1. Les réseaux modernes

2024-2025
Ecole Supérieure Polytechnique (ESP) / Département Génie Informatique (DGI)
DIC3 TR (Télécommunications et Réseaux) & M2 SRT (Systèmes Réseaux et Télécommunications)
Cours : SDN et NFV
Enseignant : Dr Ousmane SADIO

Le secteur des IT a bénéficié d'innovations telles que la virtualisation des serveurs et du stockage. Les technologies IT continueront d'évoluer dans les années à venir.

Contrairement au secteur de l'IT, les réseaux ont connu une innovation limitée au cours des 20 dernières années. Cette stagnation a conduit à des réseaux trop complexes et rigides qui ne répondent plus aux besoins actuels des entreprises.

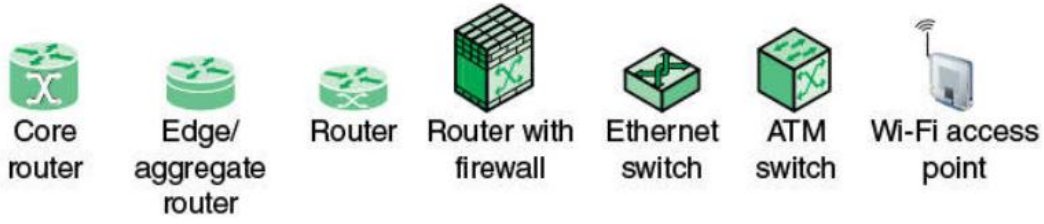
- Aujourd'hui, les exigences commerciales et techniques en matière de réseau incluent l'amélioration des performances et la réalisation d'une connectivité plus large.
- Les entreprises doivent respecter de plus en plus de règles de sécurité spécifiques à leur secteur d'activité et la demande de mobilité est de plus en plus forte.

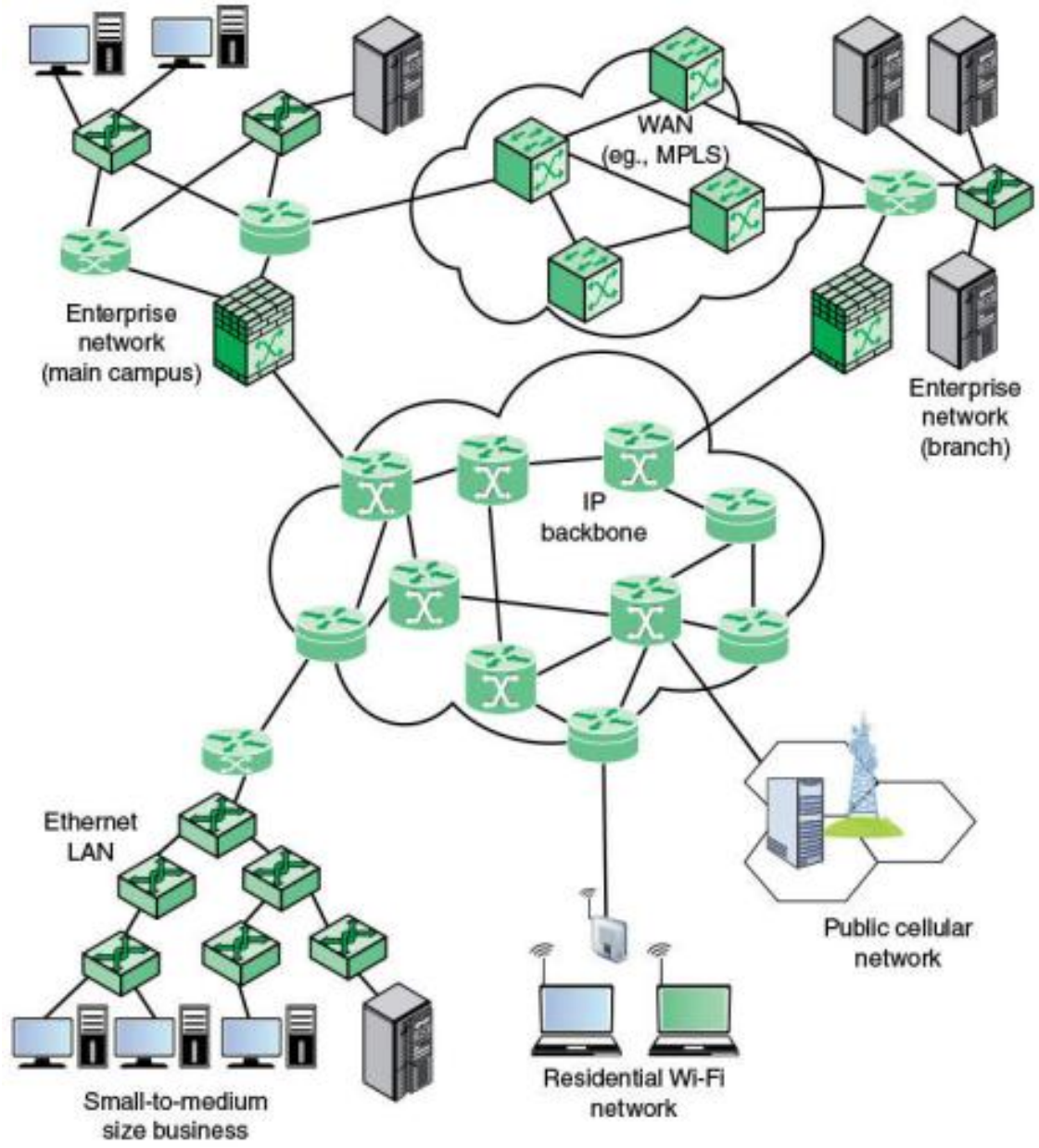
❑ Réseaux traditionnels

Ces réseaux présentent diverses architectures réseau et une terminologie qui leurs est spécifique.

- Architecture réseau globale

C'est une architecture qui peut représenter un réseau d'entreprise d'envergure nationale ou mondiale, ou une partie d'Internet avec certains de ses réseaux associés.



