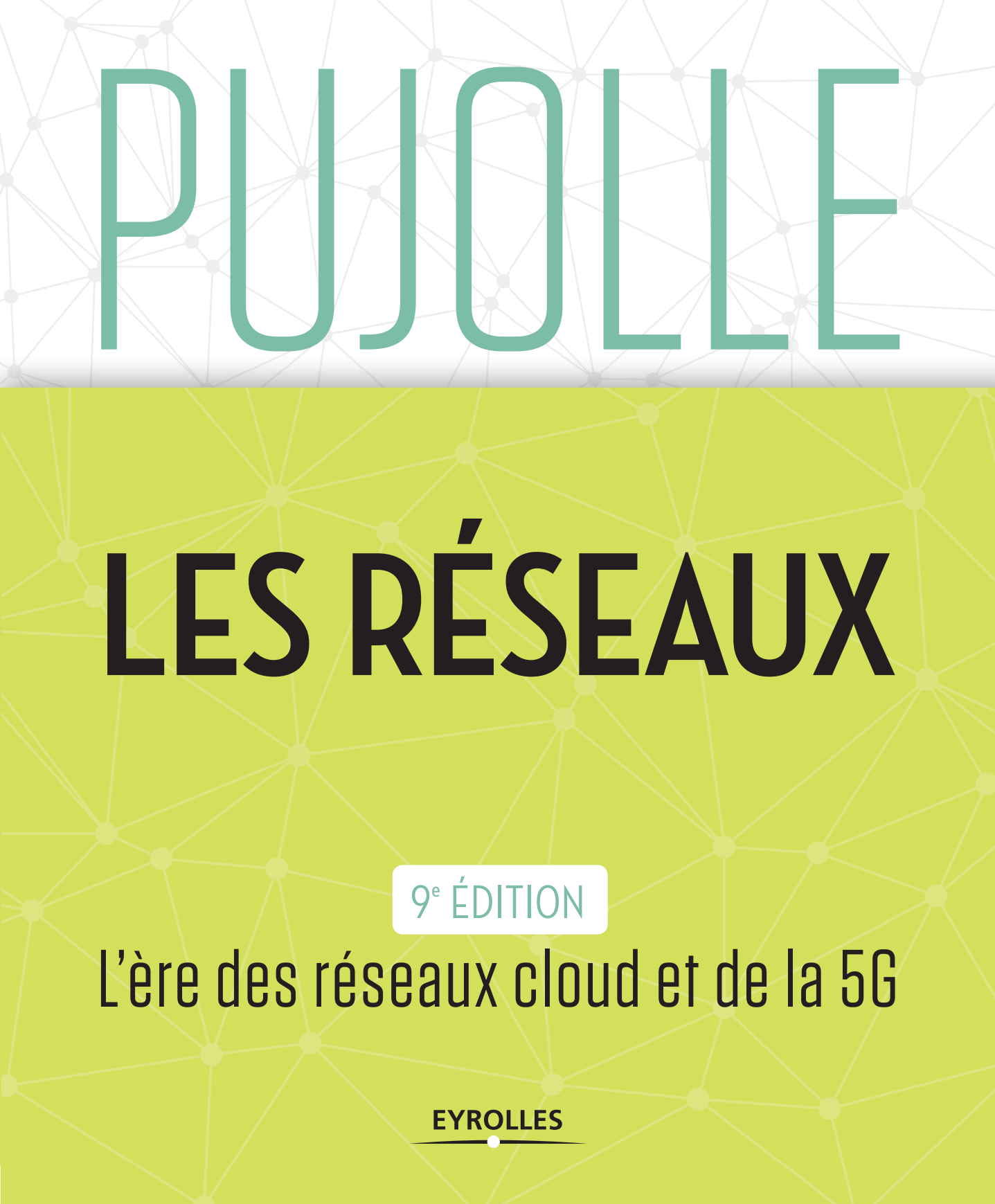




PUJOLLE

LES RÉSEAUX

9^e 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

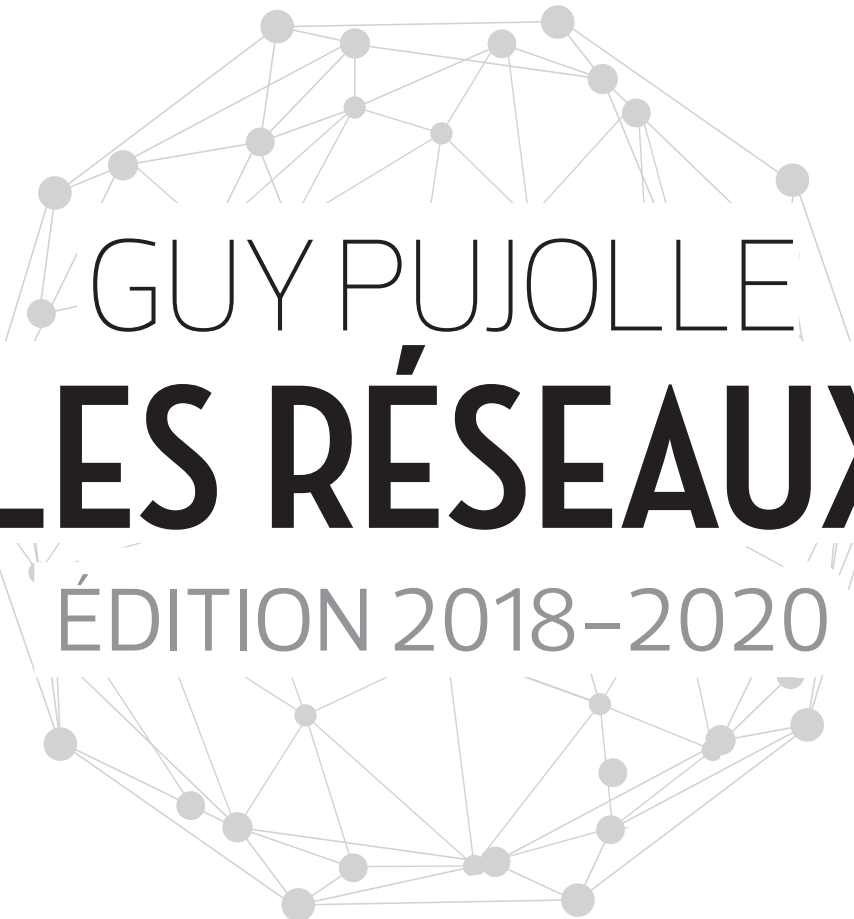
Guy Pujolle est professeur à Sorbonne Université et responsable de nombreux grands projets de recherche français et européens. Il a été professeur invité à NCSU, Stanford, Rutgers, UQAM, Postech et UFRJ. Ses recherches portent actuellement sur la conception et le développement des réseaux des années 2020.

Il est cofondateur de la société QoS MOS, 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.

www.editions-eyrolles.com

LES RÉSEAUX

ÉDITION 2018–2020

A network diagram consisting of numerous grey circular nodes connected by thin grey lines, forming a complex web-like structure that frames the central text.

GUY PUJOLLE

LES RÉSEAUX

ÉDITION 2018–2020

9^e édition
Avec la collaboration de Olivier Salvatori

EYROLLES

The Eyrolles logo, featuring a red dot centered on a horizontal line.

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

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement le présent ouvrage, sur quelque support que ce soit, sans autorisation de l'éditeur ou du Centre français d'exploitation du droit de copie, 20, rue des Grands-Augustins, 75006 Paris.

© Groupe Eyrolles 1995-2018
ISBN : 978-2-212-67535-1

Préface à la 9^e 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 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 I

Les éléments de base des réseaux	1
CHAPITRE 1	
Introduction aux réseaux	3
Le paquet	4
Cloud, MEC, Fog et Skin	5
Les environnements de Cloud	6
Les nouvelles architectures réseau	9
Les réseaux sans fil	12
Les architectures réseau : distribution ou centralisation ?	13
Conclusion	14
CHAPITRE 2	
Les composants des réseaux	15
Transfert, commutation et routage	15
Le transfert de paquets	18
Le modèle de référence	20
Commutation et routage	21
Les réseaux informatiques	22
Les réseaux de télécommunications	24
Les réseaux de câblo-opérateurs	26

L'intégration des réseaux	29
Conclusion	30

CHAPITRE 3

Réseaux virtuels et Cloud	31
La virtualisation de réseau	31
Technologies de virtualisation de réseau	35
L'isolation	36
Utilisation de la virtualisation de réseau	39
Virtualisation d'équipements de réseau	40
NFV (Network Functions Virtualization) et normalisation de la virtualisation	40
Les réseaux virtualisés	42
Conclusion	45

CHAPITRE 4

L'intelligence dans les réseaux	47
Orchestrateurs et contrôleurs	48
Les agents intelligents	54
Gestion d'un environnement complexe	55
Les systèmes multi-agents	56
Les systèmes d'agents réactifs	62
Les agents réseau	64
Les agents Internet	64
Les agents intranet	65
Les agents assistants ou bureautiques	65
Les agents mobiles	65
Les réseaux actifs	67
Les réseaux programmables	69
Les réseaux autonomes	71
Les réseaux autonomiques	71
Conclusion	74

PARTIE II

Les protocoles réseau	75
CHAPITRE 5	
Le niveau physique	77
Le médium physique	77
Les équipements	83
Le codage et la transmission	85
La transmission en bande de base	87
La modulation	89
La modulation d'amplitude	90
La modulation de phase	90
La modulation de fréquence	91
Les modems	91
Les multiplexeurs	93
Multiplexages fréquentiel et temporel	93
Le multiplexage statistique	93
La transmission	95
La numérisation des signaux	96
Numérisation des signaux analogiques	98
Détection et correction d'erreur	102
La correction d'erreur	104
La détection d'erreur	106
Architecture des routeurs	107
Architecture des commutateurs	109
Les passerelles	111
Les répéteurs	113
Les ponts	113
Les relais-routeurs	116
Les routeurs multiprotocoles	116
Les gigarouteurs	116
Les bridge-routeurs	117

Les pare-feu	119
Les proxy	120
Les appliances	121
Conclusion	123

CHAPITRE 6

Le niveau trame	125
L'architecture de niveau trame	126
Les fonctionnalités du niveau trame.	126
L'adressage de niveau trame	128
Les protocoles de niveau trame.	129
Le protocole PPP (Point-to-Point Protocol)	129
Le protocole ATM	130
L'en-tête de la trame ATM.	131
La trame Ethernet	134
Le Label Switching	137
Conclusion	138

CHAPITRE 7

Les niveaux paquet et message	139
Le niveau paquet	139
Les modes avec et sans connexion.	141
Les principaux protocoles de niveau paquet	142
Les grandes fonctionnalités du niveau paquet	142
Autres fonctionnalités du niveau paquet	155
IP (Internet Protocol)	158
Le niveau message.	165
Les fonctionnalités du niveau message	166
Les caractéristiques du niveau message.	167
Les protocoles de niveau message	170
Conclusion	179

PARTIE III

Les solutions réseau 181

CHAPITRE 8

Les réseaux de niveau physique..... 183

Les réseaux optiques 183

La fibre optique 183

Le multiplexage en longueur d'onde 186

Architecture des réseaux optiques 187

Signalisation et GMPLS..... 192

Les interfaces de niveaux physiques 193

Les interfaces avec le niveau physique 194

MPLS-TP 205

Conclusion 205

CHAPITRE 9

Les réseaux Ethernet 207

Les modes partagé et commuté..... 207

Les réseaux Ethernet partagés 208

Caractéristiques 209

L'accès aléatoire..... 214

Les réseaux Ethernet commutés..... 217

Ethernet pour les entreprises 219

Le Fast Ethernet 100 Mbit/s..... 221

Le Gigabit Ethernet (GbE)..... 222

Le 10 Gigabit Ethernet (10GbE) 224

Le 100 Gigabit Ethernet (100GbE) 225

Ethernet pour les opérateurs..... 226

Ethernet Carrier Grade 228

Ethernet pour les datacenters 232

TRILL..... 233

VXLAN 233

Conclusion 234

CHAPITRE 10

Les réseaux IP	235
L'architecture IP	235
Internet.....	236
Fonctionnement des réseaux TCP/IP	239
L'adressage IPv4 et IPv6.....	240
DNS (Domain Name System).....	244
Le routage IP	247
Les algorithmes de routage.....	248
NAT (Network Address Translation).....	257
LISP	261
Les protocoles de contrôle	262
ICMP (Internet Control Message Protocol).....	262
IGMP (Internet Group Management Protocol).....	264
Les protocoles de signalisation	264
RSVP.....	265
RTP (Real-time Transport Protocol).....	270
La qualité de service	271
IntServ (Integrated Services).....	272
DiffServ (Differentiated Services).....	273
Conclusion	285

CHAPITRE 11

Le Label Switching : MPLS et GMPLS	287
MPLS (MultiProtocol Label Switching)	287
Caractéristiques.....	289
Fonctionnement.....	290
Distribution des références.....	293
L'ingénierie de trafic.....	298
La qualité de service.....	301
MPLS-TP	302
GMPLS (Generalized MPLS)	305
Les extensions de MPLS.....	305

Réseau overlay	307
Contrôle et gestion de MPLS	309
Plan de contrôle de GMPLS	310
Conclusion	311
CHAPITRE 12	
Les réseaux SDN	313
SDN (Software-Defined Networking)	314
L'architecture ONF	315
L'interface sud	320
L'interface nord	332
Conclusion	334
CHAPITRE 13	
Le Cloud Networking	335
La virtualisation dans le Cloud Networking	336
Le Cloud-RAN	340
Les serveurs MEC	341
Les femto-datacenters	347
Les protocoles du Cloud Networking	348
Les protocoles intradatecenter	348
Les protocoles interdatacenter	351
Les protocoles avec les utilisateurs	351
Fog et Skin Networking	352
Conclusion	353
CHAPITRE 14	
Les réseaux open source	355
L'open source dans les réseaux	355
OPNFV	357
Les releases d'OPNFV	361
OSM	366
DPDK	367

ODP	368
FD.io	369
OpenStack	371
OpenStack et l'environnement réseau	375
Conclusion	376

PARTIE IV

Les réseaux d'accès	377
----------------------------------	-----

CHAPITRE 15

Les réseaux d'accès terrestres	379
La fibre optique	380
A-PON (ATM Over PON)	381
E-PON (Ethernet Passive Optical Network)	383
G-PON (Giga Passive Optical Network)	384
Les réseaux câblés (CATV)	384
Les paires métalliques	387
La boucle locale métallique	387
Les accès xDSL	388
Les modems ADSL	388
Les modems VDSL	390
Les DSLAM (DSL Access Module)	391
Les protocoles de l'ADSL	392
Le Multi-Play	393
La boucle locale électrique	396
Conclusion	397

CHAPITRE 16

Les réseaux d'accès hertziens	399
Les normes des réseaux hertziens	400
Typologie des réseaux hertziens	402
La boucle locale sans fil	402
Les systèmes WLL	403

Exemples de réseaux d'accès hertziens	404
L'allocation de ressources	407
Les techniques d'accès FCA	408
Les méthodes dynamiques DCA	413
Les réseaux de mobiles	413
Les générations de réseaux de mobiles	414
La radio cognitive et les avancées technologiques	420
La boucle locale satellite	422
Le contrôle dans les réseaux de mobiles	424
IP Mobile	424
Solutions pour la micromobilité	426
Gestion du handover dans les réseaux hétérogènes	427
Taxonomie des handovers	428
UMA (Unlicensed Mobile Access)	429
Le multihoming	431
Les protocoles de niveau réseau	432
Les protocoles de niveau transport	437
IMS (IP Multimedia Subsystem)	438
NGN (Next Generation Network)	443
Conclusion	444
 CHAPITRE 17	
Les small cells et les réseaux multisaut	445
Les réseaux small cells	446
Les femtocells	446
Les hotspots	448
Les metrocells	450
Les microcells	450
Passpoint	452
Caractéristiques	452
Les réseaux multisaut	454
Les réseaux ad-hoc	455
Les réseaux mesh	462

Les réseaux VANET	463
Les réseaux de backhaul	464
Radio logicielle et radio cognitive	466
Les cellules sur mesure	467
Conclusion	468

PARTIE V

Les réseaux de mobiles et sans fil	469
---	-----

CHAPITRE 18

Les réseaux de mobiles 1G à 5G	471
Les cinq générations de réseaux de mobiles	471
La 2G	472
La mobilité dans les réseaux 2G	473
La 3G	476
Le 3GPP	477
L'UMTS	479
La 3G+	491
Le HSDPA	492
Le HSUPA	493
Le HSOPA	494
Le LTE	495
La 4G	496
LTE Advanced	497
La 5G	503
Conclusion	512

CHAPITRE 19

Les réseaux personnels	513
WPAN	513
IEEE 802.15	514

Bluetooth	515
Communications	518
Techniques d'accès	521
UWB	523
L'interface radio	525
Complexité et énergie	527
ZigBee	528
Le niveau applicatif	530
Wi-Fi personnel	532
IEEE 802.11ad (WiGig)	532
IEEE 802.11ay	534
WirelessHD	534
Li-Fi	535
Conclusion	535
CHAPITRE 20	
Les réseaux Wi-Fi	537
IEEE 802.11	538
Architecture Wi-Fi	540
Couche physique	540
Couche liaison de données	541
Techniques d'accès	541
Fonctionnalités	544
Handovers	544
Sécurité	545
Trames Wi-Fi	552
IEEE 802.11a, b et g	553
IEEE 802.11n	555
IEEE 802.11ac	556
IEEE 802.11af	557
Qualité de service	558
Équipements Wi-Fi	561

Points d'accès	562
Contrôleurs	563
Ponts	565
Antennes	567
Conclusion	570

CHAPITRE 21

L'Internet des objets	571
Les réseaux longue distance	572
Sigfox	573
LoRa	574
Les réseaux de la 5G	576
Les réseaux PAN et LAN	577
Les réseaux de capteurs	580
RFID	582
Utilisation des RFID	583
La technologie RFID	584
EPCglobal	584
Sécurité des RFID	585
Mifare	586
NFC	586
La clé mobile	587
Le paiement sans contact NFC	588
L'Internet des objets dans le médical	590
L'Internet des objets dans le domicile	591
Le marketing de proximité	592
Les mécanismes du marketing de proximité	592
Plate-forme pour le marketing de proximité fondé sur la géolocalisation	595
Conclusion	596

PARTIE VI

Contrôle, gestion, sécurité et énergie 599

CHAPITRE 22

VLAN et VPN 601

Les VLAN..... 601

Fonctionnement des VLAN..... 603

Les VPN 607

Architecture des VPN..... 607

Catégories de VPN..... 607

VPN de niveaux trame, paquet et application 609

VPN fonctionnels..... 615

Conclusion 617

CHAPITRE 23

La gestion et le contrôle 619

La gestion de réseau 621

Gestion Internet avec SNMP 622

Gestion par le Web..... 628

Gestion par le middleware 631

Le modèle DME..... 634

SLA (Service Level Agreement) 635

Le contrôle de réseau 638

Le contrôle de congestion..... 639

Le contrôle de flux dans les réseaux IP 641

Le contrôle de flux dans IP..... 644

La signalisation 646

Caractéristiques 646

Fonctionnement 647

Le protocole RSVP..... 649

SIP (Session Initiation Protocol)..... 653

Entités..... 653

Scénarios de session..... 660

SDP (Session Description Protocol) 661

NSIS (Next Steps In Signaling)	664
Conclusion	664
CHAPITRE 24	
La sécurité et l'identité	667
Les services de sécurité	668
Les mécanismes de chiffrement	669
Les algorithmes de chiffrement	670
Solutions de chiffrement	672
Les certificats	673
L'authentification	674
L'intégrité des données	674
La non-répudiation	675
Caractéristiques des algorithmes de sécurité	675
Les algorithmes de chiffrement	675
La performance temporelle	677
Les algorithmes d'authenticité	678
Les algorithmes d'authentification	679
Autres mécanismes d'authentification	681
Exemples d'environnements de sécurité	684
PGP (Pretty Good Privacy)	684
L'infrastructure PKI	684
Les virus	687
L'identité	688
Les systèmes de gestion des identités	689
Vie privée	690
La sécurité par carte à puce	690
La sécurité dans l'environnement IP	693
Les attaques par Internet	694
Les parades	696
IPsec (IP sécurisé)	698
L'en-tête d'authentification	700
L'en-tête d'encapsulation de sécurité	701
SSL (Secure Sockets Layer)	703

Les protocoles d'authentification	705
PPP (Point-to-Point Protocol)	705
EAP (Extensible Authentication Protocol)	712
RADIUS (Remote Authentication Dial-In User Server)	719
Les pare-feu	720
La sécurité autour du pare-feu	724
La sécurité du SDN	726
Conclusion	733
CHAPITRE 25	
Les réseaux « green »	735
La consommation énergétique des réseaux hertziens	735
Stratégies de réduction de la consommation des réseaux hertziens	738
La consommation énergétique des réseaux terrestres	740
Stratégies de réduction de la consommation des réseaux terrestres	741
Conclusion	745
CHAPITRE 26	
Généralités futures	747
Les réseaux participatifs	747
La concrétisation	748
Les réseaux morphware	751
Le pilotage automatique	753
La blockchain	754
Conclusion	755
Index	757

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.

