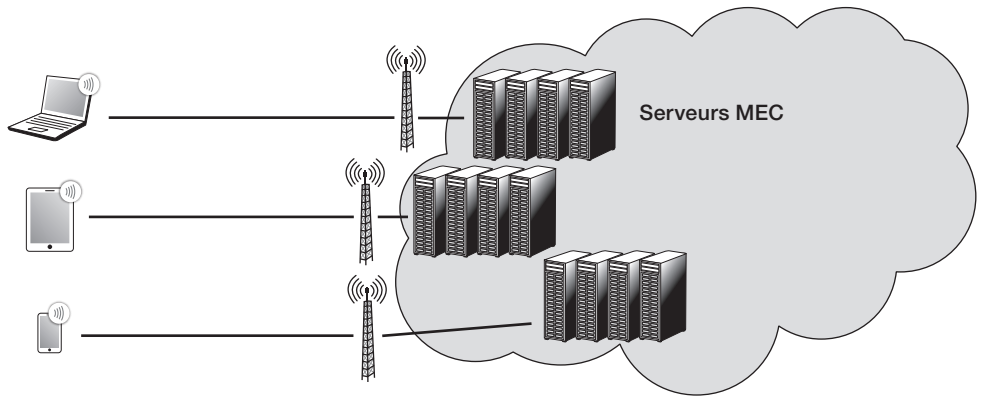


Figure 1.5

Architecture Cloud-MEC des opérateurs

La troisième architecture correspond aux besoins des équipementiers réseau. Cette solution est plus récente que les deux précédentes et se met en place depuis 2017 seulement. Les équipementiers réseau ont perdu beaucoup de leur pouvoir du fait de la montée en puissance des architectures décrites précédemment, dans lesquelles les décisions proviennent des datacenters, autant d'équipements qu'ils ne contrôlent pas, du moins pour ce qui concerne les plus gros d'entre eux.

L'idée de cette solution est de redonner la primauté aux équipements réseau de type routeur ou commutateur. Cependant, comme ils sont virtualisés, il est nécessaire de les intégrer dans de tout petits datacenters de la taille d'un équipement réseau classique.

Cette infrastructure matérielle générique recevant des machines virtuelles est appelée Fog pour indiquer sa proximité avec le client. En d'autres termes, un routeur est remplacé par une machine physique permettant de recevoir des machines virtuelles et, à l'intérieur de celles-ci, un routeur ou un commutateur virtuel. De ce fait, une telle machine peut être facilement remplacée par une autre ou être complétée par des machines virtuelles, comme un pare-feu pour la sécurité ou un serveur de stockage ou encore un serveur permettant de mettre en place un service de messagerie, par exemple.

Ce type d'architecture est conciliable avec les protocoles que l'on utilise depuis longtemps dans le cadre d'Internet, ce qui offre une intéressante solution de continuité. De plus, cette solution ajoute une machine centrale, toujours appelée un contrôleur, afin d'aider au contrôle et à la gestion du réseau.

Cette machine centrale reçoit toutes les mesures effectuées sur le réseau. Ces mesures, ou « connaissances », sont des informations contextualisées en provenance des machines

physiques et virtuelles constituant le réseau. Un tel contrôleur a une vue complète de l'ensemble des utilisateurs connectés et du réseau permettant de les interconnecter. Il a donc un pouvoir de contrôle important pour la détection des anomalies grâce à sa connaissance de tout ce qui se passe dans le réseau.

Dès que nécessaire, le contrôleur peut prendre le relais des routeurs et des commutateurs pour contrôler la périphérie. Il transfère alors aux machines virtuelles périphériques le pouvoir de contrôle dès lors qu'il n'y a plus de danger ou que le réseau revient à un fonctionnement normal. Cette architecture est illustrée à la figure 1.6.

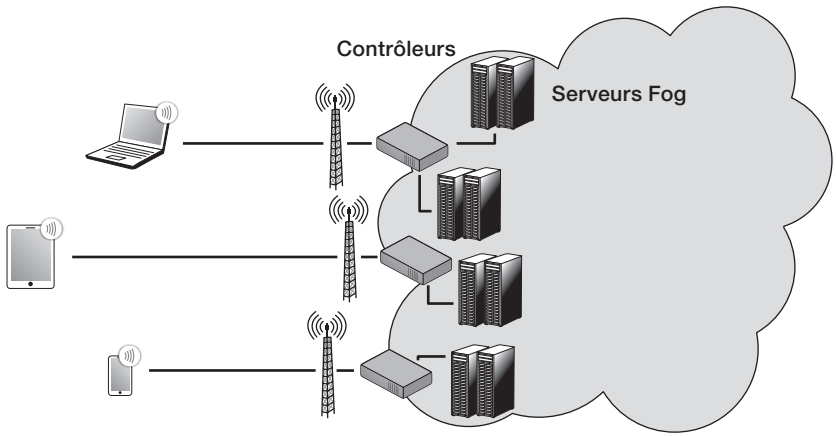


Figure 1.6

Architecture Fog des équipementiers réseau

La quatrième architecture de réseau de nouvelle génération peut être considérée comme une ubérisation des télécommunications. En effet, le réseau est construit à partir de femto-datacenters qui se trouvent chez les utilisateurs et non plus dans l'aire de l'opérateur. Les femto-datacenters sont reliés entre eux par des connexions hertziennes à très haut débit permettant de réaliser des réseaux maillés, appelés mesh.