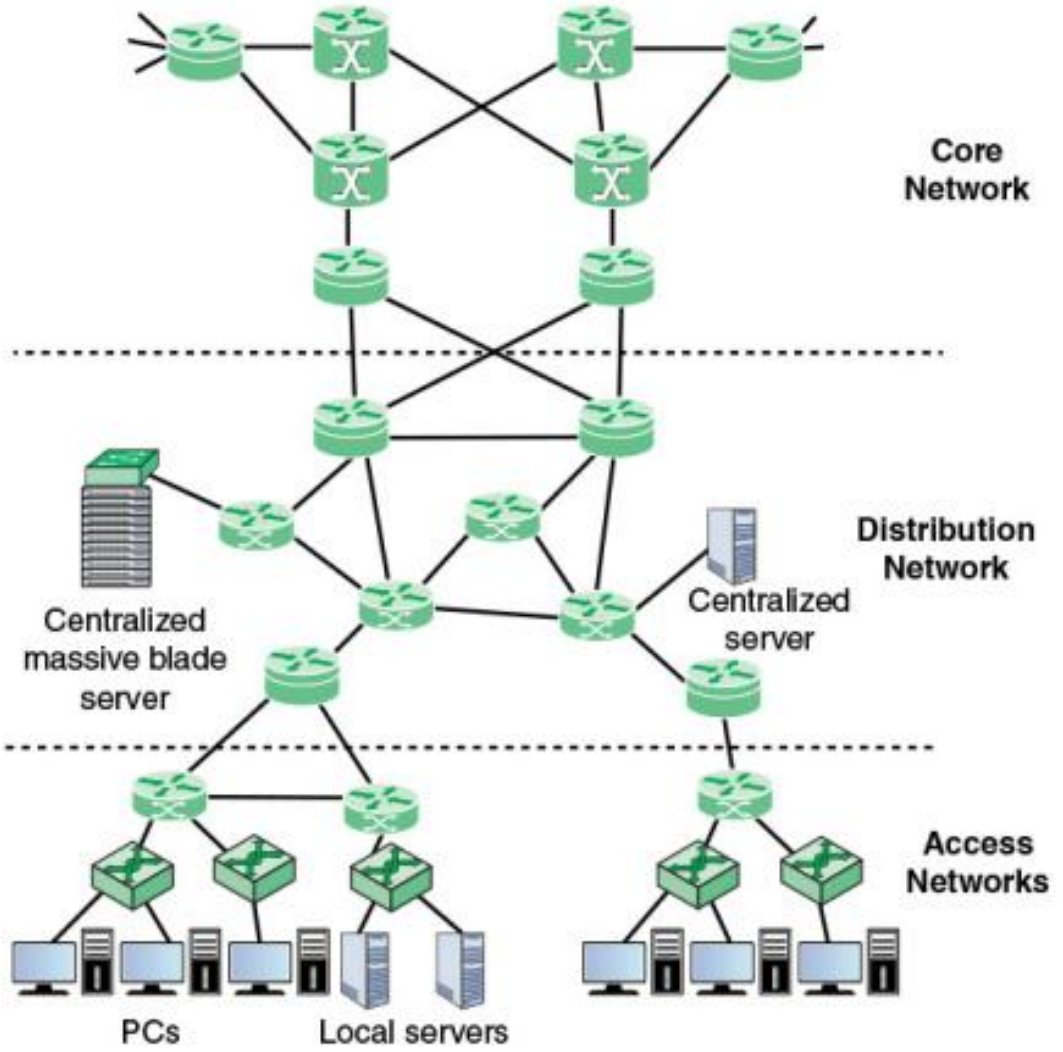


❑ Réseaux traditionnels

▪ Hiérarchie de réseau typique

Les entreprises conçoivent souvent leurs installations réseau selon une hiérarchie à trois niveaux : accès, distribution et cœur.

- Réseau d'accès : en général, est un réseau local (LAN) ou un réseau à l'échelle d'un campus.
- Réseau de distributions (agrégation): connecte les réseaux d'accès entre eux et avec le réseau cœur.
- Réseau cœur ou backbone : connecte les réseaux de distribution géographiquement dispersés ainsi que l'accès à d'autres réseaux qui ne font pas partie du réseau d'entreprise.