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.

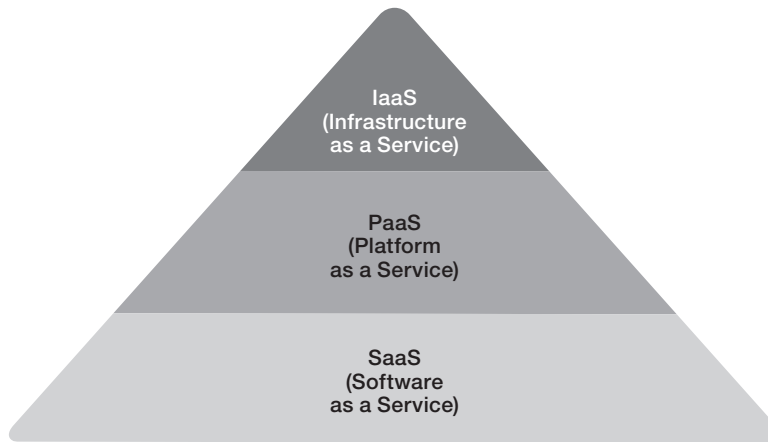
Les environnements de Cloud

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.

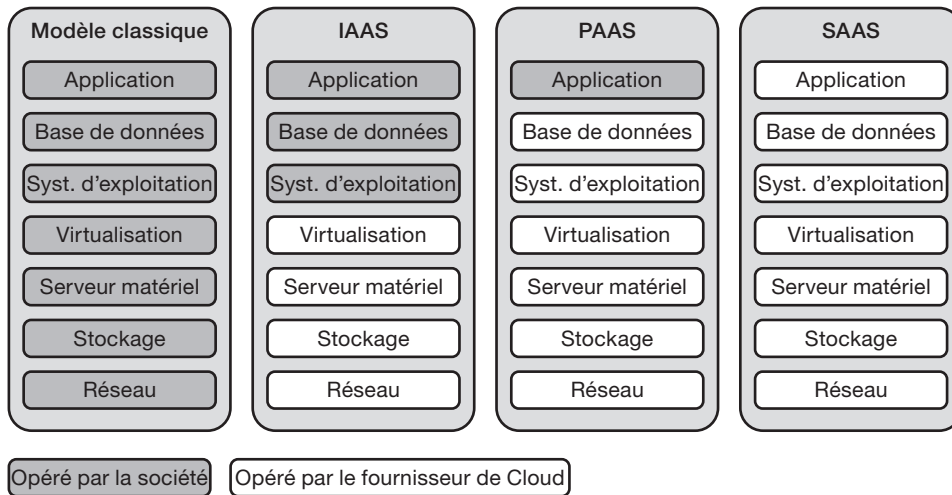


Figure 1.2

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.

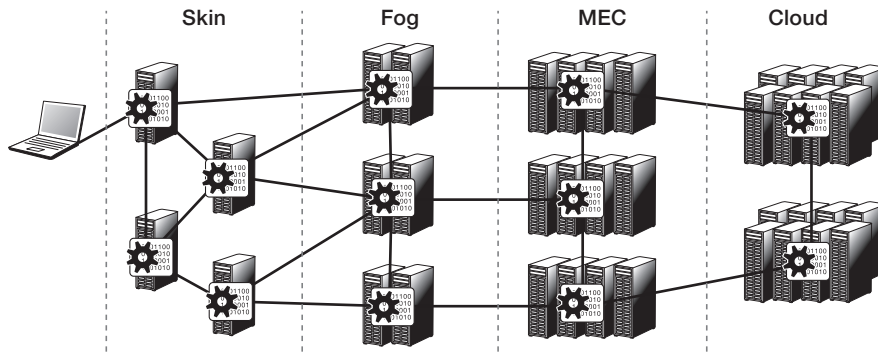


Figure 1.3

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.

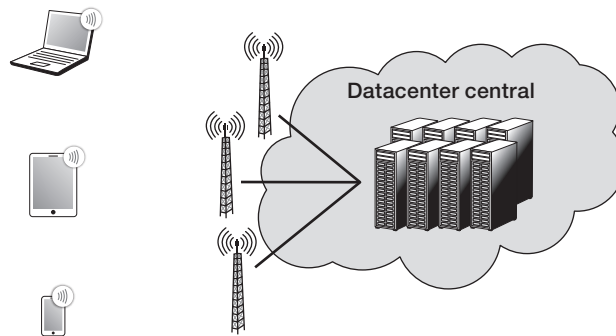


Figure 1.4

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.

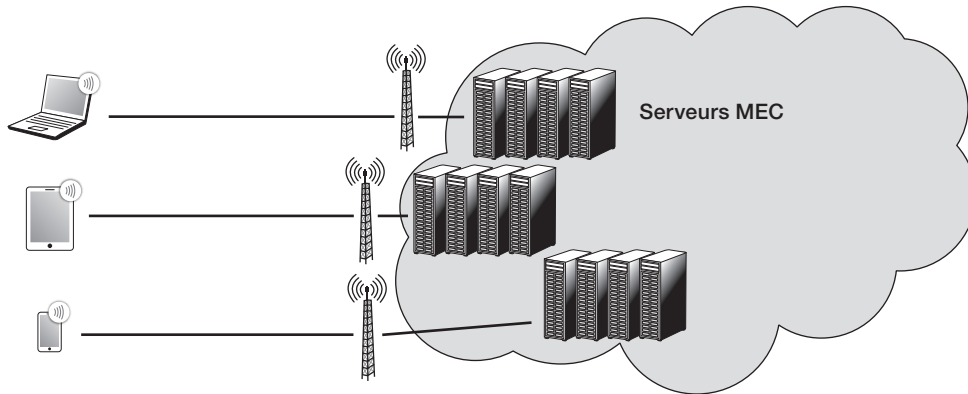


Figure 1.5

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.

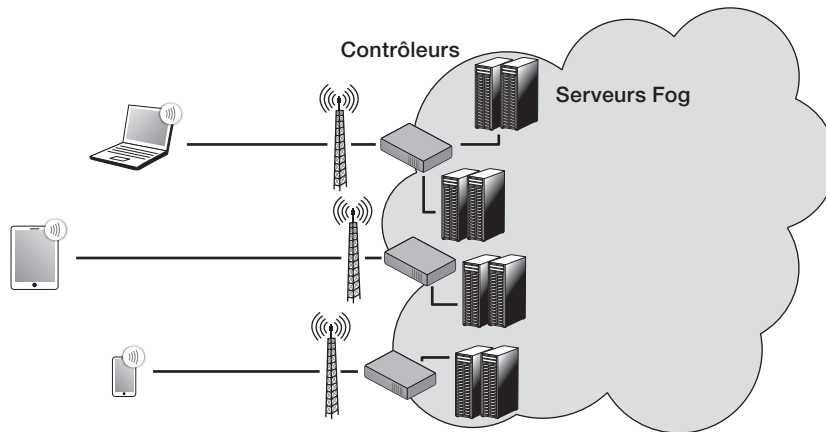


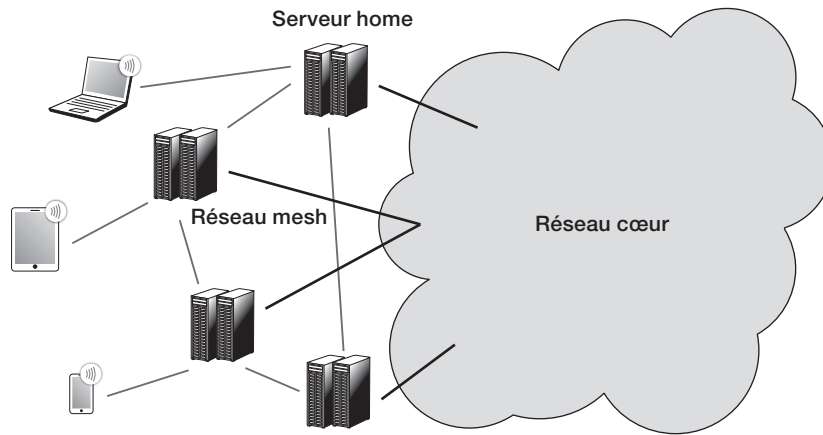
Figure 1.6

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'accélérent 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.

Les composants des réseaux

Après un premier chapitre consacré aux évolutions en cours qui touchent l'architecture des réseaux, le présent chapitre détaille le fonctionnement du transfert de paquets (*packet forwarding*) et introduit ses grands principes, qui n'ont guère changé depuis une cinquantaine d'années. Il passe ainsi en revue les techniques de transfert, la commutation et le routage, et compare les solutions mises en place dans le cadre des réseaux Internet, des réseaux de télécommunications et des réseaux de câblo-opérateurs.

Transfert, commutation et routage

Les réseaux modernes sont apparus au cours des années 1960 à la faveur d'une technologie totalement nouvelle permettant de transporter de l'information d'une machine à une autre. Ces machines étaient alors des ordinateurs de première génération, nettement moins puissants qu'un smartphone actuel. Les réseaux de téléphonie existaient quant à eux depuis longtemps. Ils utilisaient la technologie dite de *commutation de circuits* et le support de lignes physiques reliant l'ensemble des téléphones par le biais de commutateurs. Lors d'une communication, ces lignes physiques ne pouvaient être utilisées que par les deux utilisateurs en contact. Le signal qui y transitait était de type analogique.

La première révolution des réseaux a été apportée par la technologie numérique des codecs (codeurs-décodeurs), qui permettaient de transformer les signaux analogiques en signaux numériques, c'est-à-dire une suite de 0 et de 1. Le fait de traduire tout type d'information sous forme de 0 et de 1 permettait d'unifier les réseaux. Dans cette génération, la commutation de circuits était toujours fortement utilisée. Les circuits étant devenus numériques, la question s'est posée de faire passer simultanément sur un même circuit plusieurs flots, correspondant à des applications différentes. C'est ainsi qu'on a pu, par exemple, avoir 1 octet (8 bits) de téléphonie, suivi de 2 bits de transfert de fichiers puis de 8 bits

d'application vidéo. Cette solution ne s'est toutefois quasiment pas développée et a laissé la place au transfert de paquets.

Le transfert de paquets a permis de prendre en compte la forte irrégularité du débit de la communication entre deux ordinateurs, alternant les périodes de débit important et les périodes de silence, résultant du fait que, par exemple, un ordinateur doit attendre la réponse d'un autre ordinateur.

Dans la commutation de circuits, le circuit reste inutilisé pendant les périodes de silence, induisant un important gaspillage des ressources. À l'inverse, le transfert de paquets n'utilise les ressources du réseau que lors de l'émission effective des paquets. L'idée s'est donc fait jour de constituer des blocs d'information de longueur variable et de les envoyer de nœud de transfert en nœud de transfert jusqu'à atteindre la destination. Les ressources d'une liaison entre deux nœuds ne sont de la sorte utilisées que pendant le transfert des paquets. Les différents paquets provenant d'un même utilisateur et d'une même application forment un *flot*. Une fois les paquets de ce flot parvenus à destination, il est possible d'utiliser la même liaison et les ressources du réseau pour le passage d'autres paquets, provenant d'autres flots.

Parmi les nombreuses solutions de transfert de paquets qui ont été proposées, deux ont résisté au temps, le routage et la commutation. Dans le routage de paquets, les paquets sont aiguillés par chaque nœud de transfert en fonction de leur destination. La route choisie peut varier en fonction de l'état du réseau, de telle sorte que deux paquets d'un même flot peuvent suivre une route différente. Des *tables de routage* sont implémentées dans les nœuds afin d'optimiser le transport des paquets en fonction de l'état du réseau.

Issue du monde des télécommunications, la commutation de paquets consiste à mettre en place, avant d'envoyer le moindre paquet, un chemin entre les entités en communication, chemin que tous les paquets d'un même flot doivent emprunter. Ce chemin (*path*) a longtemps été appelé *circuit virtuel* parce que les paquets utilisant des chemins différents peuvent utiliser les mêmes ressources. Il n'y a donc pas de ressource réservée.

Chacune de ces techniques présente des avantages et des inconvénients. Le routage est une technique souple. Dans la mesure où chaque paquet transporte l'adresse du destinataire, la route peut varier, sans risque que le paquet soit perdu. En revanche, il est très difficile d'y assurer une qualité de service, c'est-à-dire de garantir que le service de transport sera capable de respecter une performance déterminée. Avec la commutation de paquets, la qualité de service est plus facilement assurée, puisque tous les paquets suivent un même chemin et qu'il est possible de réserver des ressources ou de déterminer par calcul si un flot donné a la possibilité de traverser le réseau sans encombre.

La principale faiblesse de la commutation de paquets réside dans la mise en place du chemin que vont suivre les différents paquets d'un flot. Ce chemin est ouvert par une procédure spécifique, appelée *signalisation* : on signale au réseau l'ouverture d'un chemin, lequel doit en outre être « marqué » afin que les paquets du flot puissent le suivre. Cette signalisation exige d'importantes ressources, ce qui rend les réseaux à commutation de paquets sensiblement plus chers que les réseaux à routage de paquets.

La figure 2.1 illustre ces deux branches du transfert de paquets, le routage et la commutation, ainsi que les principales techniques qu'elles utilisent.

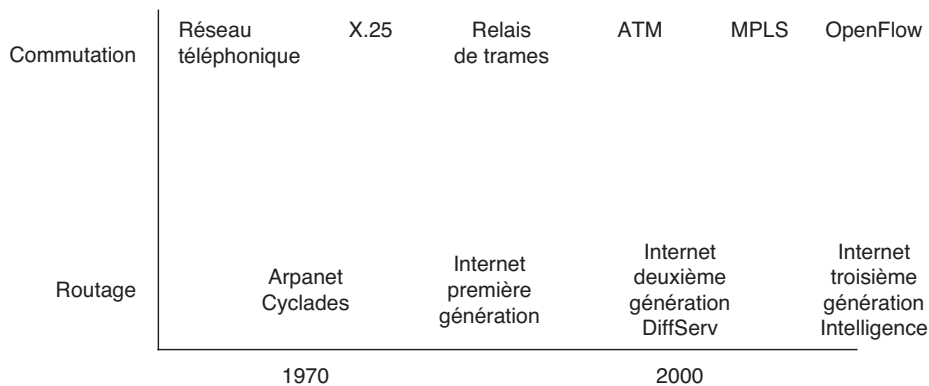


Figure 2.1

Les deux branches du transfert de paquets

Ces deux catégories de réseaux se sont développées en parallèle. Au départ, il n'y avait que peu de concurrence entre elles, car elles s'adressaient à des mondes différents. Avec le temps, les techniques de routage, liées à Internet, se sont étendues au transport d'applications synchrones telles que la téléphonie et la vidéo. En parallèle, la commutation de paquets prenait en charge la téléphonie et la télévision. Aujourd'hui, toutes deux sont en concurrence pour le transport des applications multimédias. Leurs avantages et inconvénients respectifs auraient plutôt tendance à faire choisir la commutation de paquets par les opérateurs et les très grandes entreprises et le routage par les petites et moyennes entreprises.

Les techniques de routage n'ont que peu changé. Le protocole IP (Internet Protocol) en constitue le principal déploiement : le paquet IP contenant l'adresse complète du destinataire est routé dans des nœuds de transfert appelés routeurs.

À l'inverse, les protocoles liés à la commutation ont beaucoup évolué. La première grande norme de commutation, X.25, a vu le jour dans les années 1980. Cette solution exigeait des opérations importantes pour effectuer la commutation : le chemin était tracé dans le réseau par un ensemble d'indices, appelés *références*, constituant autant de « pierres de couleur » sur toute sa longueur. Le paquet n'avait qu'à suivre ces pierres jusqu'à destination. Avec l'accroissement vertigineux du nombre de flots, les « couleurs » des pierres indiquant les chemins sont devenues insuffisantes. Une nouvelle signalisation a été introduite avec le relais de trames puis avec la technique ATM (Asynchronous Transfer Mode). Aujourd'hui, de nouvelles solutions se mettent en place avec les techniques SDN (Software-Defined Networking).