Les limites d'une telle architecture proviennent de l'appui nécessaire d'un opérateur d'infrastructure pour effectuer la maintenance et la gestion du réseau. Comme il n'existe plus d'opérateur de télécommunications à proprement parler, le réseau ubérisé n'est plus maintenu et ne peut donc résoudre les problèmes éventuels résultant, par exemple, de défaillances ou de mauvais fonctionnements. Pour installer cette architecture, il est prudent d'attendre l'apparition de solutions d'autocontrôle, d'autoréparation, d'autogestion, d'autosécurité, etc.

L'architecture ubérisée des télécommunications est illustrée à la figure 1.7. Sur cette figure, chaque domicile possède un femto-datacenter encore appelé home datacenter ou serveur home ou wall-datacenter. Ces femto-datacenters sont interconnectés entre eux pour former un réseau mesh.

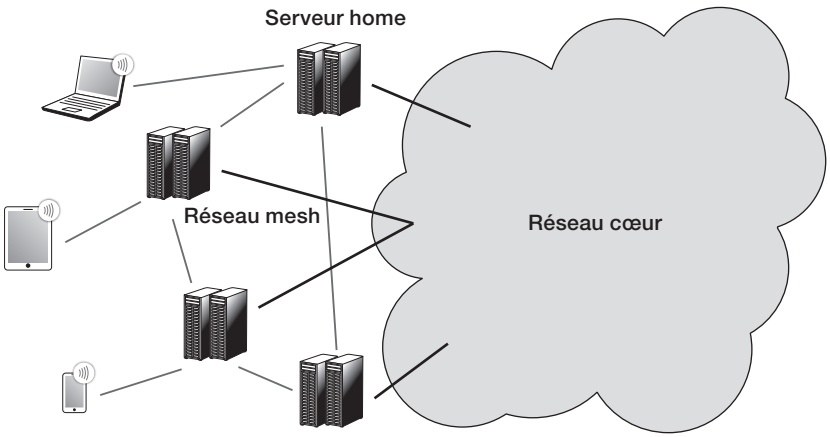


Figure 1.7

Architecture ubérisée des télécommunications

Ces quatre solutions aux protocoles et caractéristiques en tout point différents sont décrites plus en détail dans des chapitres dédiés. Il y a toutefois de grandes chances que l'architecture finale du monde des réseaux consiste en une superposition de ces architectures en fonction de la taille des datacenters.

Les réseaux sans fil

L'apparition de la technologie paquet dans les réseaux de mobiles et les réseaux sans fil date du début des années 2000 avec l'UMTS (Universal Mobile Telecommunications System). La génération d'avant, le GSM (Global System for Mobile Communications), était fondée sur le circuit, c'est-à-dire un ensemble de ressources n'appartenant qu'à l'émetteur et au récepteur et que personne d'autre ne pouvait utiliser.

Le circuit est différent du paquet en ce que les ressources ne sont affectées au paquet que lors de son passage dans un nœud de transfert.

Les réseaux de mobiles permettent la communication tout en se déplaçant. Dans les réseaux sans fil, la communication se fait par le biais d'une antenne, avec pour conséquence que l'utilisateur doit rester connecté à une même antenne. Les premiers réseaux hertziens ne disposaient que de débits très limités, mais ils ont vite atteint des performances quasiment identiques à celles des réseaux terrestres, du moins sur les paires métalliques. La 5G offrira des débits presque identiques à la fibre optique dès 2020.

Les réseaux hertziens sont regroupés en deux catégories, l'une provenant des industriels des télécommunications – et donc de la commutation –, avec une signalisation importante et une forte complexité pour prendre en charge tous les problèmes de la communication, l'autre provenant d'Internet – et donc du routage –, avec beaucoup moins de complexité, mais une qualité globale inférieure.

La quatrième génération de réseaux de mobiles, la 4G est devenue totalement compatible avec Internet. Elle atteint des débits identiques à ceux de l'ADSL et n'est plus loin des accès fibre optique.