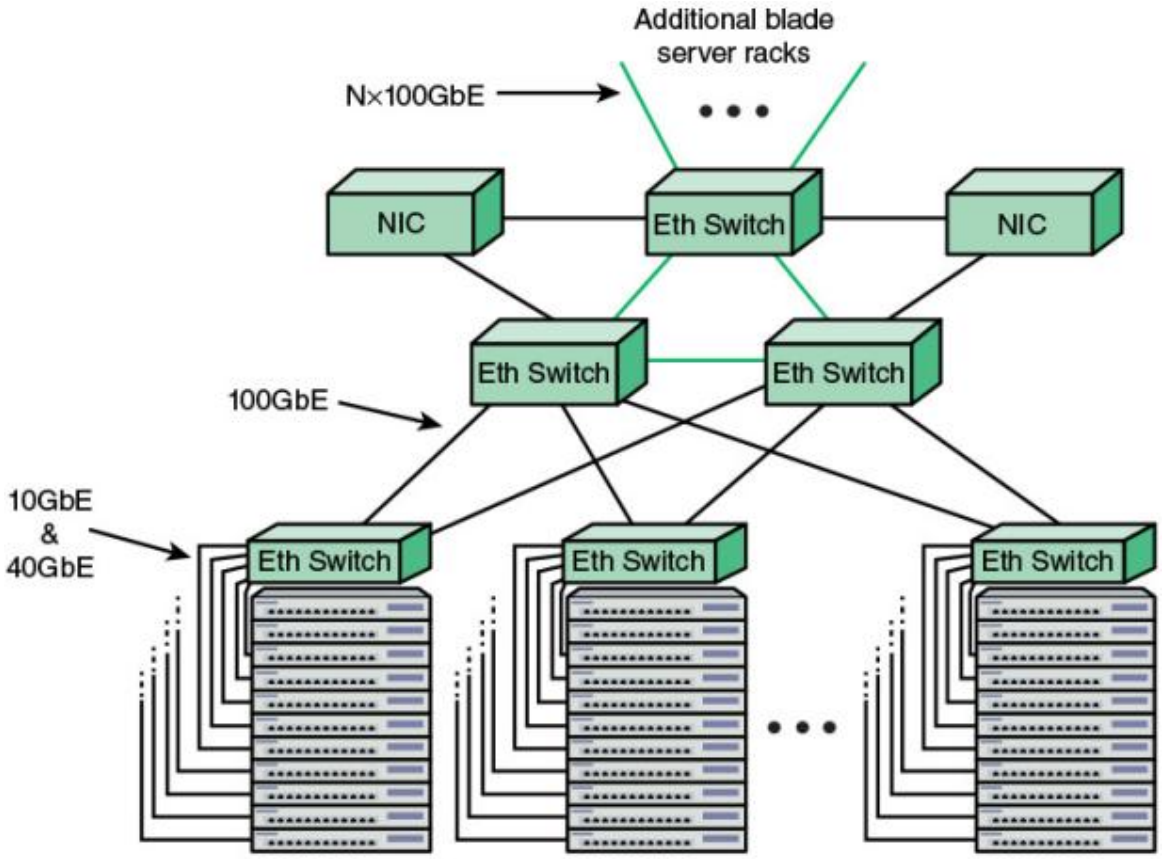


❑ Réseaux traditionnels

- Réseau de datacenter

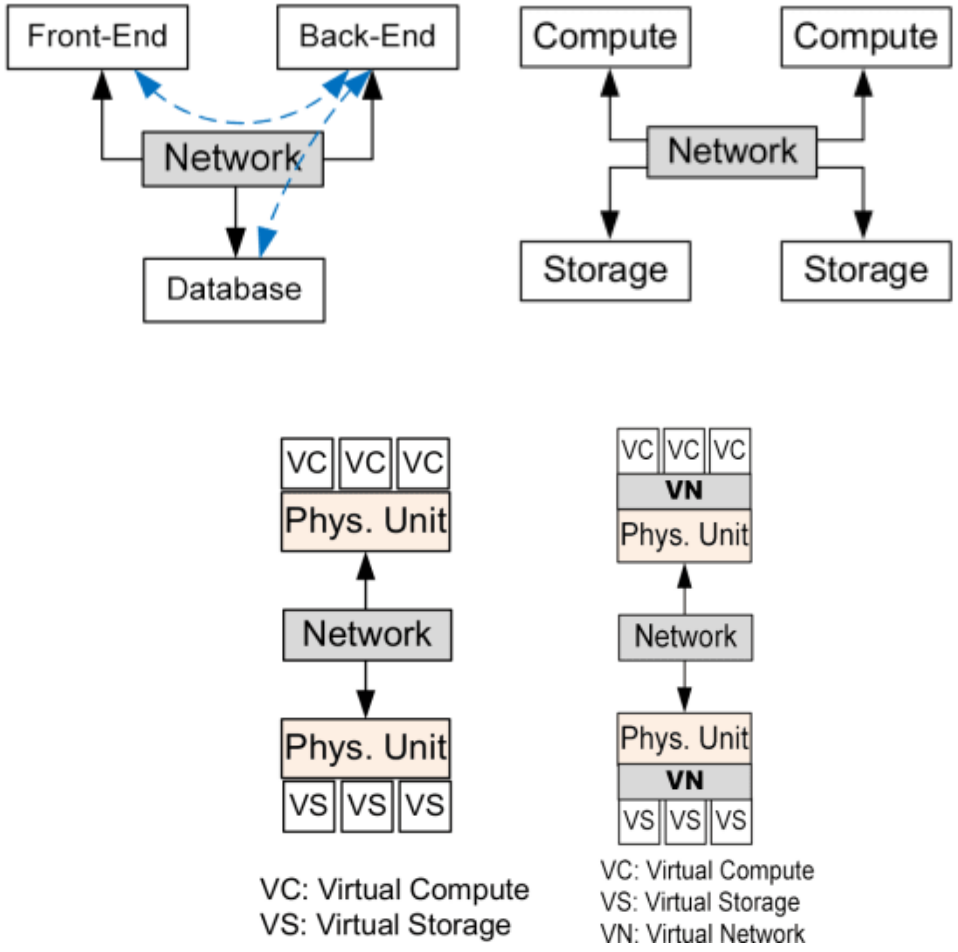
En général, un seul rack contient plusieurs serveurs et un ou deux commutateurs Ethernet 10Gbps pour interconnecter tous les serveurs et assurer la connectivité avec le reste de l'installation.

Les commutateurs sont souvent montés dans le rack et sont appelés commutateurs ToR (Top-of-Rack).



❑ Virtualisation de réseau : pourquoi ?

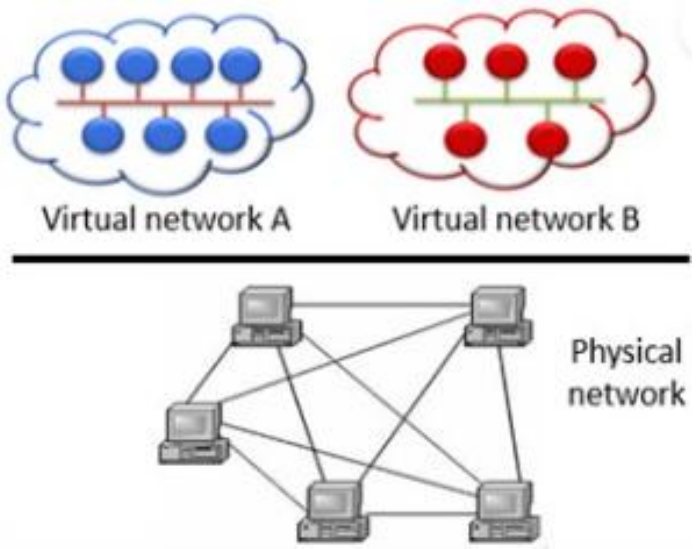
- Au début, les applications informatiques étaient monolithiques, et tout était construit dans un seul châssis. Puis les systèmes d'information ont commencé à adopter progressivement une architecture à 3 niveaux : Front End, Back End et BD.
- La tendance était alors de décomposer les serveurs d'applications en plusieurs composants indépendants:
- La virtualisation des serveurs physiques entre plusieurs unités logiques a augmenté les besoins en bande passante de chaque unité physique connectée au réseau.
- La dernière tendance consiste à virtualiser les fonctions du réseau et à désagréger les composants physiques qui le constituent.



❑ Virtualisation de réseau

Un réseau virtuel est un système qui émule un réseau physique en combinant les ressources matérielles et logicielles du réseau pour former une seule unité administrative.

Au moyen de la virtualisation du réseau, les machines virtuelles sont considérées comme s'exécutant sur différents réseaux virtuels sur le même réseau physique.



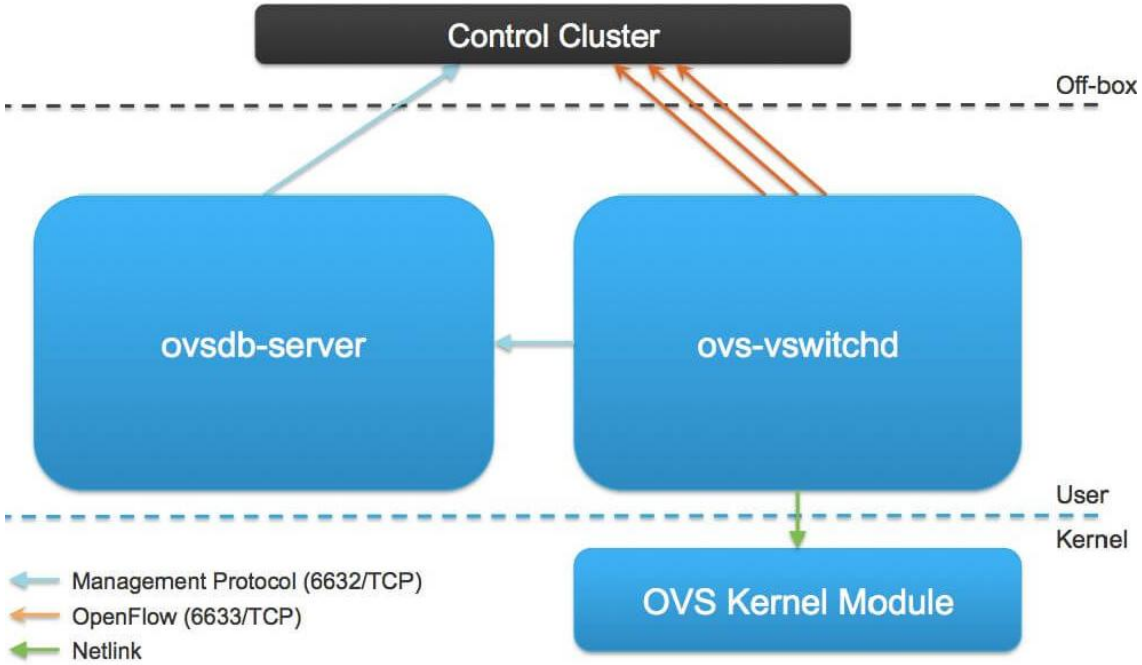
- Le trafic de plusieurs réseaux virtuels sont acheminés sur le même réseau physique : *les VM qui s'exécutent sur un même serveur physique utilisent une même carte réseau physique pour transmettre divers types de trafic.*
- Les réseaux virtuels sont indépendants les uns des autres.
- Le réseau virtuel est indépendant du matériel réseau de la couche inférieure et peut être configuré, modifié ou supprimé selon les exigences du service sans reconfiguration du matériel ou de la topologie de la couche inférieure.
- La virtualisation de réseau permet une configuration flexible du réseau virtuel. Cette virtualisation peut créer des services réseau L2 (commutation), L3 (routage) et L7 (pare-feu, équilibrage de charge) en très peu de temps.

❑ Virtualisation de réseau : OpenvSwitch

Openv Switch (OVS) est un commutateur virtuel multicouche qui offre un service pour contrôler les connexions réseau entre les VM fonctionnant dans des environnements multiserveurs hautement dynamiques tels que le Cloud. Openv Switch prend en charge plusieurs technologies de virtualisation Linux, telles que Xen et KVM.