Avant d'aller plus loin, les sections qui suivent se penchent plus en détail sur la notion de paquet. Un paquet n'est pas un bloc de données que l'on peut envoyer tel quel sur une ligne de communication. Par exemple, si l'on envoie deux paquets collés l'un à l'autre, le récepteur est incapable de distinguer la fin du premier paquet et le début du second. Pour permettre cette opération de reconnaissance, il faut encapsuler chaque paquet dans une trame. La trame possède une succession spécifique d'éléments binaires permettant de

reconnaître son début et sa fin. Pour transporter un paquet IP, on peut l'encapsuler dans une trame PPP (Point-to-Point Protocol) ; pour transporter un paquet X.25, on l'encapsule dans une trame LAP-B ; pour transporter un paquet IP dans une trame Ethernet, il faut ajouter une suite assez longue, nommée drapeau, contenant une succession de 10 pour se terminer au bout de 8 octets par 11 (1010101010...11).

Dans les générations de réseaux suivantes, l'adresse complète du destinataire, ou la référence, est reportée dans la trame afin d'en simplifier la récupération : il n'est de la sorte plus nécessaire de décapsuler la trame pour récupérer le paquet et les informations qu'il contient. Cette solution, mise en œuvre notamment dans le relais de trames et la technique MPLS (MultiProtocol Label Switching), simplifie énormément le travail effectué dans les nœuds de transfert.

Le transfert de paquets

La technique utilisée pour le transport des données sous forme numérique, c'est-à-dire sous forme de 0 et de 1, que l'on a adoptée depuis la fin des années 1960 s'appelle le transfert de paquets.

Toutes les informations à transporter sont découpées en paquets pour être acheminées d'une extrémité à une autre du réseau. Cette technique est illustrée à la figure 2.2. L'équipement terminal A souhaite envoyer un message à B. Le message est découpé en trois paquets, qui sont émis de l'équipement terminal vers le premier nœud du réseau, lequel les envoie à un deuxième nœud, et ainsi de suite, jusqu'à ce qu'ils arrivent à l'équipement terminal B. En réalité, une étape supplémentaire est nécessaire : l'encapsulation du paquet dans une trame pour réaliser le transport sur les lignes de communication.

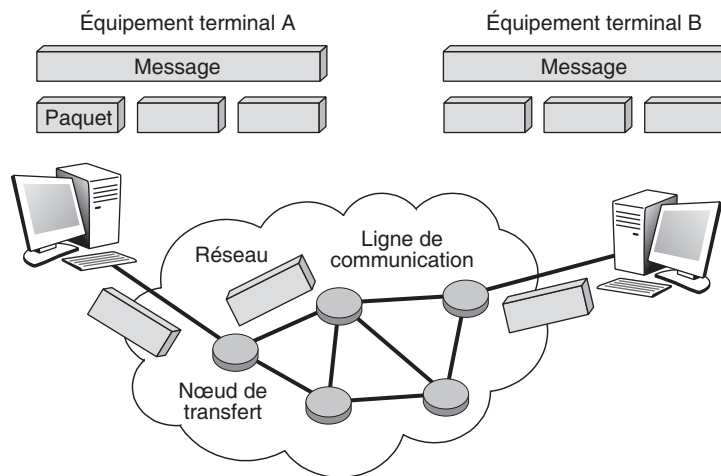


Figure 2.2

Le transfert de paquets

Le paquet peut provenir de différentes sources. La figure 2.2 suppose que la source est un message préparé par l'émetteur, tel qu'une page de texte éditée au moyen d'un traitement de texte. Le terme message est en fait beaucoup plus vaste et recoupe toutes les formes sous lesquelles de l'information peut se présenter. Cela va d'une page Web à un flot de parole téléphonique représentant une conversation.

Dans la parole téléphonique, l'information est regroupée pour être placée dans un paquet, comme illustré à la figure 2.3. Le combiné téléphonique contient un équipement qui transforme la parole analogique en une suite d'éléments binaires. Ces bits remplissent petit à petit le paquet. Dès que celui-ci est plein, il est émis vers le destinataire. Une fois le paquet arrivé à la station terminale, le processus inverse s'effectue, restituant les bits régulièrement à partir du paquet pour reconstituer la parole téléphonique.

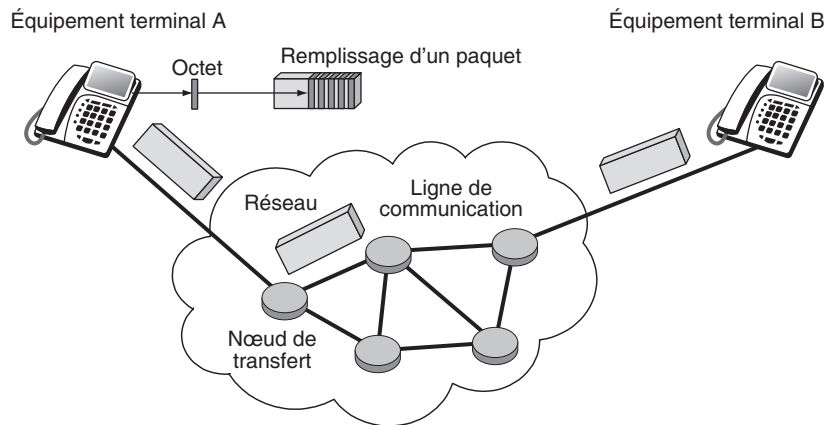


Figure 2.3

Flot de paquets téléphoniques

Le réseau de transfert est composé de nœuds, appelés nœuds de transfert, reliés entre eux par des lignes de communication sur lesquelles sont émis les éléments binaires constituant les paquets. Le travail d'un nœud de transfert consiste à recevoir des paquets et à déterminer vers quel nœud suivant ces derniers doivent être acheminés.

Le paquet forme donc l'entité de base, transférée de nœud en nœud jusqu'à atteindre le récepteur. Suivant les cas, ce paquet peut être regroupé avec d'autres afin de reconstituer l'information transmise. L'action consistant à remplir un paquet avec des octets s'appelle la mise en paquet, ou encore la paquétisation, et l'action inverse, consistant à retrouver un flot d'octets à partir d'un paquet, la dépaquétisation.

L'architecture d'un réseau est définie principalement par la façon dont les paquets sont transmis d'une extrémité à une autre du réseau. De nombreuses possibilités existent pour cela, comme celles consistant à faire passer les paquets toujours par la même route ou, au contraire, à les faire transiter par des routes distinctes de façon à minimiser les délais de traversée.

Le modèle de référence

Pour identifier correctement toutes les composantes nécessaires à la bonne marche d'un réseau à transfert de paquets, un modèle de référence a été mis au point. Ce modèle définit une partition de l'architecture en sept niveaux, prenant en charge l'ensemble des fonctions nécessaires au transport et à la gestion des paquets. Ces sept couches de protocoles ne sont pas toutes indispensables, notamment aux réseaux sans visée généraliste. Chaque niveau, ou couche, offre un service au niveau supérieur et utilise les services du niveau inférieur.

Pour offrir ces services, les couches disposent de protocoles, qui appliquent les algorithmes nécessaires à la bonne marche des opérations, comme l'illustre la figure 2.4, où l'architecture protocolaire est découpée en sept niveaux, ce qui est le cas du modèle de référence.

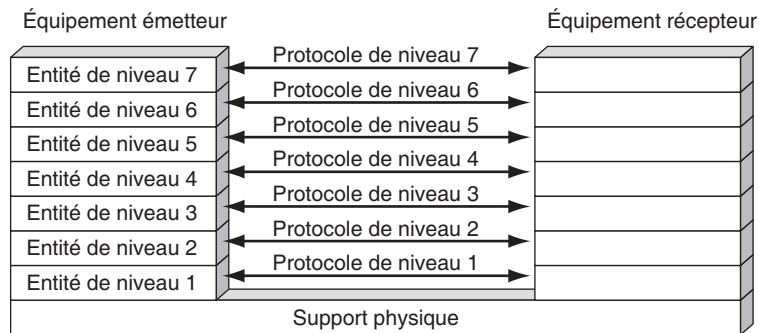
Il faut noter que si ce modèle n'est plus utilisé dans la réalité, il continue néanmoins à définir les termes et à servir de référence pour indiquer les fonctions réseau. Les architectures utilisées aujourd'hui sont celle d'Internet, représentée par le sigle TCP/IP, qui regroupe les deux principaux protocoles utilisés, et celle de l'ONF (Open Networking Foundation), qui décrit les réseaux SDN (Software-Defined Networking). Ces deux architectures ne sont d'ailleurs pas inconciliables puisque le SDN utilise les protocoles IP et TCP.

La couche 3 du modèle de référence, ou couche réseau, représente le niveau paquet, qui définit les algorithmes nécessaires pour que les entités de cette couche, les paquets, soient acheminées correctement de l'émetteur au récepteur. La couche 7 correspond au niveau application. Le rôle du protocole de la couche 7 est de transporter correctement l'entité de niveau application, le message utilisateur, de l'équipement émetteur à l'équipement récepteur.

La couche 2, ou couche liaison, représente le niveau trame. Elle permet de transférer le paquet sur une ligne physique. En effet, un paquet ne contenant pas de délimiteur, le récepteur ne peut en déterminer la fin ni identifier le commencement du paquet suivant. Pour transporter un paquet, il faut donc le mettre dans une trame, qui, elle, comporte des délimiteurs. On peut aussi encapsuler un paquet dans un autre paquet, lui-même encapsulé dans une trame.

Cet ouvrage distingue les mots «paquet» et «trame» de façon à bien faire ressortir les entités qui ne sont pas transportables directement, comme le paquet IP, et les entités transportables directement par la couche physique, comme les trames Ethernet ou ATM.

La structure en couches de l'architecture protocolaire des réseaux simplifie considérablement leur compréhension globale et facilite leur mise en œuvre. Il est possible de remplacer une couche par une autre de même niveau sans avoir à toucher aux autres couches. On peut, par exemple, remplacer la couche 3 par une couche 3 prime (3') sans modifier les couches 1, 2, 4, 5, 6 ou 7. On ne modifie de la sorte qu'une partie de l'architecture, la couche 3, sans toucher au reste. Les interfaces entre les couches doivent être respectées pour réaliser ces substitutions : l'interface de la couche 3' avec les couches 2 et 4 doit garantir que celles-ci n'ont pas à être modifiées.

**Figure 2.4**

Architecture protocolaire d'un réseau à sept niveaux

L'architecture illustrée à la figure 2.4 sert de référence à toutes les architectures réseau, d'où son nom de modèle de référence. Une autre architecture protocolaire, l'architecture TCP/IP (Transmission Control Protocol/Internet Protocol), a été définie un peu avant le modèle de référence. Son rôle premier était d'uniformiser l'interface extérieure des différents réseaux utilisés par le département américain de la Défense de façon à les interconnecter facilement. C'est cette architecture TCP/IP qui a été adoptée pour le réseau Internet, ce qui lui a offert une diffusion massive.

Une autre architecture provenant de l'utilisation de la trame plutôt que du paquet a été proposée par l'UIT-T (Union internationale des télécommunications-standardisation du secteur télécommunications) pour les applications utilisant à la fois les données, la téléphonie et l'image. Provenant principalement du monde des télécommunications, cette architecture est bien adaptée au transport de flux continu, comme la parole téléphonique. C'est la trame ATM qui représente le mieux cette architecture. Cependant, celle-ci a pratiquement disparu, pour être remplacée par la trame Ethernet. En 2012, une nouvelle architecture a été introduite, le SDN, qui utilise la puissance du Cloud pour effectuer les calculs des routes ou des chemins. La révolution apportée par cette architecture concerne la centralisation des décisions, qui étaient auparavant distribuées. Cette nouvelle architecture est examinée en détail au chapitre 12, dévolu aux réseaux SDN.

Commutation et routage

Sous le concept de transfert de paquets, deux grandes techniques se disputent la suprématie : la commutation de paquets et le routage de paquets. Dans le routage, les paquets d'un même client peuvent prendre des routes différentes, tandis que, dans la commutation, tous les paquets d'un même client suivent un chemin déterminé à l'avance. De nombreuses variantes de ces techniques ont été proposées, que nous détaillons dans la suite de l'ouvrage.

Certaines applications, comme la parole téléphonique, posent des problèmes spécifiques de transport lorsqu'elles sont acheminées sous forme de paquets. La difficulté réside dans

la récupération du synchronisme, le flot de parole devant être reconstitué au récepteur avec des contraintes temporelles fortes.

En supposant qu'une conversation téléphonique entre deux individus accepte un retard de 150 millisecondes, il n'est possible de resynchroniser les octets à la sortie que si le temps total de paquetsation-dépaquetsation et de traversée du réseau est inférieur à 150 millisecondes. Des fonctions intelligentes implémentées dans les terminaux informatiques permettent cette resynchronisation. Si un terminal ne dispose pas d'une telle intelligence, la reconstruction du flux synchrone est quasiment impossible après la traversée d'un réseau à transfert de paquets un tant soit peu complexe. Les réseaux de type Internet ont du mal à prendre en compte ces contraintes.

Les réseaux informatiques

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que stations de travail ou serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et de la vidéo est généralisée dans les réseaux informatiques, même si cela ne va pas sans difficulté.

On distingue généralement cinq catégories de réseaux informatiques, différenciées par la distance maximale séparant les points les plus éloignés du réseau :

- Les réseaux personnels, ou PAN (Personal Area Network), qui interconnectent sur quelques mètres des équipements personnels tels que téléphone mobile, portables, organiseurs, etc., d'un même utilisateur.
- Les réseaux locaux, ou LAN (Local Area Network), qui correspondent par leur taille aux réseaux intra-entreprise. Ils servent au transport de toutes les informations numériques de l'entreprise. En règle générale, les bâtiments à câbler s'étendent sur plusieurs centaines de mètres. Les débits de ces réseaux vont aujourd'hui de quelques mégabits par seconde à plusieurs centaines de mégabits par seconde.
- Les réseaux métropolitains, ou MAN (Metropolitan Area Network), qui permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole. Ils doivent être capables d'interconnecter les réseaux locaux des différentes entreprises pour leur donner la possibilité de dialoguer avec l'extérieur.
- Les réseaux régionaux, ou RAN (Regional Area Network), qui ont pour objectif de couvrir une large surface géographique. Dans le cas des réseaux sans fil, les RAN peuvent avoir une cinquantaine de kilomètres de rayon, ce qui permet, à partir d'une seule antenne, de connecter un très grand nombre d'utilisateurs. Cette solution a profité du dividende numérique, c'est-à-dire des bandes de fréquences de la télévision analogique qui ont été libérées après le passage au tout-numérique, à la fin de 2011 en France.
- Les réseaux étendus, ou WAN (Wide Area Network), qui sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et il utilise en ce cas des infrastructures

au niveau du sol, essentiellement de grands réseaux de fibre optique, soit hertzien, comme les réseaux satellite, mais seulement pour des applications particulières à débit faible.

La figure 2.5 illustre sommairement ces grandes catégories de réseaux informatiques.

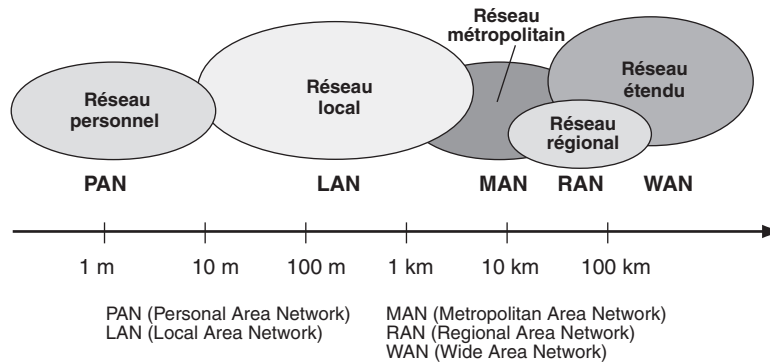


Figure 2.5

Les grandes catégories de réseaux informatiques

Les techniques utilisées par les réseaux informatiques proviennent toutes du transfert de paquets IP (Internet Protocol) généralement encapsulés dans des trames Ethernet. Ces techniques sont étudiées tout au long de l'ouvrage.

Une caractéristique essentielle des réseaux informatiques, qui les différencie des autres catégories de réseaux présentées dans la suite de ce chapitre, est la gestion et le contrôle du réseau, qui sont effectués en grande partie par les équipements terminaux. Par exemple, pour qu'il n'y ait pas d'embouteillage de paquets dans le réseau, l'équipement terminal doit se réguler lui-même. Pour cela, l'équipement terminal mesure le temps de réponse aller-retour. Si ce temps de réponse grandit trop, le terminal ralentit son débit. Cette fonctionnalité est rendue possible par l'intelligence qui se trouve dans les machines terminales commercialisées par l'industrie informatique.

Généralement beaucoup plus simple, l'intérieur du réseau est constitué de nœuds de transfert élémentaires et de lignes de communication. Le coût du réseau est surtout supporté par les équipements terminaux, qui possèdent toute la puissance nécessaire pour réaliser, contrôler et maintenir les communications.

Les réseaux informatiques forment un environnement asynchrone. Les données arrivent au récepteur à des instants qui ne sont pas définis à l'avance, si bien que les paquets peuvent mettre un temps plus ou moins long pour parvenir à leur destinataire en fonction de la saturation du réseau. Cette caractéristique explique la difficulté de faire passer de la parole téléphonique dans ce type de réseau, puisque cette application fortement synchrone nécessite de remettre au combiné téléphonique des octets à des instants précis. La suite de l'ouvrage se penche les moyens de retrouver cette synchronisation dans un réseau asynchrone.

Aujourd'hui, le principal réseau informatique est Internet. Le réseau Internet transporte des paquets dits IP. Plutôt que de parler de réseau Internet, mieux vaut parler de réseau IP, qui marque une plus grande généralité. Les réseaux IP sont des réseaux qui transportent des paquets IP d'une machine terminale à une autre. En un certain sens, Internet est un réseau IP particulier. D'autres réseaux, comme les réseaux intranet, transportent également des paquets IP, mais avec des caractéristiques différentes. Les réseaux de type SDN (Software-Defined Networking) avec routage sont également des réseaux utilisant le protocole TCP/IP, mais les calculs des tables de routage sont effectués de façon centralisée par un contrôleur.