Une uniformisation s'esquisse donc entre les mondes filaire et sans fil, de telle sorte qu'un même réseau cœur, le réseau de fibre optique central, permet de connecter un terminal fixe aussi bien qu'un terminal mobile. Cette convergence par le biais d'un réseau cœur unique est appelée NGN (Next Generation Network). Elle est décrite plus en détail au chapitre 16.

Ces réseaux filaires ou sans fil sont multimédias. Une application multimédia utilise en même temps l'image animée, la parole, les données et des assistances diverses.

Les caractéristiques de cette convergence sont les suivantes :

- Débits très importants dans le réseau cœur, notamment du fait de l'augmentation de la puissance des machines terminales et du débit de chaque client vers le réseau cœur.
- La qualité de service pour réaliser les contraintes de chaque application.
- La sécurisation du transport.
- La gestion de la mobilité et du raccordement à plusieurs réseaux simultanément (multihoming).
- La virtualisation de toutes les ressources du réseau.

La 5G, qui est étudiée en détail au chapitre 18, devrait être normalisée vers la fin de 2020, et les premiers produits apparaître sur le marché dès 2021. Il existe bien sûr des pré-5G, qui se résument à des propositions fortes destinées à influencer la normalisation. Beaucoup d'opérateurs ont annoncé la sortie de telles propositions lors de la tenue des prochains jeux Olympiques d'hiver et d'été.

La 5G tient sur trois pieds :

- La connexion massive d'objets, qui devraient s'élever à une cinquantaine de milliards en 2020.
- Des débits beaucoup plus importants en forte mobilité.
- La possibilité de satisfaire les applications demandant des temps de réaction extrêmement courts, que l'on appelle « mission critique ».

Les architectures réseau : distribution ou centralisation ?

Les architectures réseau étaient jusqu'à présent distribuées. À partir de 2015, l'arrivée du Cloud a chamboulé la donne au profit d'une centralisation des services dans des datacenters regroupant des centaines, voire des milliers de serveurs. Au début de 2018, les plus gros datacenters dépassent le million de serveurs. Ces centres disposent de puissances de calcul considérables et de mémoires gigantesques.

L'idée de cette nouvelle génération d'architectures réseau est de regrouper de façon centralisée toutes les informations disponibles sur le réseau, que ce soit de la part des applications ou de l'infrastructure, et de tout contrôler également de façon centralisée. Les avantages

sont que le centre peut accumuler une multitude d'informations qui ne pourraient pas être traitées simplement de façon distribuée.

Dans de telles architectures, c'est le centre qui décide de tout, en particulier du chemin ou de la route à suivre par les paquets. Le choix du chemin, qui est le cas le plus classique de la solution centralisée, est facilité par la vision complète du réseau dont dispose le centre, qui peut ainsi réserver les ressources nécessaires tout au long du chemin pour obtenir la qualité de service voulue.

Le centre peut également choisir une solution de routage. Dans ce cas, il calcule la table de routage, qu'il distribue aux nœuds du réseau. Il doit toutefois recalculer la table de routage dès que l'état du réseau change et la distribuer à l'ensemble des nœuds. La solution de commutation avec établissement de chemin est à cet égard préférable, car elle ne demande pas de distribution régulière des tables. De plus, une fois le chemin choisi, il n'est pas nécessaire de le modifier, même si des chemins meilleurs peuvent être trouvés par la suite, puisque la qualité de service qui a été requise est toujours disponible.

Baptisée SDN (Software-Defined Networking), cette nouvelle architecture centralisée a été normalisée par l'ONF (Open Networking Foundation).

On pourrait traduire SDN par réseau logiciel (le chapitre 3 détaille les différences entre réseaux matériels et réseaux logiciels). Mais l'architecture SDN possède un centre, ce que l'expression réseau logiciel ne laisse pas soupçonner. La présente édition montre cependant qu'il existe tout aussi bien des réseaux logiciels distribués. Le sigle SDN est donc réservé à des réseaux qui possèdent un centre de contrôle appelé contrôleur. Le contrôleur dispose d'une interface avec les applications, appelée interface nord, et d'une interface avec les nœuds du réseau, appelée interface sud.

Conclusion

Les architectures réseau n'ont cessé d'évoluer depuis leur naissance, à la fin des années 1960 et au début des années 1970. Ces évolutions s'accélèrent avec l'arrivée du Cloud et de ses dérivés MEC, Fog et Skin. Jusqu'au début des années 2020, la tendance sera à la centralisation du contrôle, mais évoluera ensuite certainement à nouveau vers une distribution.

Les autres évolutions marquantes du moment concernent le monde open source, qui n'a pas encore été introduit, mais qui est un mouvement majeur détaillé en différents endroits de ce livre, notamment au chapitre 14, et l'intelligence pour gérer et contrôler les réseaux de façon beaucoup plus automatisée, qui est également introduite tout au long du livre.