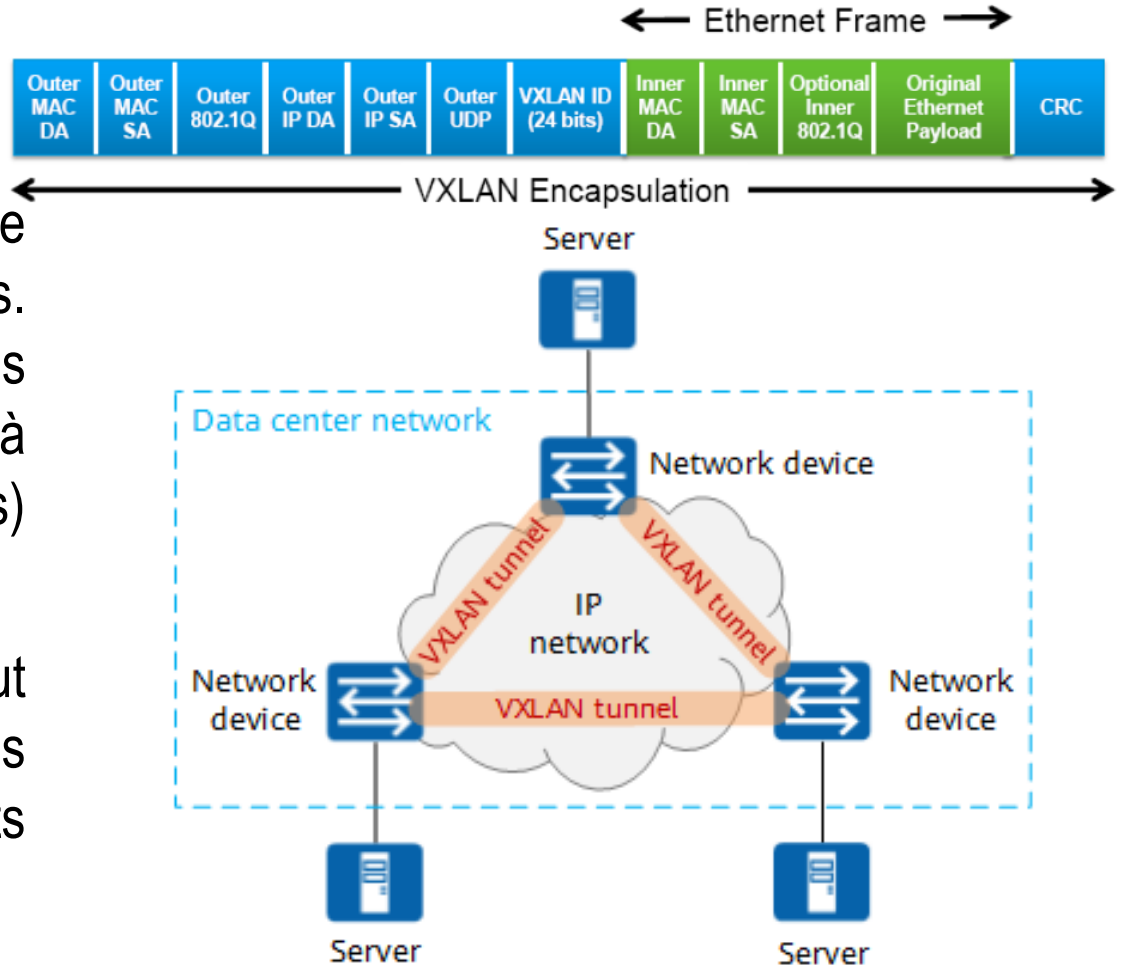
- ovs-vswitchd: démon qui permet de commuter effectivement les paquets vers les bons ports virtuels.
- openvswitch_mod: le module kernel permet de capturer le trafic provenant des interfaces réseau, et d'y réinjecter le trafic légitime.
- ovsdb-server: un serveur de base de données léger qu'ovs-vswitchd interroge pour obtenir sa configuration.

Open vSwitch supporte plusieurs fonctionnalité de commutateurs L2 et L3 : 802.1Q VLAN, filtrage de trafic, QoS, STP, tunnel GRE / VXLAN, agrégation de lien LACP, OpenFlow, OVSDB…



❑ VXLAN (Virtual eXtensible Local Area Network)

VXLAN est une technologie de virtualisation du réseau sur la couche 3 et constitue une extension du VLAN. VXLAN encapsule une trame Ethernet de couche 2 dans un paquet UDP et transmet le paquet sur un réseau de couche 3.



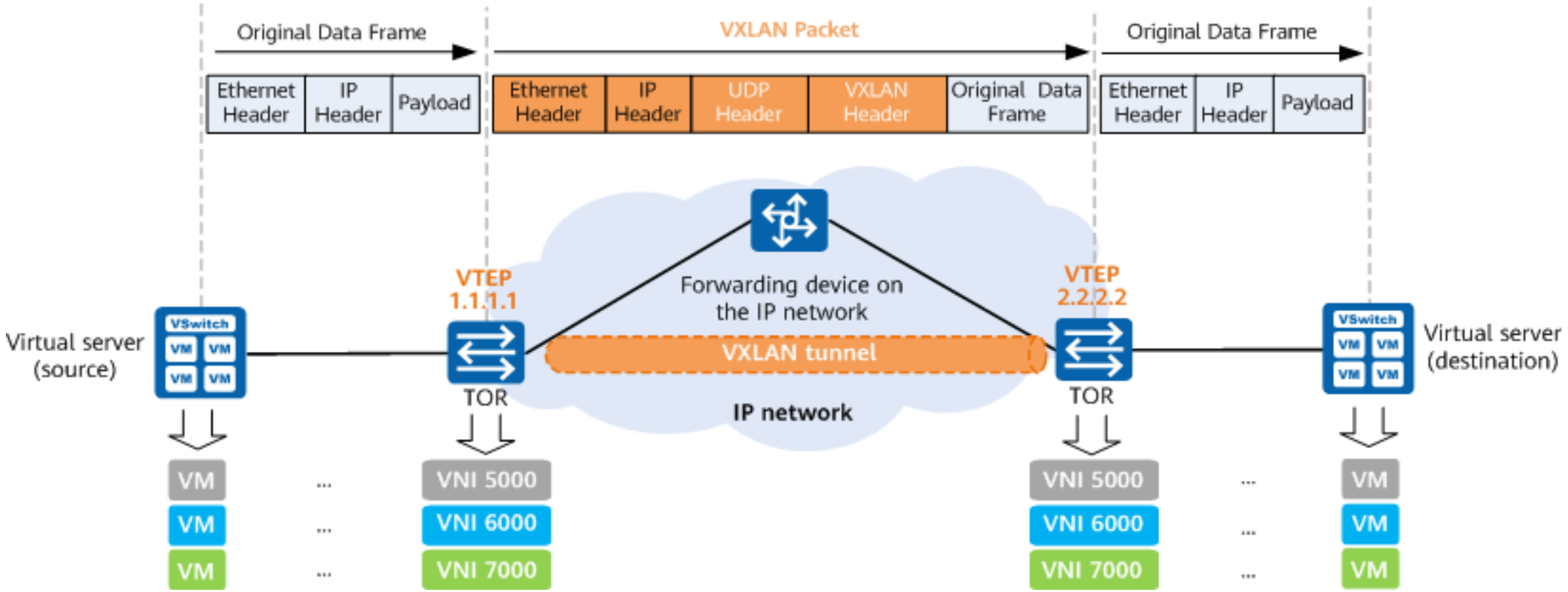
- Pourquoi le VXLAN?