Les réseaux de télécommunications

Les opérateurs et les industriels des télécommunications ont une vision des réseaux différente de celle des informaticiens. Leur application de base, la parole téléphonique, impose de sévères contraintes, telles que la synchronisation aux extrémités ou le temps de traversée du réseau, qui doit être limité. À l'inverse des réseaux informatiques, qui partent d'un environnement asynchrone et doivent l'adapter pour accepter des applications synchrones, les réseaux de télécommunications sont fondés par essence sur le passage d'applications fortement synchrones.

La parole est une application temps réel, qui exige que les signaux soient remis au récepteur à des instants précis dans le temps. On dit que cette application est isochrone pour bien préciser cette demande de forte synchronisation.

La solution qui a été utilisée quasiment depuis les débuts des télécommunications pour résoudre le problème de la synchronisation est la commutation de circuits. Cette technique consiste à mettre en place entre l'émetteur et le récepteur un circuit physique n'appartenant qu'aux deux utilisateurs en relation. La synchronisation correspond à la remise d'un octet à intervalle régulier. Comme on l'a vu précédemment, un équipement appelé codec (codeur-décodeur) transforme la parole en octet à l'émetteur et fait la démarche inverse au récepteur. Le codec doit recevoir les échantillons d'un octet à des instants précis. La perte d'un échantillon de temps en temps n'est pas catastrophique, puisqu'il suffit de remplacer l'octet manquant par le précédent. En revanche, si ce processus de perte se répète fréquemment, la qualité de la parole se détériore.

Les réseaux de télécommunications orientés vers le transport de la parole téléphonique sont relativement simples et n'ont pas besoin d'une architecture complexe. Ils utilisent des commutateurs de circuits, ou autocommutateurs. Il y a une trentaine d'années, lorsqu'on a commencé à imaginer des réseaux intégrant la téléphonie et l'informatique, la seule solution proposée se fondait sur des circuits, un pour la parole téléphonique et un autre pour faire circuler les paquets de données.

Des recherches menées au début des années 1980 ont conduit les industriels et les opérateurs des télécommunications à adopter le transfert de paquets, mais en l'adaptant au transport intégré de l'information (parole téléphonique plus données informatiques). Appelée Asynchronous Transfer Mode (ATM), ou mode de transfert asynchrone, cette technique est un transfert de paquets très particulier, dans lequel tous les paquets ont une

longueur à la fois fixe et très petite. Ce paquet dont la longueur est constante est appelé une trame. Il est simple d'y retrouver le début et la fin puisqu'il suffit de compter le nombre d'octets. Avec l'adoption, en 1988, du transfert de trames ATM, le monde des télécommunications a connu une véritable révolution.

La technique ATM n'a cependant pu résister à l'arrivée massive d'Internet et de son paquet IP. Toutes les machines terminales provenant du monde informatique ayant adopté l'interface IP, le problème du transfert des paquets est devenu celui des paquets IP. Le monde des télécommunications admet, depuis le début des années 2000, que les réseaux doivent posséder des interfaces IP. Ce qui fait encore débat, c'est la façon de transporter les paquets IP d'un terminal à un autre. Le monde des télécommunications propose, comme l'examine en détail la suite de l'ouvrage, d'encapsuler le paquet IP dans une trame puis de transporter cette trame et de la décapsuler à l'arrivée pour retrouver le paquet IP.

La figure 2.6 illustre le cas général où le paquet IP est encapsulé dans une trame, classiquement la trame Ethernet, laquelle est transportée dans le réseau de transfert. Le cas de l'encapsulation dans un réseau ATM demande une étape supplémentaire, consistant à découper le paquet IP, puisque la trame ATM est beaucoup plus petite que lui.

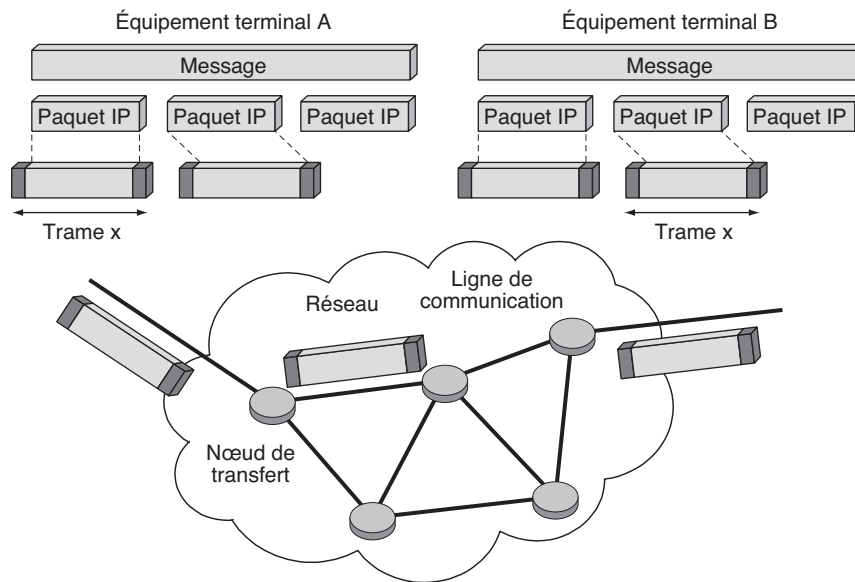


Figure 2.6

Encapsulation du paquet IP dans une trame

Les réseaux de nouvelle génération, dits SDN, utilisent principalement la commutation, mais supportent également le routage. Le contrôleur possède une connaissance approfondie des clients et des applications *via* son interface nord et une vision complète du réseau et

de son utilisation *via* l'interface sud. Grâce à cet ensemble de connaissances, le contrôleur peut calculer le meilleur chemin satisfaisant la demande du client.

La signalisation dans le SDN est donc centralisée, contrairement aux techniques précédentes, qui sont toutes distribuées. Le système de signalisation, réalisé sur l'interface sud, s'appelle OpenFlow, il a été normalisé par l'ONF (Open Networking Foundation). Cette signalisation n'est toutefois pas la seule solution disponible (*voir le chapitre 12*).

En résumé, les réseaux de télécommunications sont passés d'une technologie circuit à une technologie paquet. Malgré le succès du transfert ATM, optimisé pour le multimédia, le recours au paquet IP et à son encapsulation dans une trame Ethernet est devenu incontournable. La question déterminante réside dans la façon de transporter le paquet IP pour assurer une qualité de service.

Les réseaux de câblo-opérateurs

Les opérateurs vidéo et les câblo-opérateurs ont pour mission de mettre en place des réseaux câblés et hertziens chargés de transmettre les images de télévision par la voie terrestre ou hertzienne. Cette infrastructure de communication fait transiter des canaux vidéo vers l'utilisateur final. L'amortissement du câblage ou des relais hertziens passe par la mise à disposition des utilisateurs de nombreux canaux de télévision.

Les opérateurs hertziens assurent depuis de longues années la diffusion de canaux de télévision. Leur réseau était essentiellement analogique jusqu'au début des années 2000. Sa numérisation est finalisée depuis 2011 en France, aussi bien pour la télévision par satellite que pour la TNT (télévision numérique terrestre), par le biais de relais numériques terrestres dans ce dernier cas.

La qualité des images vidéo est d'une grande variété, depuis les images saccadées et de faible définition jusqu'aux images animées de très bonne qualité. La classification des applications vidéo, effectuée suivant le niveau de qualité des images, est généralement la suivante :

- **Visioconférence.** D'une définition relativement faible, sa fonction est de montrer le visage du correspondant. Pour gagner en débit, on diminue le nombre d'images par seconde. La visioconférence se transporte aisément sur un canal numérique à 128 kbit/s au moyen d'une compression simple à réaliser. On peut abaisser le débit jusqu'à 64 kbit/s, voire moins, au prix d'une qualité dégradée.
- **Télévision.** Correspond à un canal de 4 ou 5 MHz de bande passante en analogique. La numérisation de ce canal permet d'obtenir un débit de plus de 200 Mbit/s. Grâce à la compression, on peut faire descendre ce débit à 2 Mbit/s, pratiquement sans perte de qualité, voire à quelques centaines de kilobits par seconde avec une compression poussée, mais au prix d'une qualité parfois dégradée. De plus, à de tels débits, les erreurs en ligne deviennent gênantes, car elles perturbent l'image au moment de la décompression. Un compromis est à trouver entre une forte compression et un taux d'erreur de 10^{-9} , qui ne détruit qu'une infime fraction de l'image et ne gêne pas sa vision. La transmission se fait selon les normes DVB-T (Digital Video Broadcasting-Terrestrial), notamment en Europe, ISDB (Integrated Service Digital Broadcasting), au Japon et en Amérique

du Sud et ATSC (Advanced Television Systems Committee) en Amérique du Nord. Les deux standards pour le flot de transmission d'un canal de télévision numérique sont aujourd'hui H.262 / MPEG-2 et H.264 / MPEG-4.

H.264 ou MPEG-4 AVC (Advanced Video Coding) est un format de codage pour l'enregistrement et la distribution de la vidéo et de l'audio en Full HD. Ce standard a été développé et est pris en charge par l'UIT-T VCEG (Video Coding Experts Group) et l'ISO/IEC JTC1 MPEG (Moving Picture Experts Group).

Les améliorations incessantes apportées aux codecs devraient permettre dans quelques années de faire passer un canal de télévision sur une bande encore plus restreinte, tout en y ajoutant de nouvelles fonctionnalités.

- **Télévision haute définition (HDTV).** Demande des transmissions à plus de 500 Mbit/s si aucune compression n'est effectuée. Après compression, on peut descendre à une valeur de l'ordre de 8 Mbit/s. Par exemple, sur un canal DVB-T de 24 Mbit/s, il est possible de faire transiter trois canaux de télévision haute définition.
- **Télévision 3D.** Cette nouvelle génération requiert des débits encore plus importants puisqu'elle consiste à transporter plusieurs images pour en obtenir une seule donnant l'impression d'être en trois dimensions. Après compression, on peut descendre à une valeur de l'ordre de 20 Mbit/s.
- **Télévision ultra-haute définition (UHDTV).** C'est un format numérique de vidéo dont la caractéristique principale est une définition de l'image comportant quatre à seize fois plus de pixels que la télévision haute définition (HDTV). 4K est un format d'images numériques ayant une définition supérieure ou égale à 4096 pixels de large.
- **Vidéoconférence.** Ce terme générique désigne une conférence entre deux ou plusieurs utilisateurs qui s'effectue par le biais de réseaux de télécommunications. On peut aussi prendre comme définition de la vidéoconférence la très haute qualité. Proche du cinéma, la qualité vidéoconférence requiert des débits considérables, de plusieurs dizaines de mégabits par seconde. Compte tenu de ces débits, ce type de canal n'est accessible qu'avec l'utilisation d'un câblage en fibre optique jusqu'à l'utilisateur et en utilisant des codecs (codeur-décodeur) spécialisés assez onéreux. Un cas particulier, qui s'est développé depuis les années 2010 dans les très grandes entreprises, concerne les murs de présence : il s'agit de projeter sur un mur une vidéoconférence de haute qualité avec un son stéréophonique et une transmission en temps réel.

Les câblo-opérateurs se préoccupent en premier lieu de diffuser des images animées de type TV. Les structures de câblage mises en place pour cela permettent de diffuser chez l'utilisateur de nombreux canaux de télévision, qui se comptent aujourd'hui par centaines.

Les applications vidéo vont de la télésurveillance à la vidéo à la demande, ou VoD (Video on Demand), en passant par la messagerie vidéo et le Home Media Center domestique pour la diffusion vidéo généralisée à l'échelle d'une maison.

Les réseaux câblés utilisés par les diffuseurs sur la partie terminale du réseau de distribution sont appelés CATV (Community Antenna TeleVision). Le CATV utilise un câble coaxial de 75 Ω , dont la largeur de bande dépasse 1 GHz. On l'utilise aussi comme câble d'antenne de télévision. Il s'agit d'un support unidirectionnel, qui implique d'envoyer le

signal vers un centre, lequel le rediffuse à toutes les stations connectées, contrairement à ce qui se passe, par exemple, dans le réseau Ethernet, où le signal est diffusé dans les deux sens du support physique.

Dans un réseau CATV, la diffusion des chaînes de télévision s'effectue facilement du centre vers la périphérie. Pour ajouter des canaux dans le sens inverse, du client vers la tête de réseau, des accès Internet par exemple, on divise la bande passante en deux : une partie pour aller vers la tête de réseau, l'autre desservant les utilisateurs. On parle en ce cas de bande montante et de bande descendante.

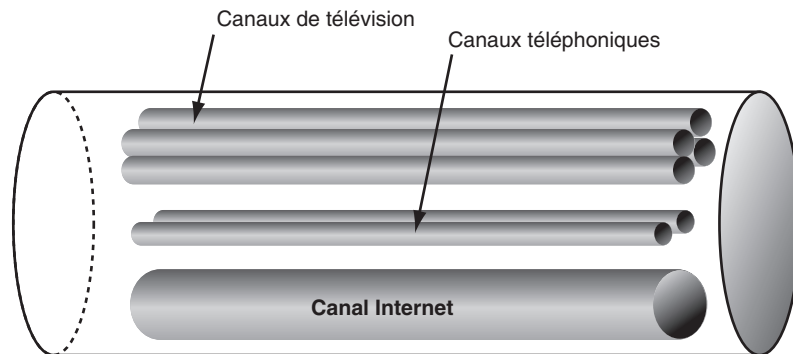
Depuis que le prix de revient de la fibre optique et des connecteurs associés est devenu concurrentiel, on l'utilise de plus en plus à la place du câble coaxial. La bande passante de la fibre optique est beaucoup plus importante et permet d'augmenter très fortement le débit des accès Internet.

Les réseaux câblés ont été exploités pendant longtemps en analogique et non en numérique. Les débits sont aujourd'hui suffisants pour y faire transiter des applications multimédias. Cependant, la principale difficulté est de faire transiter plusieurs milliers de canaux montants du terminal vers le réseau sur un canal partagé d'une capacité limitée. Mille clients émettant potentiellement à 1 Mbit/s représentent un débit total de 1 Gbit/s, ce qui est généralement nettement plus que la bande disponible sur la partie montante. Il faut donc très souvent une technique de partage du canal pour arbitrer les accès montants des utilisateurs.

Dans certains pays, comme les États-Unis, les foyers constituent pour les câblo-opérateurs une porte d'entrée simple vers l'utilisateur final. Le câblage, qui est une des clés de la diffusion généralisée de l'information, a été durant de nombreuses années l'objet de toutes les convoitises des opérateurs de télécommunications. Le succès des techniques xDSL, utilisant le câblage téléphonique, a toutefois limité l'impact des réseaux câblés. Le déploiement de la fibre optique, de la TNT et des réseaux de mobiles 4G a fortement réduit l'intérêt de ces réseaux. Ce sera encore plus vrai avec les réseaux 5G.

La principale technique utilisée par les câblo-opérateurs pour transporter les canaux de télévision est le multiplexage en fréquence, qui consiste en une partition de la bande passante en sous-bandes. Chaque sous-bande transporte un canal de télévision. Cette solution est illustrée à la figure 2.7.

Le multiplexage en fréquence d'un grand nombre de sous-bandes présente l'inconvénient de requérir autant de types de récepteurs que de canaux à accéder. Il faut un décodeur pour la télévision, un modem câble pour Internet et un accès téléphonique pour la parole numérique. Les techniques de multiplexage temporel, dans lesquelles le temps est découpé en petites tranches affectées régulièrement aux utilisateurs, sont beaucoup plus puissantes puisqu'un même émetteur-récepteur permet de recevoir tous les canaux.

**Figure 2.7**

Multiplexage en fréquence dans le CATV

En conclusion, la technique employée par les câblo-opérateurs permet une intégration dans le CATV d'un grand nombre d'applications utilisant des sous-bandes différentes, adaptées à différents types de transmissions. Son principal inconvénient vient du multiplexage en fréquence, qui conduit les câblo-opérateurs à utiliser un grand nombre de bandes en parallèle. Ces bandes peuvent être considérées comme des canaux de communication indépendants les uns des autres, de telle sorte qu'il n'y a pas d'intégration des flux : un client peut utiliser en parallèle un canal de télévision, un canal d'accès Internet et un canal pour la téléphonie. Le canal de télévision est connecté à un câblo-opérateur, le canal d'accès Internet à un opérateur Internet et le canal de téléphonie à un opérateur téléphonique. L'intégration de ces différents réseaux chez un même opérateur est aujourd'hui une réalité mise en lumière tout au long de ce livre.

L'intégration des réseaux

Les sections précédentes ont introduit brièvement les trois grandes catégories de réseaux, informatique, de télécommunications et des câblo-opérateurs, qui se proposent de transporter les données informatiques, la parole téléphonique et la vidéo. Chacun de ces réseaux essaie aujourd'hui de prendre en charge les trois médias simultanément pour tendre vers un réseau intégré. Cette section détaille les caractéristiques d'une telle intégration des réseaux dans un réseau multimédia, ainsi que les contraintes qu'il doit supporter.

Le monde des télécommunications a adopté diverses solutions pour doter ses réseaux de commutation de solutions permettant d'obtenir une qualité de service satisfaisante. La première d'entre elles a consisté à utiliser des chemins associés à une classe de service. Les paquets suivant ce chemin étaient traités en priorité dans le commutateur. Cette solution a ensuite évolué vers l'ingénierie de trafic. Au moment de l'ouverture du chemin, le paquet de signalisation note, dans chaque commutateur, les caractéristiques du trafic ayant été négociées entre le client et l'opérateur du réseau. Cette négociation donne naissance à un SLA (Service Level Agreement), présenté en détail au chapitre 23. Grâce à ces

informations, les nœuds peuvent décider de laisser passer ou non un paquet de signalisation souhaitant ouvrir un chemin. Il est donc relativement simple de négocier une qualité de service correspondant aux différentes applications des réseaux multimédias.

Les réseaux de routage ont bien plus de difficulté à garantir cette qualité de service puisqu'il ne peut y avoir de réservation de ressources et qu'il n'est pas possible de déterminer à l'avance les routeurs par lesquels doivent passer les paquets d'un même flot. Une première solution à ce problème consiste à surdimensionner le réseau pour que les paquets s'écoulent de façon fluide. Si cette solution était acceptable entre 2000 et 2005 grâce à l'importante capacité de transport développée lors de la « bulle Internet », ce n'est plus le cas aujourd'hui.

Une nouvelle solution a été proposée consistant à introduire une classification des clients et à ne surdimensionner que ceux de plus haute priorité. Cela suppose de discriminer les clients, soit par le paiement d'un abonnement plus élevé, soit en restreignant le nombre de clients de l'application considérée. La téléphonie sur IP fonctionne grâce à cette solution. Seuls les paquets IP sortant de téléphones IP se voient affecter la priorité la plus haute. En calculant le nombre maximal de voies téléphoniques pouvant s'écouler sur chaque liaison, on peut en déduire la capacité de la ligne pour qu'elle soit vue comme surdimensionnée.

Les dernières évolutions apportent une nouvelle solution avec le SDN en ouvrant des chemins parfaitement adaptés aux flots qui doivent y transiter. Le SDN devrait représenter environ 20 % du marché des réseaux en 2020 et beaucoup plus en 2025.

Conclusion

Ce chapitre a introduit les premiers concepts des réseaux. La convergence de ces réseaux provenant de différents horizons, comme l'informatique, les télécommunications et la vidéo, vers un réseau unique est maintenant achevée.

Le chapitre s'est en outre arrêté sur le passage des réseaux transportant les informations sous forme analogique aux réseaux transportant les informations sous forme numérique. Les réseaux numériques se sont développés en proposant plusieurs options, le routage et la commutation, et en utilisant aussi bien des supports physiques terrestres que des transmissions radio.

Aujourd'hui, les réseaux analogiques ont quasiment disparu, sauf pour des applications très spécifiques, comme la téléphonie pour la communication entre un contrôleur aérien et un avion, pour des raisons de fiabilité et de disponibilité. Mais même dans ce cas, le passage au numérique s'effectuera dans quelques années. Les raisons en sont le coût des équipements et la réutilisation simple des composants numériques qui n'utilisent que deux valeurs, 0 et 1.

Les difficultés à résoudre pour la marche parfaite des réseaux hertziens et terrestres sont notamment la mise à niveau de la sécurité, la gestion du réseau global, le contrôle de la mobilité et l'introduction d'une virtualisation complète.

La suite de l'ouvrage détaille de façon graduelle toutes les solutions envisagées et examine les éléments nécessaires à la construction d'un réseau de bout en bout.

Réseaux virtuels et Cloud

Ce chapitre examine la virtualisation de réseau, qui se généralise après la virtualisation du stockage et du calcul. Le Cloud est également une lame de fond dans le domaine applicatif, mais aussi un environnement éminemment important pour l'accueil des machines virtuelles. La puissance que l'on peut y obtenir est telle que les temps de calcul pour obtenir une table de routage ou exécuter un algorithme de gestion d'un handover ou d'un contrôle de sécurité sont minimes, ce qui permet des temps de réaction particulièrement faibles.

La virtualisation de réseau

La virtualisation n'est pas une technique nouvelle, puisqu'elle avait été introduite sur les premiers gros ordinateurs dans les années 1960, qui utilisaient une mémoire virtuelle, c'est-à-dire une mémoire qui, au lieu d'être en RAM, se trouvait sur un disque dur. Toute l'astuce était de ramener les pages de mémoire du disque dur sur la mémoire RAM juste avant que l'unité centrale en ait besoin. Par la suite, un certain nombre de mécanismes ont été implémentés avec cette solution afin que l'utilisateur ait l'impression que les services dont il a besoin se trouvent sur une machine située à proximité, alors qu'ils se trouvent en réalité sur une machine lointaine.

La virtualisation du stockage a connu un formidable succès en permettant de regrouper plusieurs serveurs de stockage sur une machine unique, chaque utilisateur ayant pourtant l'impression de disposer d'un serveur distinct. La virtualisation de réseau tient du même principe : plusieurs réseaux virtuels se partagent une même infrastructure physique.

La virtualisation de réseau a été lancée par un projet américain appelé GENI (Global Environment for Network Innovations), dans lequel Intel proposait de construire un routeur uniquement constitué de sa partie matérielle, sans aucun système d'exploitation réseau. Les éditeurs de logiciels n'avaient plus qu'à implémenter leur système sur la

machine. L'avantage de la virtualisation réside précisément dans la possibilité d'implémenter plusieurs systèmes d'exploitation réseau sur une même machine à l'aide d'un « hyperviseur ».

L'architecture d'un serveur de virtualisation permettant de prendre en charge plusieurs machines virtuelles sur des systèmes d'exploitation différents se présente comme illustré à la figure 3.1.

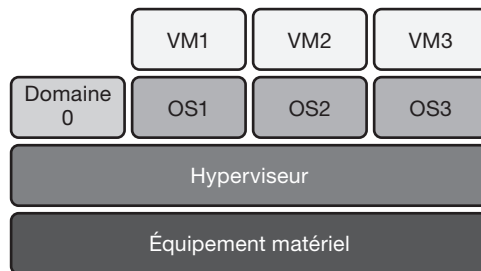


Figure 3.1

Architecture d'un serveur de virtualisation

Sur cette figure, un équipement matériel, par exemple un serveur d'un datacenter, possède un hyperviseur. L'hyperviseur est un système d'exploitation spécifique capable de supporter plusieurs systèmes d'exploitation, qui, eux-mêmes, supportent des machines virtuelles, ou VM (Virtual Machine).

Les machines virtuelles peuvent être très diverses, comme un routeur, un commutateur, un logiciel de traitement du signal, un boîtier, etc. Le nombre de machines virtuelles supportées dépend de la puissance de la machine physique, du nombre d'unités centrales et de la capacité des mémoires de stockage. Si les machines virtuelles dépensent peu de ressources, plusieurs dizaines d'entre elles peuvent s'exécuter simultanément.

Une VM (machine virtuelle) spécifique, appelée domaine 0, permet de réaliser les entrées-sorties des autres machines virtuelles. Elle est détaillée à la section de ce chapitre consacrée à l'hyperviseur Xen.

La VM est elle-même un logiciel qui décrit exactement ce que fait la machine physique que l'on veut virtualiser. Le code représente la VM. Les avantages immédiats de cette virtualisation sont l'agilité et la flexibilité qu'elle procure. Par exemple, on peut facilement changer de VM sans toucher à la partie matérielle et remplacer un routeur par un commutateur en quelques secondes. En revanche, la consommation énergétique augmente puisqu'il faut beaucoup plus de puissance de la part de l'unité centrale lorsqu'on virtualise le travail d'un ASIC (Application Specific Integrated Circuit), c'est-à-dire d'un élément matériel spécialisé.

Un autre avantage de la virtualisation est de permettre le regroupement des machines virtuelles sur un même serveur lorsque celles-ci sont peu utilisées, comme des routeurs durant la nuit. Ces regroupements s'effectuent par migration d'une VM d'un serveur

physique vers un autre serveur physique. Un des moyens de regagner l'énergie perdue par une demande supplémentaire d'unité centrale est de regrouper les machines virtuelles et de mettre en veille les serveurs qui n'ont plus de machines virtuelles à exécuter. En règle générale, on n'éteint pas les machines physiques, mais on les met en veille afin de permettre un redémarrage immédiat ou quasi immédiat lorsque le système a de nouveau besoin de plus de puissance.

Un routeur virtuel n'est ainsi qu'une instance logique d'un routeur physique. Plusieurs routeurs virtuels peuvent s'exécuter en même temps sur un même serveur physique, avec les entrées-sorties nécessaires pour réaliser complètement le routeur physique. On obtient alors la possibilité de déployer plusieurs réseaux, que l'on peut appeler des réseaux virtuels, sur un même réseau physique. Un réseau virtuel est le regroupement d'un ensemble de machines virtuelles compatibles.

Les routeurs ou les commutateurs virtuels utilisent les liaisons physiques pour s'interconnecter. On peut même aller beaucoup plus loin en regroupant des équipements de réseau virtualisés utilisant des protocoles différents sur une même infrastructure physique. De ce fait, on peut créer des réseaux virtuels de différents types sur cette infrastructure, comme un réseau de routeurs virtuels IPv4 et un réseau avec des commutateurs virtuels pour créer un réseau MPLS (MultiProtocol Label Switching).

Aux réseaux virtuels que l'on décide de créer sur une même infrastructure peuvent s'ajouter des équipements réseau virtuels, comme des pare-feu (*firewall*), des serveurs d'authentification, des serveurs pour gérer des applications réseau telles que la voix sur IP, ou VoIP (Voice over IP). On peut également y ajouter d'autres machines virtuelles de stockage et de calcul dispersées ou regroupées dans les datacenters qui forment l'ossature de l'infrastructure.

Un tel environnement est illustré à la figure 3.2, dans laquelle les réseaux A, B, C et D coexistent sur les mêmes serveurs d'infrastructure et les mêmes lignes physiques.

Le réseau virtuel A est réalisé à partir de VM (Virtual Machine) avec le système d'exploitation A. De même, le réseau virtuel B est réalisé avec les VM B et ainsi de suite. Chaque VM d'un même serveur physique peut employer des protocoles complètement différents, et les réseaux être également totalement différents. Chacun peut utiliser les protocoles liés à une application donnée, comme la VoIP, le transfert de fichiers, la messagerie électronique, l'accès à un système de sécurité, la diffusion de vidéo, etc.

Les avantages de cette technique de virtualisation sont nombreux. Le premier est de pouvoir faire tourner sur une même infrastructure physique des réseaux virtuels utilisant des technologies totalement différentes. On peut, par exemple, obtenir un premier réseau utilisant le système d'exploitation réseau IOS de Cisco, un deuxième utilisant Junos de Juniper, un troisième et un quatrième utilisant les systèmes de Nokia et d'Ericsson, etc. Il est également possible de faire tourner plusieurs releases différentes d'un même système d'exploitation réseau. Il est évident que les exemples précédents n'ont guère de chance d'être réalisés, car les équipementiers ne souhaitent pas forcément commercialiser leur logiciel sans leur matériel. Le découplage matériel/logiciel ne sera disponible que pour

des systèmes ouverts parvenus à maturité. Le chapitre 14 donne des exemples de telles architectures open source, qui constitueront les standards des années 2020.

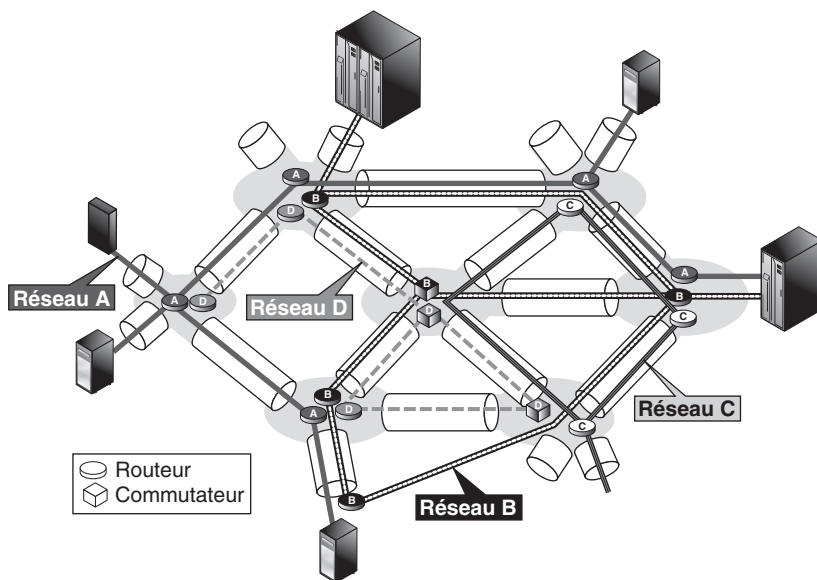


Figure 3.2

Virtualisation de routeurs

Un second avantage de la virtualisation concerne l'utilisation des ressources. Il est évident que les ressources peuvent être beaucoup mieux utilisées en mettant en marche et en arrêtant des machines virtuelles ou encore en les déplaçant : si l'une d'elles n'a pas assez de ressources sur la machine physique sur laquelle elle est placée, par exemple, il est possible de la déplacer vers d'autres serveurs physiques.

Dans tous les cas, les ressources d'un même réseau virtuel doivent être totalement isolées des autres réseaux virtuels. L'isolation interdit qu'un paquet puisse passer d'un réseau virtuel à un autre pour éviter qu'un problème sur un réseau puisse affecter un autre réseau. Le passage pourrait être permis au travers de passerelles externes particulièrement robustes pour maintenir l'isolation. Cela implique une excellente sécurité dans les logiciels de virtualisation puisqu'il faut éviter des attaques sur les hyperviseurs. Si l'une des machines virtuelles tombe en panne, non seulement cela ne doit pas affecter les autres réseaux, mais ceux-ci ne doivent pas même s'en apercevoir. Si, bien sûr, un routeur physique tombe en panne, toutes les machines virtuelles sont elles aussi en panne.

Technologies de virtualisation de réseau

Comme indiqué précédemment, les technologies de virtualisation de réseau s'appuient soit sur des hyperviseurs, soit sur des conteneurs (*containers*).

Hyperviseurs et conteneurs

On compte trois grands types de solutions pour réaliser des systèmes virtuels : la paravirtualisation, la virtualisation de système d'exploitation et l'isolation par conteneur.

Un exemple de paravirtualisation est décrit à la figure 3.3. Au-dessus du matériel de l'infrastructure, l'hyperviseur permet de supporter différents systèmes d'exploitation qui ont été modifiés afin que les instructions puissent s'exécuter directement sur le processeur de l'infrastructure. Dans cette catégorie, on trouve les hyperviseurs Citrix Xen Server (open source), VMware vSphere, VMware ESX, Microsoft Hyper-V Server, Bare Metal et KVM (open source). L'avantage de cette solution est une exécution rapide, mais à la condition de modifier un certain nombre d'éléments du système d'exploitation.

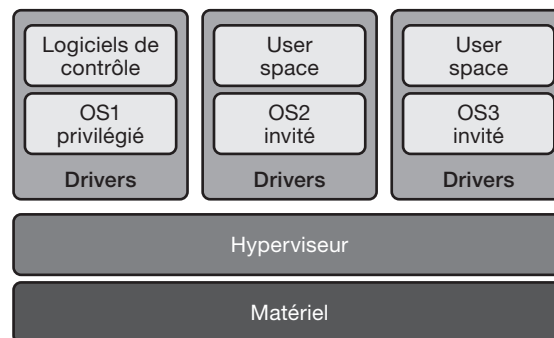
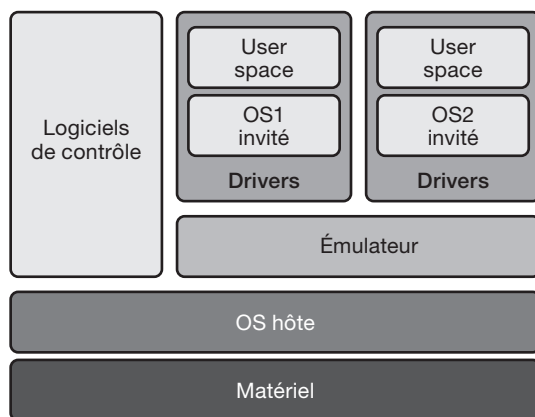


Figure 3.3

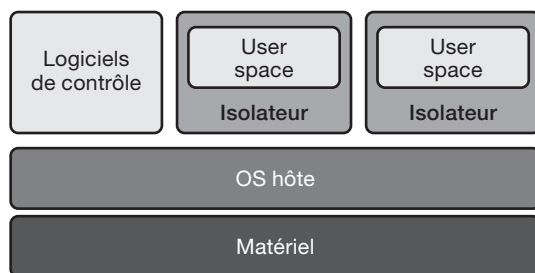
Exemple de paravirtualisation à l'aide d'un hyperviseur de type 1

Dans la deuxième solution, appelée hyperviseur de type 2, le système d'exploitation qui est supporté par l'hyperviseur n'est pas modifié. De ce fait, certaines instructions ne peuvent plus s'exécuter sur l'hyperviseur, qui est en réalité le système d'exploitation hôte de l'infrastructure physique. Il faut ajouter entre les deux, comme illustré à la figure 3.4, un émulateur qui permet d'exécuter les instructions du système d'exploitation invité sur le système d'exploitation hôte. Dans cette catégorie, on peut placer Microsoft VirtualPC, Microsoft Virtual Server, Parallels Desktop, Parallels Server, Oracle VM VirtualBox (open source), VMware Fusion, VMware Player, VMware Server, VMware Workstation et QEMU (open source).

**Figure 3.4**

Exemple de fonctionnement d'un hyperviseur de type 2

La troisième catégorie, représentée à la figure 3.5, supporte les machines virtuelles en les mettant dans des conteneurs, ou isolateurs. Le conteneur contient en lui-même un environnement d'exécution complet, avec ses pilotes, ses fichiers binaires, ou bibliothèques, ainsi que l'application elle-même. Le conteneur permet d'isoler l'exécution des applications dans ce que l'on appelle encore des contextes ou des zones d'exécution. Dans cette catégorie on peut placer Docker, Linux-Vserver, chroot, BSD Jail et OpenVZ.

**Figure 3.5**

Exemple de conteneur supportant des machines virtuelles

L'isolation

L'isolation est un principe fondamental de la virtualisation de réseau puisqu'il faut absolument éviter qu'un réseau impacte les autres réseaux.

Une première solution simple, mais peu efficace, serait de partitionner les ressources entre les différents réseaux. Dans ce cas, il n'y aurait pas grand-chose à gagner, car les ressources d'un réseau non utilisées à un instant t ne peuvent être utilisées par d'autres

réseaux virtuels. Il faut donc trouver une solution pour à la fois partitionner les ressources et faire en sorte que les ressources non utilisées puissent profiter aux autres.

On peut obtenir cette propriété par des ordonnanceurs. Le plus simple est d'avoir dans un nœud autant de files d'attente que de réseaux virtuels. À chaque file, on octroie des crédits en fonction des ressources qui ont été allouées au nœud. Chaque réseau utilise un crédit pour envoyer un paquet. Lorsqu'une station n'a plus de crédit, elle ne peut émettre. Tant qu'il y a d'autres files actives, elle est arrêtée. Si, à un moment donné, toutes les files sont vides, une réallocation de crédits est attribuée à toutes les files. Cela peut toutefois conduire à un blocage à la fois des files d'attente n'ayant plus de crédit et de celles ayant des crédits mais pas de paquets à servir. Pour éviter ce problème, les files d'attente bloquées peuvent créer des crédits négatifs et continuer à transmettre. Lorsque la somme des crédits positifs et négatifs devient égale à zéro, on réinitialise le système en accordant des crédits positifs à l'ensemble des nœuds.

On peut, à partir de cet exemple repris de Xen (<http://www.xen.org>), modifier des paramètres ou en ajouter d'autres, comme permettre à une file d'attente de servir plusieurs paquets, c'est-à-dire d'utiliser plusieurs jetons sans interruption. On utilise ainsi moins d'énergie, une même VM étant à l'œuvre sans interruption.