- Dans un datacenter, on peut créer un LAN constitué de serveurs situés sur des zones géographiques différents. Ces serveurs peuvent être considérés comme des commutateur L2. Ainsi, la migration dynamique des VM à travers tout le datacenter (plusieurs zones géographiques) devient possible.

- Le VLAN ID n'a que 12 bits. ce qui signifie qu'il ne peut adresser que 4096 VLAN. lors de la refonte des protocoles pour la virtualisation, le VXLAN s'est vu attribuer 24 bits d'adresse, ce qui lui permet de disposer 16 millions ID.

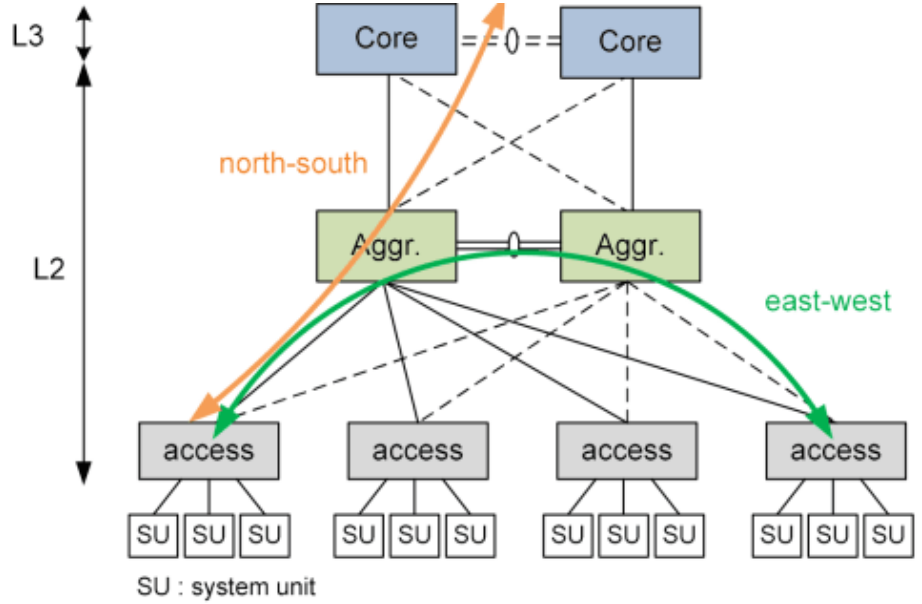
❑ VXLAN : architecture

- VTEP (Virtual Tunnel Endpoint): il s'agit du point de départ ou d'arrivée d'un tunnel VXLAN, qui encapsule et décapsule respectivement les trames de données utilisateur originales.
- VNI (Virtual Network Interface): un identifiant de 24 bits similaire à un ID de VLAN. Les VM avec des VNI différents ne peuvent pas communiquer au niveau de la couche 2.



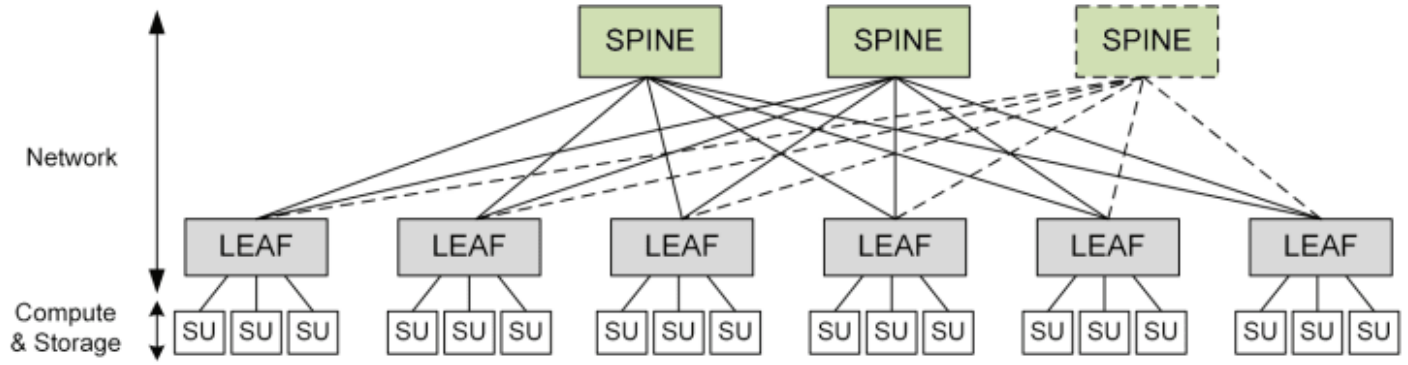
❑ Cloud Computing : CLOS fabric

Avec l'utilisation croissante des techniques de virtualisation, le trafic au sein du datacenter (Est-Ouest) a fortement augmenté. Les architectures de réseau des datacenters, initialement conçues pour répondre aux besoins de trafic Nord-Sud, se sont révélées inadaptées. La bande passante d'accès n'a cessé d'augmenter de 10G, 40G, 100G à 400G.



Le routage étant effectué à un niveau haut dans l'infrastructure, le trafic échangé entre les applications d'un même datacenter saturait rapidement les liens Nord-Sud. La quasi-totalité du trafic, même local, remonte vers les routeurs cœur.

Afin de répondre à cette augmentation du trafic au sein du datacenter, une nouvelle architecture fabric a été mise en place, appelée **CLOS fabric**. Elle est basée sur de nouveaux protocoles, éliminant Spanning-Tree et optimisant l'utilisation de tous les liens.



❑ Réseaux traditionnels : problématique

L'approche traditionnelle du réseau se caractérise par deux facteurs principaux :

1. Les fonctionnalités réseau sont principalement implémenté dans un équipement dédié : routeur, commutateur, pare-feu…
2. La plupart des fonctionnalités réseau sont implémentées dans du matériel dédié : ASIC (Application-Specific Integrated Circuit).

Les entreprises/organisations sont de plus en plus confrontées aux limites qui accompagnent cette approche centrée sur le matériel :

- La configuration traditionnelle prend beaucoup de temps et est sujette aux erreurs : configuration manuelle pour l'ajout/suppression de matériels, configuration VLAN, ACL, QoS, implémentation de politiques réseau…
- Les environnements multi-constructeurs exigent un haut niveau d'expertise : un administrateur doit avoir une connaissance approfondie de tous les types de d'équipements présents.
- Passage à l'échelle : l'impossibilité d'avoir un réseau qui s'adapte au trafic oblige les opérateurs à surprovisionner leurs réseaux.