Xen

Xen est un hyperviseur, que l'on appelle encore moniteur de VM, ou VMM (Virtual Machine Monitor). C'est un logiciel open source qui fonctionne sur des plates-formes matérielles standards. En plus du VMM, situé sur le matériel physique, l'architecture Xen est composée de plusieurs domaines tournant de manière simultanée sur l'hyperviseur, appelés machines virtuelles (*voir figure 3.6*). Chaque VM peut avoir son propre système d'exploitation et ses applications. Le VMM contrôle l'accès au matériel des domaines multiples et gère le partage des ressources entre les différents domaines. Ainsi, une des tâches principales du VMM est d'isoler les différentes machines virtuelles, de sorte que l'exécution d'une VM n'affecte pas les performances des autres.

Tous les pilotes de périphérique sont conservés dans un domaine isolé qui leur est réservé. Appelé domaine 0 (dom0), il leur fournit un support matériel fiable et efficace. Le domaine 0 a des privilèges spéciaux comparé aux autres domaines, appelés domaines utilisateur (domU), et dispose, par exemple, d'un accès total au matériel de la machine physique. Les domaines utilisateur possèdent des pilotes virtuels et opèrent comme s'ils pouvaient accéder directement au matériel. Cependant, ces pilotes virtuels communiquent avec le dom0 afin d'avoir accès au matériel physique.

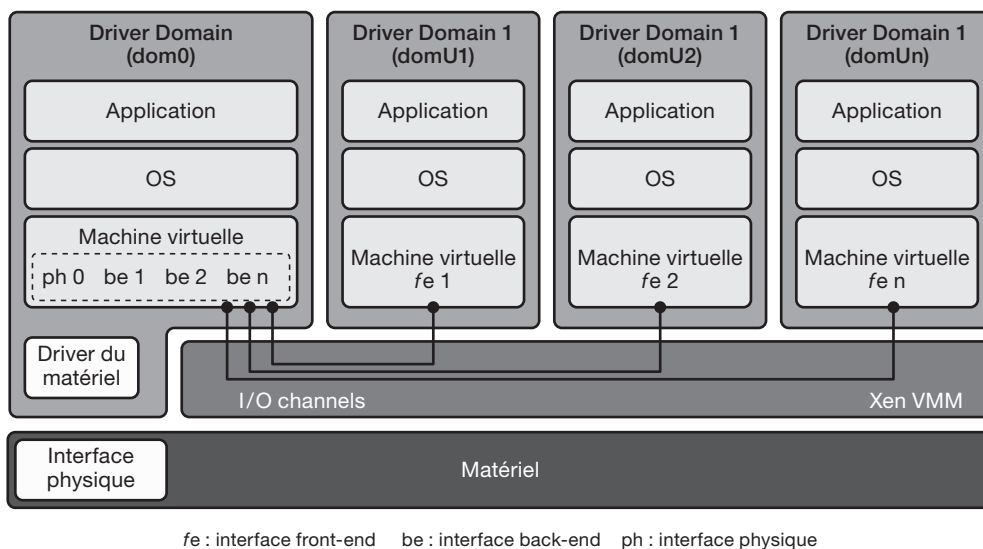


Figure 3.6

Hyperviseur Xen et machines virtuelles

Xen virtualise une interface de réseau physique unique en démultiplexant les paquets entrants de l'interface physique vers les domaines utilisateur et, de manière inverse, en multiplexant les paquets sortants générés par ces domaines utilisateur. Dans cette procédure, appelée virtualisation des entrées-sorties du réseau, le **dom0** accède directement aux périphériques d'entrées-sorties en utilisant ses pilotes de périphériques natifs et effectue des opérations d'entrées-sorties de la part des **domU**.

Les domaines utilisateur emploient des périphériques d'entrées-sorties virtuels contrôlés par des pilotes virtuels afin de demander au **dom0** l'accès au périphérique, comme illustré à la figure 3.7. Chaque domaine utilisateur possède ses propres interfaces de réseau virtuel, appelées interfaces de premier plan, requises pour les communications du réseau. Les interfaces d'arrière-plan sont créées dans le **dom0** correspondant à chaque interface de premier plan dans un domaine utilisateur et agissent en tant que proxy pour les interfaces virtuelles dans le **dom0**.

Les interfaces de premier plan et d'arrière-plan sont connectées les unes aux autres *via* un canal d'entrée-sortie qui emploie un mécanisme *zero-copy* pour remettre en correspondance la page physique contenant le paquet et le domaine cible. De cette manière, les paquets sont échangés entre les interfaces d'arrière-plan et de premier plan. Les interfaces de premier plan sont perçues par les systèmes d'exploitation fonctionnant sur les domaines utilisateur comme des interfaces réelles. Cependant, les interfaces d'arrière-plan dans le **dom0** sont connectées à l'interface physique ainsi que les unes aux autres *via* un pont réseau virtuel. C'est l'architecture par défaut, appelée mode pont, utilisée par Xen. Ainsi, à la fois le canal d'entrées-sorties et le pont réseau établissent un chemin de communication entre les interfaces virtuelles créées dans les domaines utilisateur et l'interface physique.

Différents éléments du réseau virtuel peuvent être implémentés en utilisant Xen puisque celui-ci permet à de multiples machines virtuelles de fonctionner simultanément sur le même matériel, comme le montre la figure 3.7. Dans ce cas, chaque VM fait fonctionner un routeur virtuel, qui possède ses propres plans de contrôle et de données, la couche de virtualisation de Xen étant de bas niveau.

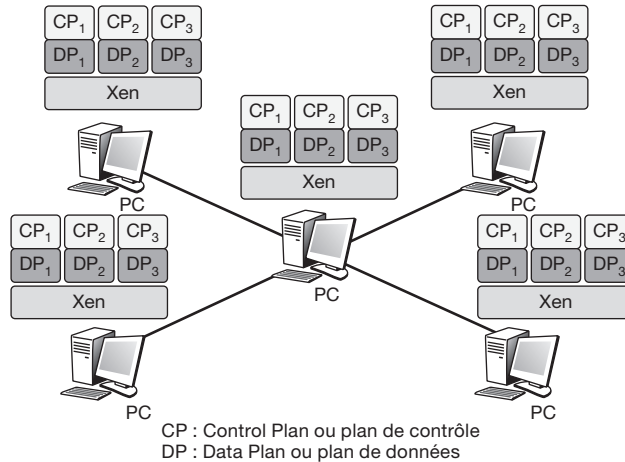


Figure 3.7

Virtualisation avec l'hyperviseur Xen

Utilisation de la virtualisation de réseau

Deux types d'utilisation peuvent être faits de la virtualisation de réseau :

- La création de plusieurs réseaux virtuels à l'intérieur d'une même entreprise afin de gérer séparément la téléphonie, la télésurveillance, les vidéoconférences dans l'entreprise, etc.
- Le partage de mêmes réseaux virtuels par des opérateurs différents afin de réduire les coûts. Quand un de ces derniers veut augmenter sa capacité, il demande à l'opérateur d'infrastructure d'augmenter ses ressources.

Une autre utilisation de la virtualisation qui ne cesse de croître concerne les applications de type Cloud. En termes simples, le principe du Cloud consiste à placer les ressources d'une entreprise quelque part dans le réseau afin de les partager avec d'autres utilisateurs. Le Cloud propose des ressources de types serveur, calcul, stockage, logiciel, etc. L'utilisateur peut partager ces ressources avec d'autres utilisateurs, tout en prenant en compte la sécurité des informations.

Les ressources virtuelles peuvent migrer pour optimiser des ressources physiques. De même, le client peut se déplacer sur Internet et avoir accès à ses ressources de n'importe où. Pour relier les ressources à l'utilisateur, il faut créer des réseaux. Et ceux-ci ne peuvent être que virtuels puisqu'il serait impossible de créer un nouveau réseau physique à chaque déplacement ou demande de ressources supplémentaires d'un utilisateur.

La virtualisation est enfin une technologie idéale pour tester de nouveaux protocoles et de nouvelles architectures sans arrêter le réseau opérationnel puisqu'il suffit de construire un nouveau réseau virtuel avec les nouvelles générations de protocoles ou d'architectures. L'isolation est dans ce cas une propriété essentielle pour que les tests ne viennent pas gêner les réseaux opérationnels.

On peut en conclure que la virtualisation présente de nombreux avantages. Elle est aujourd'hui considérée comme une opportunité pour apporter de la souplesse aux réseaux. De plus, elle permet de passer d'une technologie à une autre sans trop de complications.

Les désavantages de la virtualisation sont liés à la surcharge apportée par l'hyperviseur et aux besoins de mémoire et de puissance de calcul, surtout si l'on veut séparer totalement les différents domaines.

Virtualisation d'équipements de réseau

Il est possible de virtualiser de nombreux équipements de réseau. La virtualisation d'un contrôleur Wi-Fi, par exemple, permet de gérer des points d'accès associés à chaque contrôleur virtuel. Les points d'accès associés peuvent avoir leur propre pile protocolaire.

On peut aussi virtualiser des pare-feu. À l'accès dans l'entreprise, les flots sont renvoyés vers le pare-feu virtuel général, qui, à son tour, peut renvoyer le flot vers un pare-feu spécifique, toujours virtuel. Les pare-feu peuvent ainsi bénéficier de toute la puissance nécessaire pour réaliser les inspections permettant de détecter des attaques.

Les points d'accès eux-mêmes peuvent être virtualisés. Il suffit pour cela d'introduire dans le boîtier un hyperviseur soutenant plusieurs systèmes d'exploitation. Chaque point d'accès virtuel possède ainsi ses propres logiciels de gestion et de contrôle et est indépendant des autres points d'accès : il peut donc représenter un opérateur particulier. De même, il est possible de virtualiser les antennes 2G, 3G et 4G (BTS, NodeB et E-NodeB) et de partager ces antennes virtuelles entre différents opérateurs.

Globalement, toute ressource peut être virtualisée, sauf les capteurs, qui ont besoin d'un élément matériel pour mesurer une valeur. Un capteur virtuel est donc un logiciel associé à un capteur physique pour effectuer des calculs à partir de la valeur mesurée. Bien évidemment, ce logiciel peut être modifié, d'où son nom de capteur virtuel. L'avenir est ainsi clairement à la virtualisation de l'ensemble des matériels.

NFV (Network Functions Virtualization) et normalisation de la virtualisation

La normalisation des machines virtuelles s'effectue à l'ETSI (European Telecommunications Standards Institute). On pourrait penser qu'elle ne concerne que les Européens, mais pas du tout : l'ETSI s'est ouvert au niveau mondial, et tous les opérateurs et équipementiers participent à cette standardisation.

Le terme utilisé, NFV (Network Functions Virtualization), indique la volonté de définir une fois pour toutes les différentes fonctions utilisées dans le domaine des réseaux. Cependant, normaliser des fonctions n'était pas suffisant. L'ETSI est allé plus loin en proposant

de développer en open source les différentes fonctions réseau, comme le routage d'un routeur, la commutation d'un commutateur, la protection d'un pare-feu, etc. À partir de ces machines virtuelles, on peut construire un réseau complet en open source avec plusieurs réseaux virtuels simultanés.

L'architecture standard des années 2020 en cours de développement a pris le nom d'OPNFV (Open Platform for NFV). Elle est décrite en détail au chapitre 14.

Le plus important de cette normalisation est cependant ailleurs : il s'agit de permettre le découplage de la fonction réseau et de l'équipement physique, une nouveauté radicale. Dans un routeur de l'ancienne génération, la fonction de routage et le transfert des paquets s'effectuent dans le même équipement physique. Dans la nouvelle génération, la fonction de routage peut être effectuée dans un serveur éloigné de la machine physique qui réalise le transfert du paquet. Cette dissociation permet de regrouper les fonctions de routage dans des serveurs de datacenters en optimisant globalement le fonctionnement. Les ressources attribuées aux machines virtuelles qui exécutent ces fonctions sont parfaitement ajustées. De plus, ces ressources peuvent varier entre les heures de pointe et la nuit, où celles affectées à l'équipement virtuel diminuent fortement.

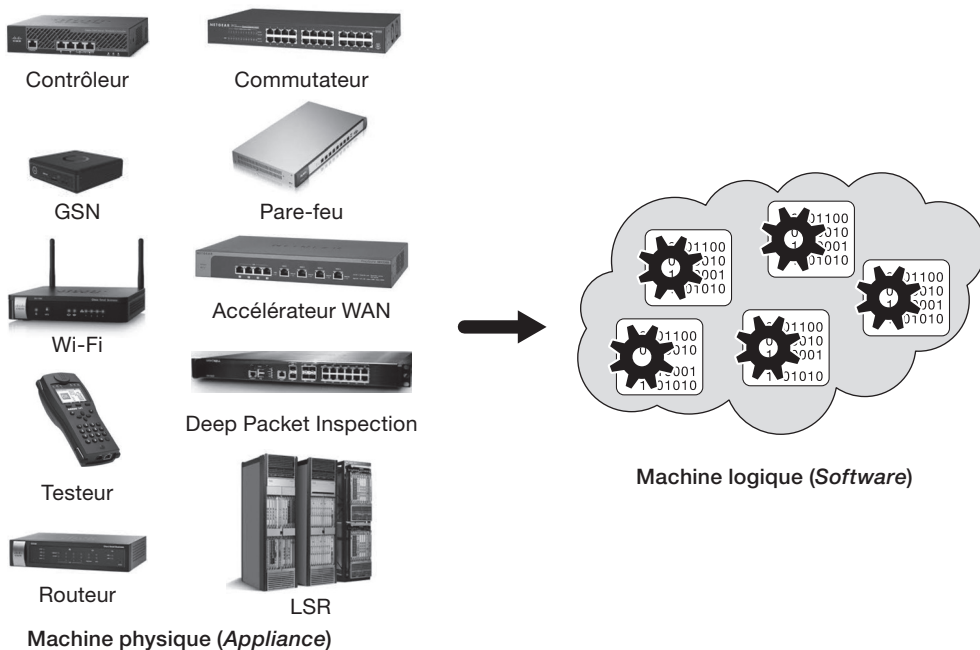


Figure 3.8

Passage de machines physiques à des machines logiques grâce à la virtualisation

La figure 3.8 illustre ce passage des machines physiques vers des machines virtuelles correspondant à des fonctions réseau. D'autres fonctions non-réseau, comme le stockage, le calcul, la sécurité, etc., peuvent être ajoutées simplement.

Les réseaux virtualisés

Les caractéristiques des réseaux détaillées aux sections précédentes sont mises à contribution dans la présente section pour introduire les principes de la virtualisation.

Un réseau de nouvelle génération est décrit à la figure 3.9.

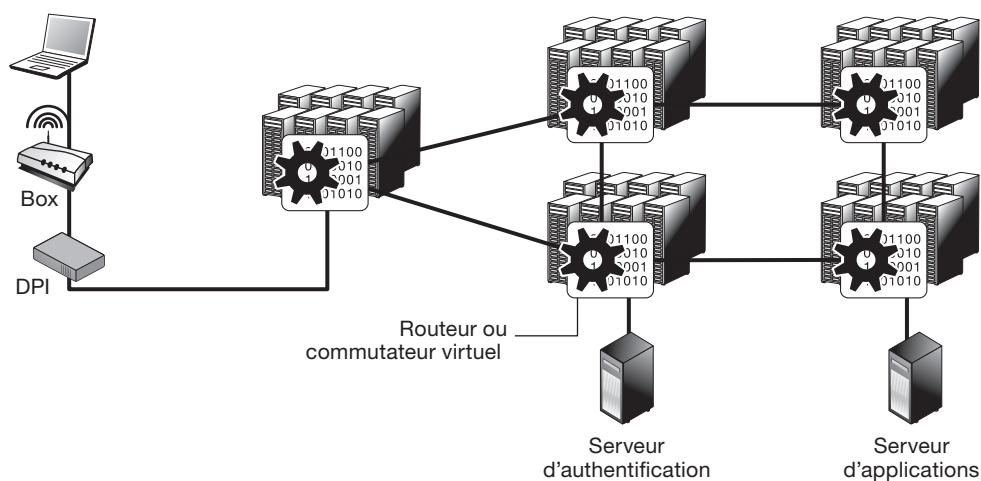
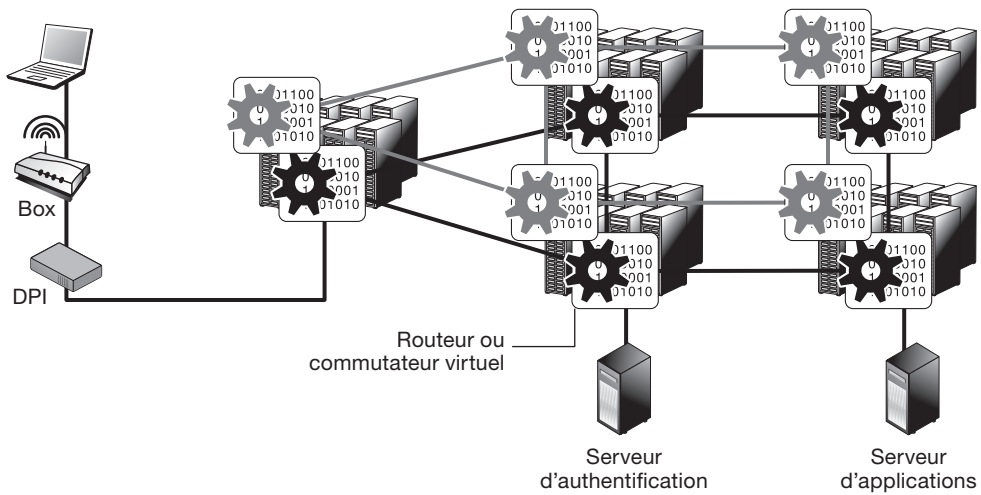


Figure 3.9

Un réseau de nouvelle génération

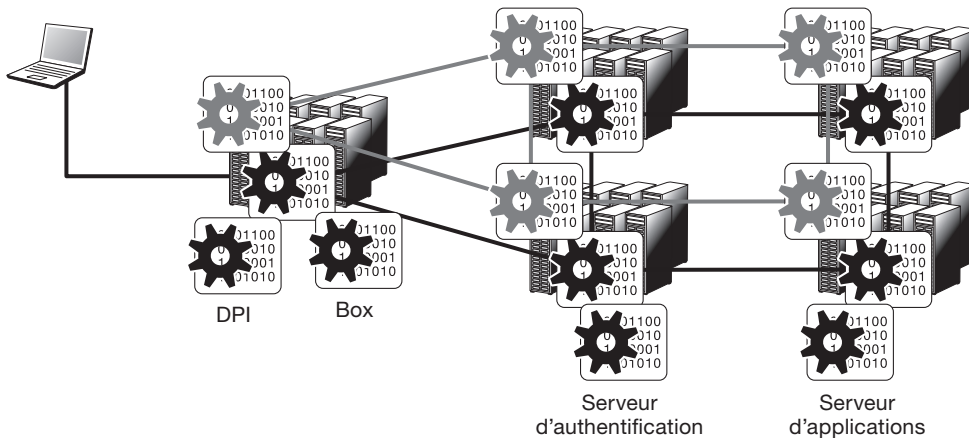
L'infrastructure est réalisée à partir de datacenters, dans lesquels sont positionnées des machines virtuelles, ici des routeurs ou des commutateurs, et des boîtiers divers, tels que box, serveurs d'authentification et d'applications, pare-feu et DPI (Deep Packet Inspection), ce dernier inspectant les flots qui transitent dans le réseau. Ces boîtiers sont également virtualisés (*voir plus loin*).

Comme l'illustre la figure 3.10, il est possible d'ajouter un deuxième réseau virtuel, qui utilise par exemple des protocoles complètement différents du premier.

**Figure 3.10**

Un réseau de nouvelle génération supportant deux réseaux virtuels

En allant toujours un peu plus loin dans le processus, on peut virtualiser les différents boîtiers dans les datacenters, comme l'illustre la figure 3.11, où les boîtiers physiques sont devenus des machines virtuelles intégrées aux datacenters. Il faut évidemment garder sous forme physique les éléments qui ne peuvent être virtualisés, comme les antennes ou les capteurs.

**Figure 3.11**

Environnement réseau totalement virtualisé

L'optimisation de l'emplacement des VM n'est pas simple. On appelle ce processus l'urbanisation des machines virtuelles. Il faut noter que l'urbanisation peut changer du tout au tout en fonction de l'objectif poursuivi. Par exemple, l'urbanisation pour optimiser les performances est totalement différente de l'urbanisation pour optimiser la consommation énergétique. Dans le premier cas, il faut distribuer les VM un peu partout dans le réseau afin qu'elles disposent chacune du plus de ressources physiques possibles. Dans le deuxième cas, il faut regrouper par migration toutes les machines virtuelles sur des serveurs physiques communs, de sorte à pouvoir mettre en veille de très nombreux serveurs physiques, la consommation électrique étant fortement proportionnelle à la vitesse du processeur. L'urbanisation est encore tout à fait différente si l'on essaie d'optimiser la sécurité ou la disponibilité du réseau ou encore sa fiabilité.

Grâce au NFV, on peut rassembler toutes les fonctions dans un même datacenter, comme l'illustre la figure 3.12. On peut parler dans ce cas précis de NFVaaS, c'est-à-dire que l'on a les fonctions réseau disponibles dans un Cloud représenté ici par un datacenter unique. On voit que les fonctions réseau ont migré des datacenters qui formaient l'infrastructure physique du réseau vers un datacenter qui peut se trouver très loin des nœuds de ce même réseau.

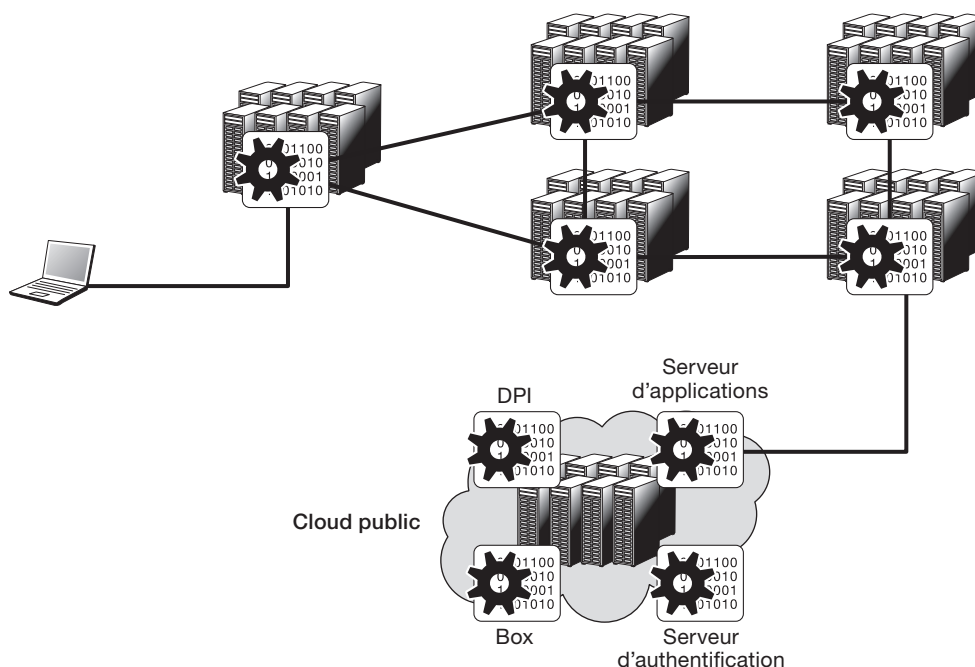


Figure 3.12

Un réseau géré en NFVaaS (NFV as a Service)

L'architecture des réseaux NFV peut se résumer comme illustré à la figure 3.13. Les machines virtuelles portant les fonctions de réseau s'appellent des VNF (Virtual Network

Functions). Ces fonctions s'installent sur une infrastructure appelée NFVI (NFV Infrastructure). Elles sont portées par des machines physiques avec hyperviseur ou conteneur permettant la virtualisation. Pour qu'elles puissent fonctionner sans problème, elles doivent être orchestrées et gérées par un environnement appelé MANO (Management And Network Orchestration). Ces orchestrateurs, examinés en détail au chapitre 4, sont des organes permettant de créer les machines virtuelles, puis de les chaîner, c'est-à-dire de déterminer l'ordre dans lequel il faut les traverser, et enfin de les «urbaniser», soit les placer sur des machines physiques afin que l'ensemble fonctionne du mieux possible.

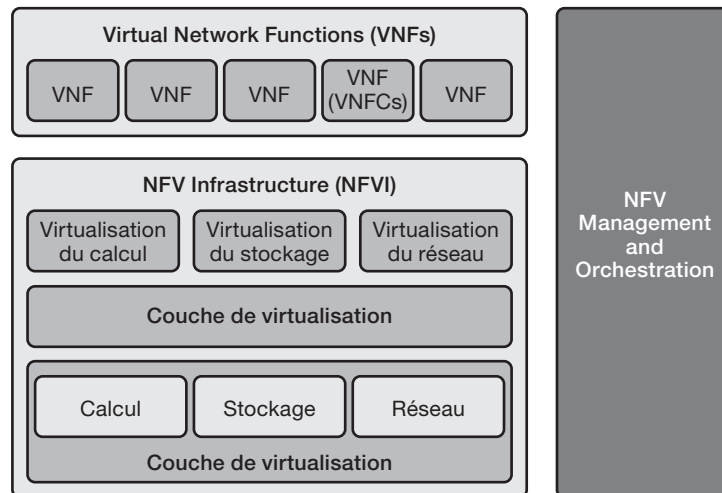


Figure 3.13

Ensemble des éléments entrant en jeu dans la virtualisation de réseau

Conclusion

La virtualisation est une technique importante, qui permet d'introduire de nouvelles technologies sous forme de réseaux virtuels particuliers. Il est ainsi possible, sans risque, de tester sur un réseau opérationnel de nouvelles architectures. Cette solution offre également aux réseaux l'opportunité d'une pensée à long terme, car lorsque l'architecture du futur sera trouvée, elle pourra s'introduire petit à petit dans le monde des réseaux grâce à la virtualisation.

La virtualisation des réseaux et, plus largement, celle des ressources constituent un tournant dans l'architecture des réseaux. Dans les années 2020, tous les équipements réseau seront virtualisés, et les équipements virtuels pourront se déplacer en fonction du contexte afin d'optimiser les performances globales suivant des critères qui restent à définir. La complexité de ces nouveaux environnements est optimisée par des processus de plus en plus intelligents, faisant souvent appel à de l'intelligence artificielle, comme le détaille le chapitre 4.

L'intelligence dans les réseaux

L'intelligence est un terme classique en informatique qui désigne simplement la capacité de communiquer, de raisonner et de décider. Jusqu'au début des années 2000, l'intelligence dans les réseaux était très faible. Les concepts de réseaux intelligents, qui datent du début des années 1990, introduisent une intelligence primaire, dont le rôle est d'adapter automatiquement des composants du réseau aux demandes des utilisateurs, mais sans raisonnement et uniquement en suivant des règles définies à l'avance.

L'intelligence n'a cessé d'augmenter depuis 2000 et continuera de le faire dans le futur, au point que l'on parle dès à présent de « smart networking » en introduisant dans la gestion et le contrôle des réseaux des agents intelligents, détaillés un peu plus loin dans ce chapitre, capables d'apporter, par exemple, des diagnostics. On voit aussi apparaître les réseaux autonomes, qui ont tendance à remplacer les réseaux programmables ou les réseaux actifs. Un réseau autonome est un réseau qui est capable de s'autoconfigurer et dont les nœuds peuvent devenir autonomes en cas de panne ou de coupure des communications.

Depuis le début des années 2000, l'intelligence réelle, c'est-à-dire à base de raisonnement, apparaît dans certains composants du réseau pour prendre des décisions de contrôle ou de gestion. Les organes qui prennent les décisions proviennent du domaine de l'intelligence artificielle et des objets intelligents. En particulier, les systèmes multi-agents se proposent de gérer la sécurité ou les pannes.

Les réseaux d'aujourd'hui et de demain vont faire appel à une intelligence beaucoup plus importante pour véritablement piloter le réseau par des équipements appelés orchestrateurs et contrôleurs. L'objectif est de réaliser des pilotages automatiques de réseau, à la manière de ce qui se fait dans les avions. Cependant, la difficulté est bien plus grande, car le système est fortement distribué. Comme expliqué au chapitre 12, consacré au SDN, la solution retenue dans un premier temps consiste à centraliser la commande.

Le présent chapitre introduit dans un premier temps ces orchestrateurs et contrôleurs permettant de réaliser des pilotages automatiques puis examine les outils transitoires qui rendent possibles ces processus complexes de pilotage.

Orchestrateurs et contrôleurs

Avant d'aborder les outils provenant de l'intelligence artificielle, cette section examine les moyens de développer des automatismes beaucoup plus poussés que ceux des produits commercialisés depuis quelques années.

Les contrôleurs sont des organes capables de commander les équipements réseau, et plus précisément de les configurer afin qu'ils puissent transférer les paquets de l'entrée d'un nœud vers la bonne file de sortie. Les contrôleurs s'occupent également des autres éléments réseau, comme les pare-feu ou les DPI (Deep Packet Inspection). Ils doivent posséder tous les algorithmes nécessaires pour configurer ces éléments de réseau, comme des équilibresurs de charges (*load balancers*), des gestionnaires de VLAN (Virtual Local Area Network), mais aussi des pare-feu, etc.

Comme leur nom l'indique, les orchestrateurs jouent le rôle de chefs d'orchestre pour l'environnement réseau. Leur première fonction est de créer les machines virtuelles, ou VM, qui seront nécessaires pour réaliser le réseau destiné à prendre en charge le flot de paquets provenant de l'application qui demande l'ouverture d'une communication.

Après avoir choisi les VM nécessaires, il faut les chaîner (*chaining*), c'est-à-dire décrire le parcours des paquets au travers des différentes VM. Un exemple de chaînage est décrit à la figure 4.1. Entre les points d'entrée et de sortie du réseau, les paquets doivent traverser des VM qui réalisent des fonctions de réseau, ou VNF (Virtual Network Functions), par exemple un routeur suivi d'un pare-feu, suivi d'un autre routeur, puis d'un boîtier donnant des fonctions particulières, puis... Il peut aussi y avoir des aiguillages, avec des fonctions en parallèle.

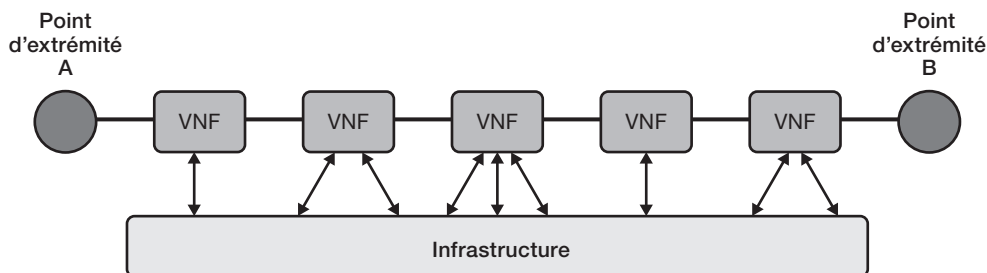


Figure 4.1

Le chaînage de machines virtuelles

Après le chaînage, l'orchestrateur doit réaliser la fonction d'urbanisation, c'est-à-dire placer les VM sur des machines physiques. Comme illustré à la figure 4.1, une VM peut avoir

plusieurs instances physiques de la fonction virtuelle se situant dans différents serveurs d'infrastructure, certains pouvant se situer assez loin de la machine réalisant le travail. Des duplications et triplifications sont également possibles.

La suite de cette section donne quelques exemples de contrôleurs, avant de se pencher sur les orchestrateurs que l'on peut acquérir aujourd'hui.

Il existe deux grandes catégories de contrôleurs : ceux provenant du monde open source et ceux, fermés, provenant de certains équipementiers. Beaucoup d'équipementiers ont choisi de partir d'une souche open source et de la compléter par des modules spécifiques. Le contrôleur le plus utilisé, et de loin, est ODL (OpenDaylight).

Parmi les autres contrôleurs open source, citons notamment les suivants :

- NOX, le premier contrôleur compatible avec le protocole de signalisation OpenFlow, examiné en détail au chapitre 12.
- FlowVisor, réalisé en Java, qui utilise également la signalisation OpenFlow et se comporte comme un proxy transparent entre un commutateur et de multiples contrôleurs, tous OpenFlow.
- POX, écrit en Python et toujours orienté OpenFlow, avec une interface de haut niveau pour le SDN (Software-Defined Networking).
- Floodlight, écrit en Java et orienté OpenFlow.
- ONOS (Open Network Operating System), un système d'exploitation réseau distribué en open source, équivalent d'un contrôleur distribué.
- OpenContrail, un contrôleur open source repris par Juniper.

De nombreux autres contrôleurs sont également disponibles, tels LOOM, Ryu ou Trema.

Regardons de façon plus précise les trois contrôleurs open source les plus utilisés aujourd'hui, qui sont ODL, OpenContrail et ONOS.

L'architecture de la dernière version du contrôleur ODL, appelée Oxygen, est décrite à la figure 4.2.

Le contrôleur contient trois parties. La partie haute, qui correspond à l'interface nord (Northbound Interface), contient les interfaces avec les applications qui demandent une communication vers un destinataire. Au travers de cette interface, le contrôleur récupère toutes les informations nécessaires pour permettre l'ouverture d'un chemin ou d'une route dans le réseau en garantissant la qualité de service et, plus généralement, l'agrément qui a été conclu entre l'utilisateur et le gestionnaire du réseau, ou SLA (Service Level Agreement).

La seconde partie correspond à la partie basse de la figure 4.2 : l'interface sud (Southbound Interface), située entre le contrôleur et les équipements réseau, qui peuvent être virtuels ou non. Cette interface transporte dans un sens les configurations à appliquer dans les nœuds du réseau et dans l'autre toutes les informations provenant des mesures effectuées sur le réseau, qui vont permettre au contrôleur de prendre les bonnes décisions.

La troisième partie, au centre du contrôleur, correspond à toutes les fonctions qui peuvent être exercées pour prendre des décisions, sécuriser le réseau et, plus globalement, contrôler les fonctions dispersées dans le réseau.

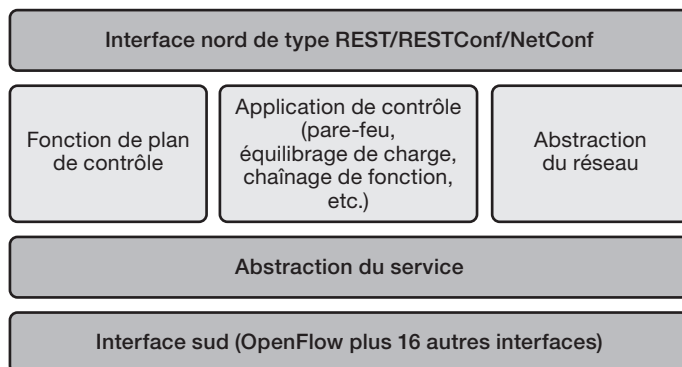


Figure 4.2

Architecture d'Oxygen, la dernière release du contrôleur ODL

La figure 4.3 illustre le contrôleur OpenContrail qui provient d'un projet open source repris en main par Juniper. Les composants interface nord et sud plus les fonctions de contrôle se retrouvent dans ce contrôleur. La figure indique les éléments provenant de l'intelligence intégrée dans le boîtier virtuel. Il s'agit de la transformation des données qui proviennent de l'interface nord, pour les informations applicatives, et de l'interface sud, pour la remontée des informations de mesure à partir des équipements réseau, qu'ils soient virtuels ou non. Cet ensemble de données est rassemblé dans un Big Data, dont les outils dits *analytics* sont utilisés pour prendre les décisions d'ouverture de chemin ou de route dans le réseau.

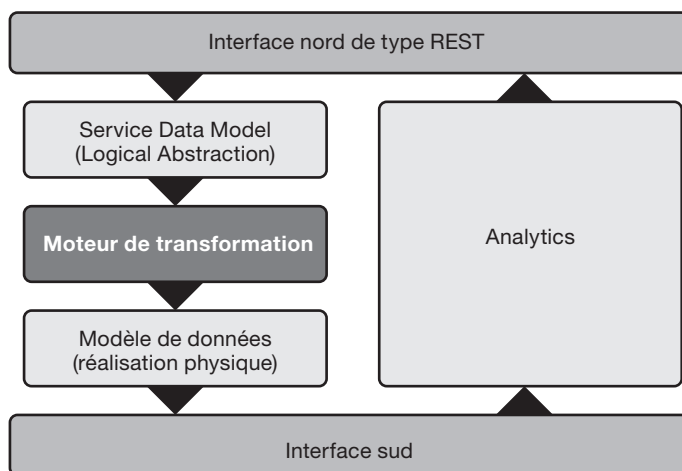


Figure 4.3

Architecture du contrôleur OpenContrail

Le contrôleur ONOS (Open Network Operating System) utilise les mêmes concepts que les deux précédents, mais en introduisant, nouveauté importante, un système distribué, qui permet de faire fonctionner le système en utilisant plusieurs contrôleurs simultanément. Les contrôleurs sont interconnectés par des interfaces est et ouest qui permettent d'agrandir le réseau en enlevant la limitation introduite par un seul contrôleur.