❑ Plan de contrôle / plan de données

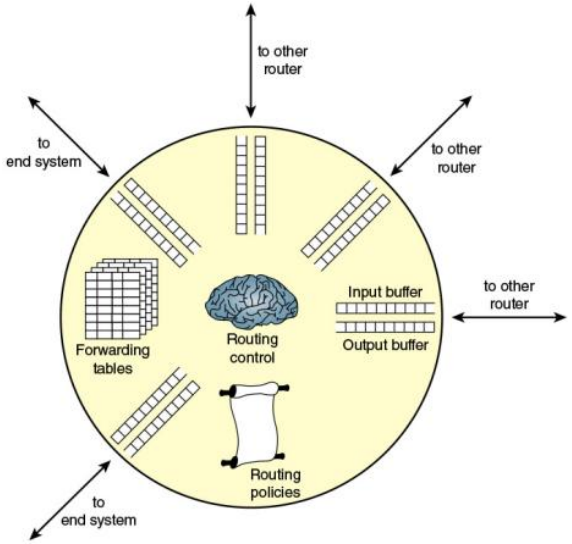
- Plan de données (data plane) : est la partie du réseau comportant le trafic des utilisateurs. Concerne toutes les activités impliquent des paquets de données envoyés par l'utilisateur final :
  - Transmission
  - Fragmentation et réassemblage
  - Réplication pour la multidiffusion
- Plan de contrôle (control plane) : est la partie du réseau comportant le trafic de signalisation et de routage. Concerne toutes les activités nécessaires à l'exécution du plan de données mais qui n'impliquent pas les paquets de données de l'utilisateur final
  - Création de tables de routage
  - Définition des politiques de traitement des paquets (par exemple, sécurité)

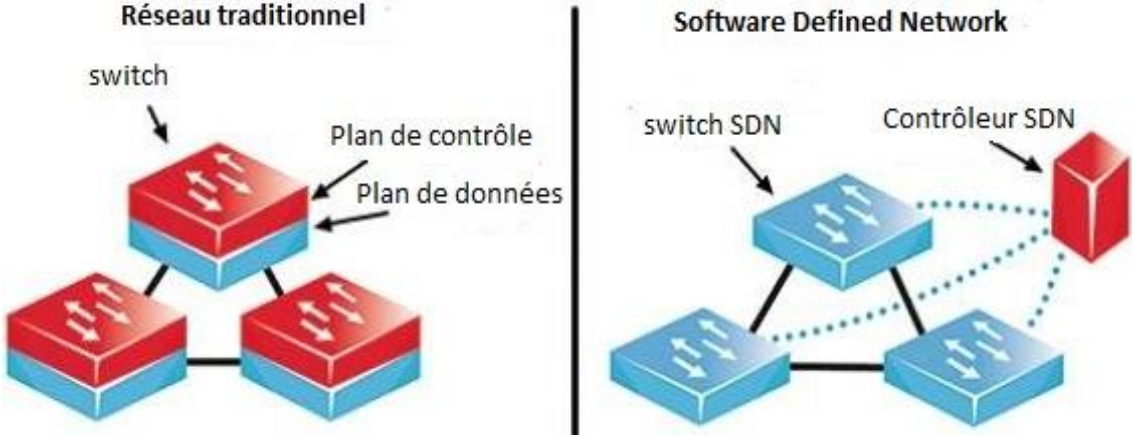
❑ Séparation plan de contrôle / plan de données

Dans les réseaux traditionnels, le plan de contrôle et le plan de données sont exécutés sur un même matériel. Dans les réseaux programmables, la séparation de ces deux plans implique :

- De laisser le plan de données au matériel du réseau.
- De déplacer le plan de contrôle vers un contrôleur central.
- Les commutateurs n'ont que des éléments de transmission.
- En programmant le contrôleur, nous pouvons rapidement changer le comportement de l'ensemble du réseau, il s'agit du :

  => Software Defined Networking





❑ Transition vers le SDN et NFV

- Plus de QoS et QoE

Avec l'augmentation constante du volume et de la variété du trafic réseau, généré par des sources à forte demande de trafic telles que le **big data**, le **cloud computing** et le **réseau mobile**, il devient de plus en plus difficile de répondre à des exigences strictes en matière de QoS et de QoE.

- Plus d'agilité et d'efficacité

Les entreprises ont éprouvé le besoin d'exécuter de nouvelles configurations et opérations à distance sur leurs infrastructures. Cela a rapidement montré les avantages des solutions d'automatisation. Les entreprises ont également migré vers le Cloud à la recherche d'infrastructures évolutives. Ces capacités d'infrastructure réseau, en plus d'une solide approche de la virtualisation, ont été des facteurs clés pour envisager:

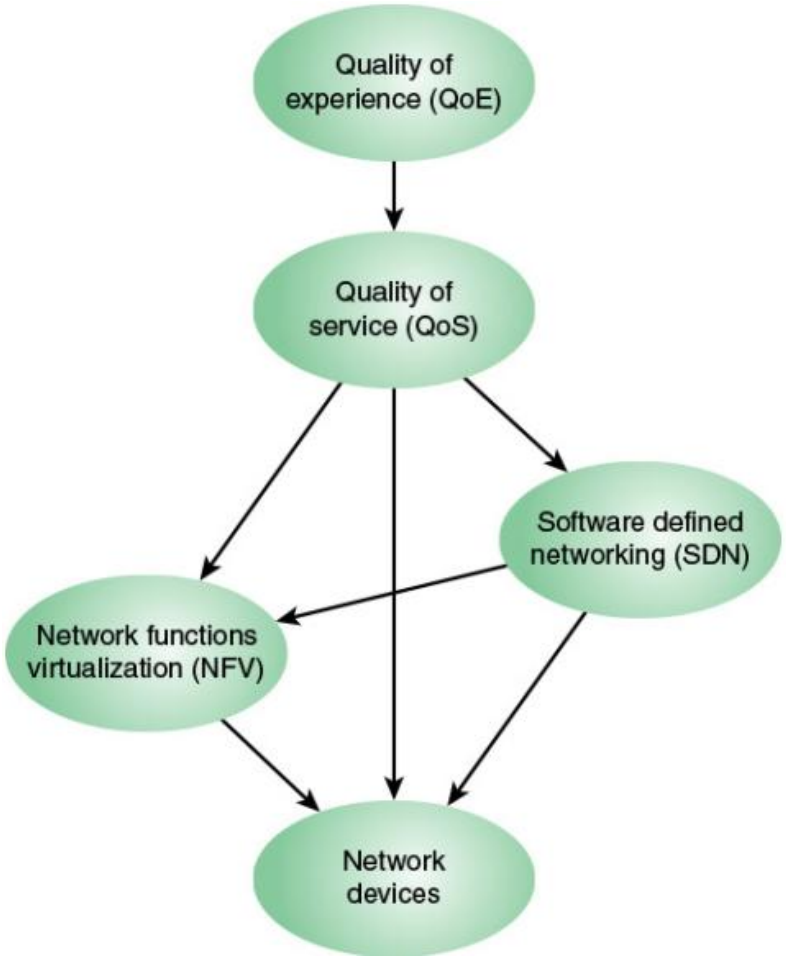
- **Software-Defined Networking (SDN) :** approche basée sur l'automatisation de la mise en œuvre et de la gestion des réseaux par le biais du plan de contrôle programmable.
- **Network Functions Virtualization (NFV) :** approche basée sur la virtualisation qui permet de s'affranchir des contraintes des équipements génériques pour l'implémentation de fonctions réseau (routeur, commutateur, pare feu, IDS/IPS…).

❑ Eléments de réseaux modernes

Les mesures de QoS sont généralement utilisées pour spécifier le service requis par les différents utilisateurs du réseau et pour dicter les politiques de gestion du trafic utilisées sur le réseau.

- En cas d'utilisation seule de NFV, les fonctions de réseau sont implémentées de façon logicielle et exécutées sur des VM. Les paramètres de QoS sont communiqués aux VM.
- En d'utilisation seule du SDN, les fonctions de contrôle réseau sont implémenté sur un contrôleur. Ce dernier est responsable de l'application des paramètres de QoS pour les différents utilisateurs.
- Si SDN et NFV sont utilisés dans un réseau, les relations suivantes s'appliquent :
  - Le plan de données est virtualisé (sur les VM) via la NFV
  - Le plan de contrôle devient programmable via le SDN

Si des considérations de QoE entrent en jeu, elles sont utilisées pour ajuster les paramètres de la QoS.



❑ Eléments de réseaux modernes : cas d'utilisation

Un bon moyen de comprendre l'importance du réseau SDN est d'examiner la façon dont il est utilisé dans la pratique.

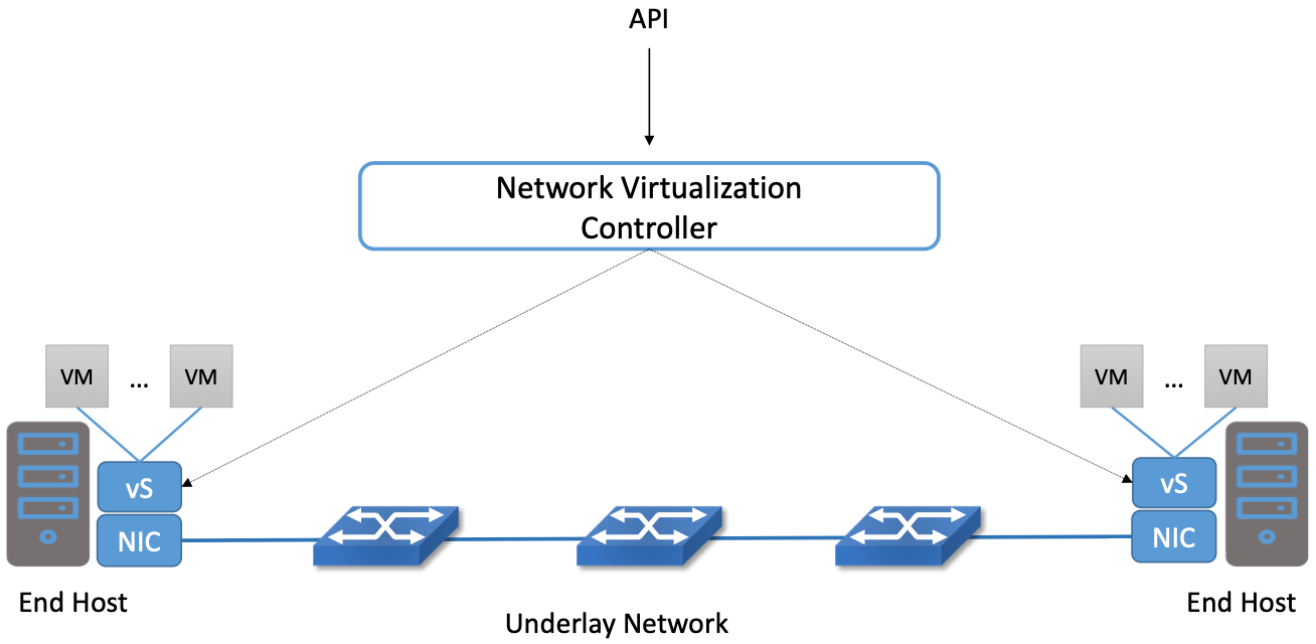
- Le SDN est largement déployé par les fournisseurs Cloud. Google, Facebook et Microsoft étant ceux qui l'ont le plus ouvertement adopté. Cependant leurs solutions sont encore en grande partie propriétaires.
- Les grands opérateurs de réseaux comme AT&T, DT, NTT et Comcast parlent publiquement de leurs projets de déploiement de solutions SDN, en particulier dans leurs réseaux d'accès. Cependant la plupart de leurs initiatives utilisent des approches hybrides.
- Les entreprises ont commencé à adopter le SDN. Aujourd'hui, la virtualisation des réseaux et le SD-WAN connaissent un succès considérable dans les entreprises.

❑ Eléments de réseaux modernes : cas d'utilisation

(1) Virtualisation des réseaux

Le contrôleur de virtualisation de réseau est un contrôleur SDN qui expose une API nord permettant de créer, de surveiller et de modifier des réseaux.

- Le contrôleur se connecte à des commutateurs virtuels fonctionnant sur des hyperviseurs prenant en charge des machines virtuelles.
- Les réseaux virtuels sont créés en programmant les commutateurs virtuels pour qu'ils transmettent les paquets, avec l'encapsulation appropriée, d'un hôte à l'autre à travers le réseau sous-jacent.

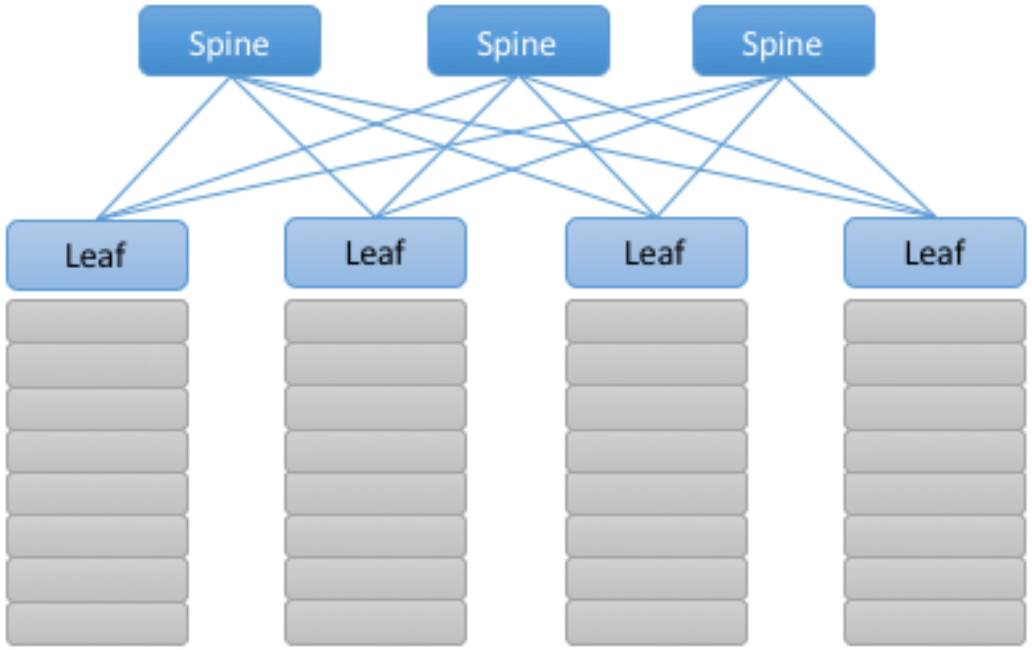


❑ Eléments de réseaux modernes : cas d'utilisation

(2) Switch Fabric (matrice de commutation)

Les fournisseurs Cloud ont abandonné les commutateurs propriétaires au profit de commutateurs *bare-metal*. Le switch fabric, basé sur une topologie en matrice, est contrôlé de manière entièrement logicielle.

- Chaque rack dispose d'un commutateur Top-of-Rack (ToR) qui interconnecte les serveurs de ce rack. Ces commutateurs sont appelés *leaf switches*.
- Le logiciel de contrôle de la *fabric* implémente la commutation L2 à l'intérieur des racks et le routage L3 entre les racks.
- Comme chaque ToR est à 2 sauts de tous les autres ToR, il existe plusieurs chemins à coût égal.