La figure 4.4 décrit ce contrôleur en tout point conforme aux caractéristiques introduites précédemment, la seule différence provenant du système central distribué, qui permet d'affecter les machines virtuelles à différents contrôleurs, entraînant de la sorte des connexions primaires et secondaires en secours.

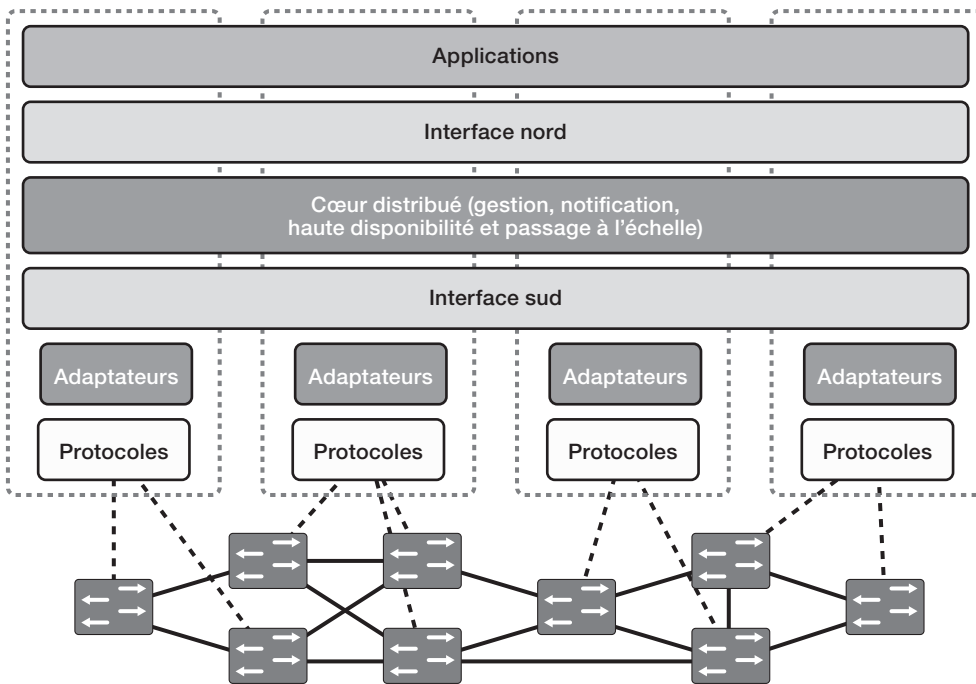


Figure 4.4

Architecture du contrôleur ONOS

La figure 4.5 va encore un peu plus loin dans la description des fonctions qui apportent l'intelligence à ce contrôleur. Les fonctions internes incluent la gestion du réseau à l'aide d'un graphe provenant d'une base de données de connaissances, c'est-à-dire d'informations contextuelles.

Cassandra, une base de données distribuée open source, est un système de gestion conçu pour traiter de très grandes bases de données et, dans le cas présent, *in-memory*, c'est-à-dire que les données se trouvent dans la mémoire RAM pour réaliser des fonctions temps réel. Ces données peuvent être d'une taille immense et réparties sur de nombreux serveurs.

Cassandra fournit un service hautement disponible. L'intelligence est apportée par cette base de connaissances sur laquelle de nombreux traitements de type Big Data analytics peuvent être exercés. C'est la base distribuée des registres qui confère la forte consistance du système global

Zookeeper est un projet open source permettant de développer et maintenir un serveur offrant une coordination distribuée hautement fiable.

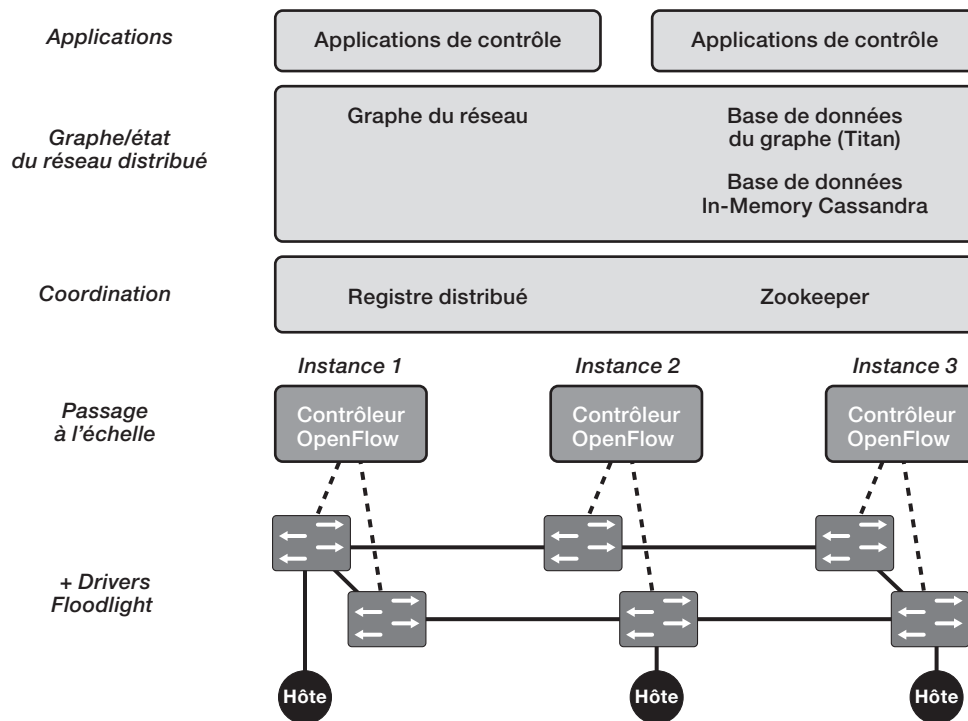


Figure 4.5

Modules apportant l'intelligence d'ONOS

Les orchestrateurs apportent l'intelligence nécessaire aux tâches de mise en place d'un réseau et d'allocation des ressources aux VM afin de réaliser une communication avec la qualité de service voulue. Plusieurs solutions open source offrent des fonctionnalités plus ou moins importantes. La suite de cette section décrit brièvement deux projets, Open-O (Open-Orchestration) et ONAP (Open Network Automation Protocol).

Open-O est un projet collaboratif de la fondation Linux axé sur la création d'une plateforme open source réalisant une orchestration de réseau d'opérateur. L'objectif principal est d'établir un cadre ouvert pour organiser des services composites de bout en bout dans les réseaux utilisant les infrastructures émergentes de type SDN et NFV.

Open-O possède une architecture conforme à MANO (Management And Network Orchestration) et adopte les langages de modélisation de services standards tels que Yang ou Tosca afin d'assurer cohérence et flexibilité. Open-O comporte trois fonctions d'orchestration principales : GS-O (Global Services Orchestrator), SDN-O (SDN Orchestrator) et NFV-O (Network Functions Virtualization Orchestrator). L'orchestrateur fournit des micro-services liés aux différents modules décrits à la figure 4.6.

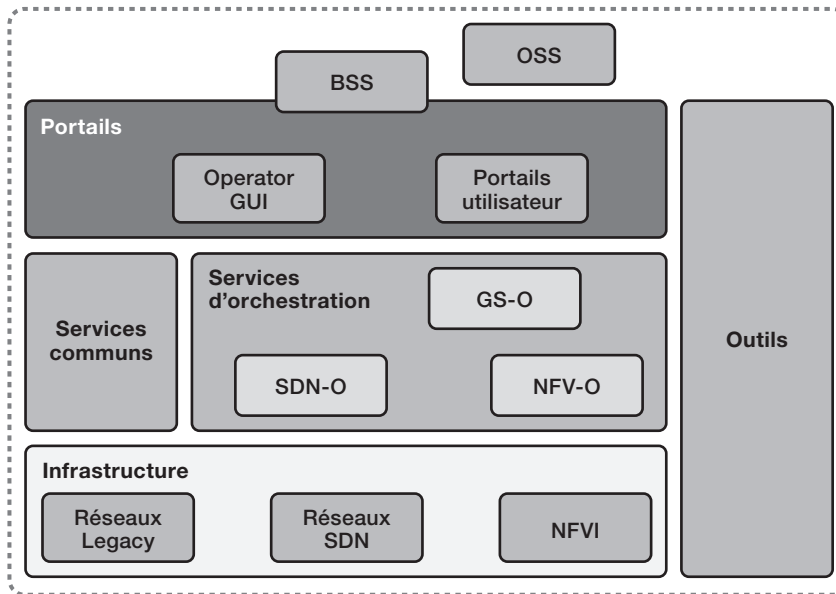


Figure 4.6

Architecture d'Open-O

ONAP est une extension d'Open-O ou, plus exactement, l'adjonction d'Open-O à un autre projet collaboratif consacré plus spécialement à l'automatisation des processus de commandes de réseau. Ce second projet est dit ECOMP (Enhanced Control, Orchestration, Management & Policy), une plate-forme développée par AT&T.

ECOMP permet de mettre en place des services automatiquement, avec leur cycle de vie et leur gestion. Cette plate-forme se compose de huit logiciels couvrant les grandes architectures, un environnement de conception, une plate-forme de définition et une d'exécution et enfin un environnement pour exécuter la logique programmée. La phase de conception utilise une approche en boucle fermée fondée sur les politiques, ce qui permet d'automatiser le processus de mise en place des services et de les gérer par la suite.

L'architecture de la plate-forme ONAP est illustrée à la figure 4.7. Elle comporte un portail permettant de gérer l'interface avec la plate-forme qui comporte trois grands modules. Le premier, provenant d'ECOMP, réalise la conception du service demandé grâce à un

ensemble de politiques. Le deuxième module, provenant d'Open-O, s'occupe de l'orchestration de la mise en place des éléments pour réaliser la communication et la contrôler. Le dernier module s'occupe du cycle de vie de l'environnement mis en place. Il contient des modules d'intelligence à partir des données provenant aussi bien des clients que du réseau.

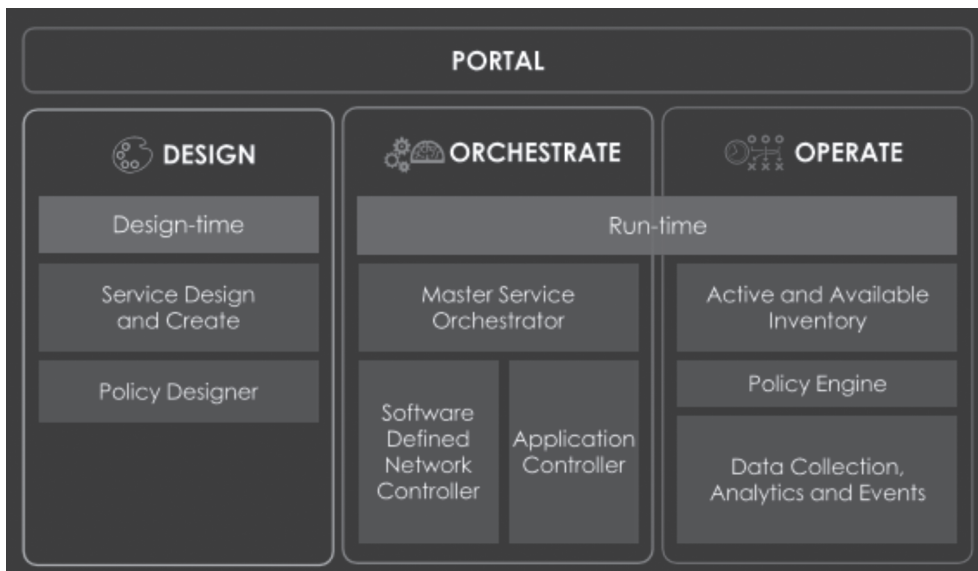


Figure 4.7

Architecture de la plate-forme ONAP (© Amdocs)

En conclusion de cette section, on voit arriver de nombreux logiciels open source dont le but est d'automatiser la vie des réseaux. Cette automatisation s'effectue essentiellement par des modules opérant des fonctions provenant de l'intelligence artificielle, que ce soit du Big Data, du machine learning, du deep learning ou d'autres solutions intégrées dans des agents intelligents. Les sections suivantes examinent plus en détail les outils mis en jeu pour arriver à cette automatisation.

Les agents intelligents

Les agents intelligents constituent une première catégorie d'outils dont l'introduction à grande échelle modifie les environnements de gestion, de contrôle et d'orchestration en les rendant plus autonomes et plus réactifs.

La section suivante se penche sur les raisons de cette puissance puis sur la façon de construire des systèmes multi-agents.

Gestion d'un environnement complexe

Les réseaux étant de plus en plus complexes, la gestion et le contrôle de ces environnements sont devenus nécessaires pour de multiples raisons. De plus, les environnements réseau sont aujourd'hui dynamiques. Des applications nombreuses et variées se superposent et rendent le contrôle des ressources difficile. Le gain statistique, c'est-à-dire ce que l'on gagne en traitant les paquets de façon statistique dans les réseaux à transfert de paquets, est indéniable. Mais si les flux dépassent trop fortement les capacités du réseau, un effondrement des performances est inévitable.

Les environnements réseau sont par nature distribués, ce qui complique leur contrôle et leur gestion. Dans le cas de petits réseaux, de moins d'une cinquantaine de nœuds, le contrôle est centralisé afin d'accéder plus facilement à une intelligence grâce à l'ensemble des données récupérées côtés client et réseau et stockées dans le centre.

Le gigantisme impose un contrôle encore plus fin. Le dimensionnement est un problème complexe à appréhender, et l'on peut affirmer qu'il n'existe pas d'outil véritablement efficace dans ce domaine, dans la mesure où les paramètres à prendre en compte dans un environnement de réseau complexe sont difficiles à apprécier. On a le choix entre débit, temps de réponse, taux d'utilisation des coupleurs de ligne et des unités centrales, taux d'erreur bit, taux d'erreur paquet, taux de reprise et taux de panne. En outre, les valeurs de la moyenne, de la variance et parfois des moments d'ordre supérieur doivent être prises en considération pour avoir une idée réelle des performances.

L'ingénierie de la conception du réseau présente deux grands aspects, le qualitatif et le quantitatif. Le qualitatif correspond souvent à une sécurité de fonctionnement, dans le sens où il est possible de prouver que le système est stable ou qu'il n'existe pas d'état dans lequel le réseau se bloque. L'aspect quantitatif fait référence aux valeurs des paramètres indiqués au paragraphe précédent, le but d'une analyse quantitative étant de montrer que ces valeurs sont raisonnables pour un bon fonctionnement du réseau.

La sécurité est une fonction importante pour laquelle peut intervenir de l'intelligence. Aujourd'hui, une certaine normalisation permet de mieux cerner les problèmes, et quelques grandes classes de sécurité ont été définies, correspondant à des besoins bien exprimés par les utilisateurs. On peut facilement imaginer l'apport d'outils intelligents dans le monde de la sécurité pour reconnaître les anomalies, les analyser, donner un diagnostic, proposer une solution et résoudre le problème.

La gestion est également un domaine où les agents intelligents peuvent jouer un rôle moteur. Lorsqu'un réseau est en état de marche, il faut l'administrer, c'est-à-dire être en mesure de contrôler toutes les opérations qui s'y déroulent dans le réseau, depuis les pannes jusqu'à la comptabilité en passant par la sécurité, la gestion des performances et la gestion des noms des utilisateurs.

Plusieurs domaines d'administration spécifiques utilisent déjà des composants intelligents, notamment les suivants :

- configuration (Configuration Management) ;
- sécurité (Security Management) ;

- pannes (Fault Management);
- audit des performances (Performance Management);
- comptabilité (Accounting Management).

L'intelligence des agents peut provenir de différents horizons. Le schéma le plus classique émane de l'intelligence artificielle distribuée, ou IAD.

L'intelligence artificielle signifie que l'on met à la place d'un être humain un agent intelligent pour réaliser une tâche. L'IAD équivaut à une société d'agents autonomes travaillant en commun pour aboutir à un objectif global. Parmi les nombreuses raisons qui incitent à se diriger vers l'utilisation de l'IAD, citons notamment les suivantes :

- Prise en compte de points de vue différents. Lorsque les données deviennent de plus en plus précises, des incohérences peuvent survenir dans la base de règles. Les façons d'exprimer les connaissances sont différentes selon qu'on s'adresse à l'utilisateur, au développeur ou au technicien. De plus, deux experts possédant la même expertise n'arrivent pas toujours au même résultat. Les points de vue sont également souvent contradictoires : l'un veut privilégier les coûts, et donc un système moins cher, alors que l'autre choisit de développer la publicité, et donc un système plus cher. L'utilisation de l'IAD permet, par négociation, d'aboutir à un compromis entre différentes options.
- Adéquation au monde réel. D'une manière générale, c'est toujours un groupe d'experts, avec des qualifications et des spécialités différentes, qui parvient, par collaboration, à réaliser un objectif fixé. De plus, s'il semble aisé de comprendre, et donc de modéliser, le comportement des individus (l'ensemble de leurs échanges) grâce aux nombreuses études sociologiques disponibles, en revanche le fonctionnement du cerveau et le raisonnement sont moins connus.

Pour ces raisons, l'application de l'intelligence artificielle distribuée s'impose peu à peu dans le cadre de la maîtrise des réseaux.

Les systèmes multi-agents

Un agent est une entité autonome, capable de communiquer avec d'autres agents, ainsi que de percevoir et de représenter son environnement. L'ensemble de ces agents en interaction forme les systèmes multi-agents. On classe ces derniers selon de nombreux critères, tels que la taille des agents, leur nombre en interaction, les mécanismes et les types de communication, le comportement, l'organisation et le contrôle de chaque agent, la représentation de l'environnement, etc.

À partir de ces critères, on distingue deux grandes catégories de systèmes multi-agents :

- les systèmes d'agents cognitifs;
- les systèmes d'agents réactifs.

Les agents cognitifs ont une représentation explicite de l'environnement et des autres agents. Ils savent tenir compte de leur passé et fonctionnent selon un mode social d'organisation. Les systèmes de ce type ne possèdent qu'un petit nombre d'agents. Plusieurs niveaux de complexité peuvent être envisagés :