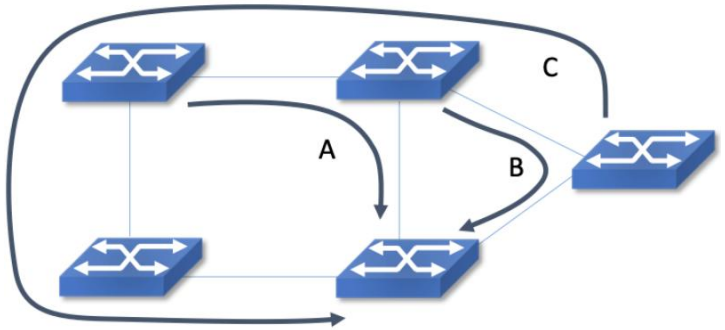
❑ Eléments de réseaux modernes : cas d'utilisation

(3) Ingénierie du trafic pour les réseaux étendus (WAN)

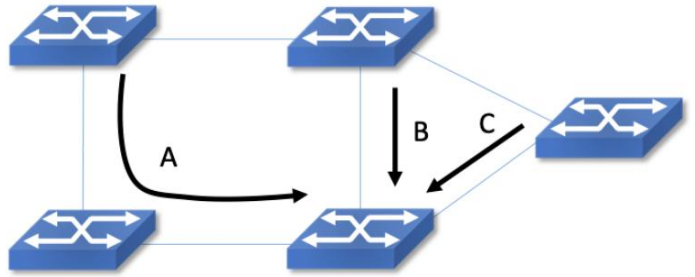
Un autre cas d'utilisation inspiré dans le Cloud est l'ingénierie du trafic appliquée aux liaisons à grande distance entre les datacenters. Le backbone de Google, appelé B4, est entièrement construit à l'aide de commutateurs bare-metal et de SDN. De même, Microsoft a défini une approche d'interconnexion appelée SWAN.

On suppose que les liens ont les mêmes capacités.

- Le flux A est placé en choisissant l'un des deux chemins les plus courts. Le flux B est placé ensuite et prend l'autre chemin plus court. Lorsque le flux C est placé en dernier, il n'y a pas d'autre choix que le chemin le plus long.
- Avec un algorithme central qui examinerait les trois flux, le placement des flux se fera de façon optimale de sorte que l'ensemble de chemins empruntés soient les plus courts possibles.



Ingénierie du trafic non optimale



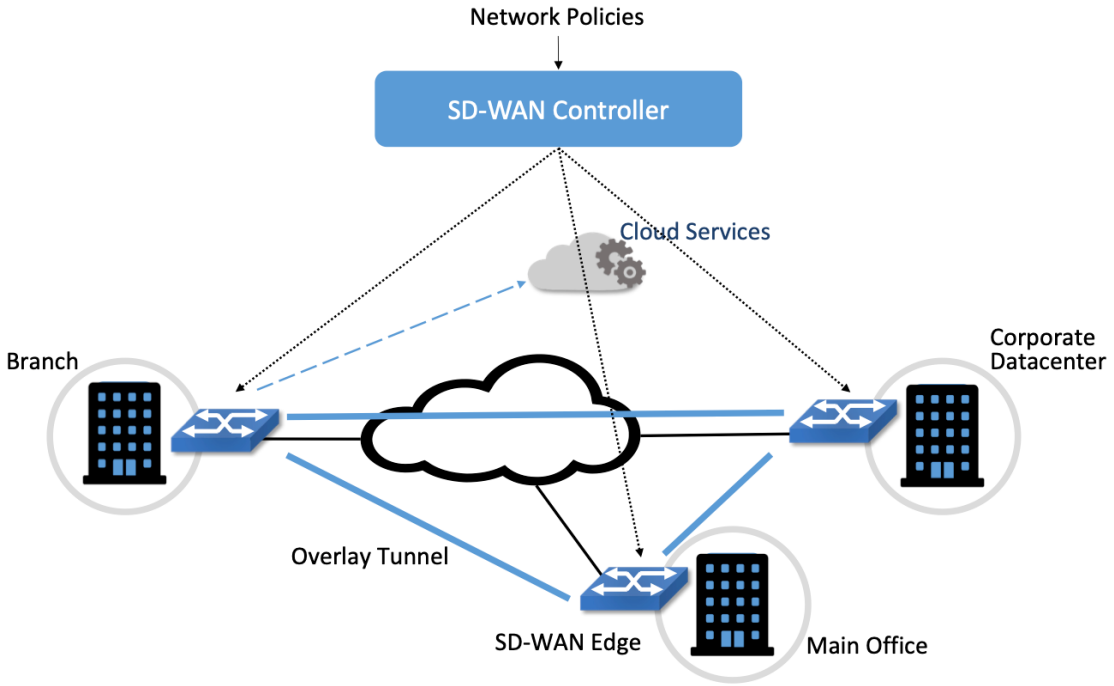
Ingénierie du trafic optimale

❑ Eléments de réseaux modernes : cas d'utilisation

(4) SD-WAN

L'essor rapide du SD-WAN en tant qu'alternative au MPLS est un autre exemple de la puissance du SDN.

- Le provisionnement d'un VPN utilisant MPLS nécessite toujours une configuration locale importante du routeur Customer Edge (CE) et du routeur Provider Edge (PE).
- Une entreprise souhaite généralement appliquer sur ses sites un ensemble de politiques concernant la sécurité, la priorisation du trafic, l'accès aux services, les VPN...
  - Avec, le SD-WAN, ces exigences peuvent être indiquées à un contrôleur central, qui peut ensuite envoyer toute la configuration nécessaire aux commutateurs situés dans les sites appropriés.
  - Cependant les SD-WAN tendent vers des solutions propriétaires.

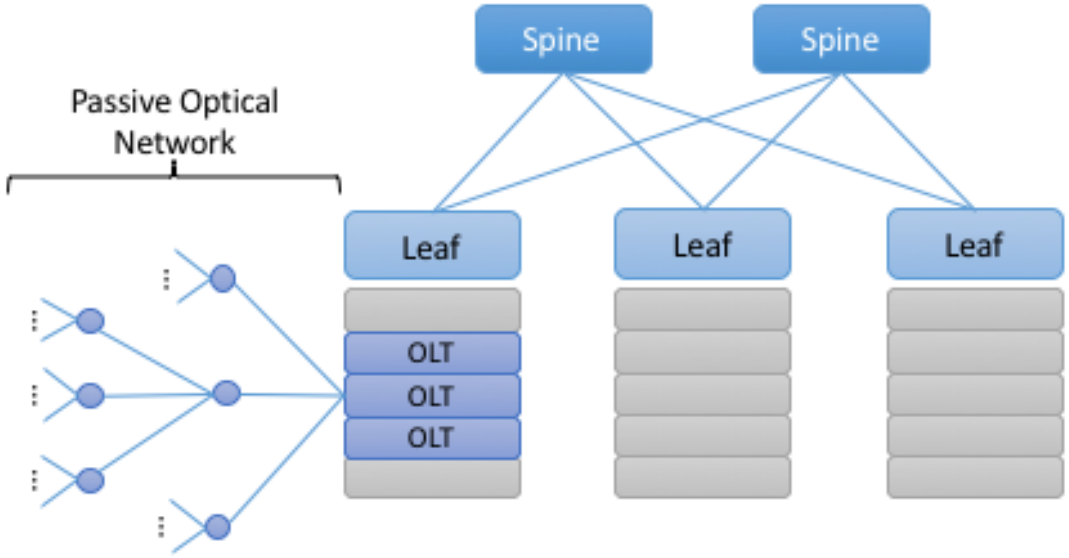


❑ Eléments de réseaux modernes : cas d'utilisation

(5) Réseaux d'accès

Les réseaux d'accès (PON/FTTH, RAN 5G) relient les foyers, les entreprises et les appareils mobiles à l'internet constituent une autre occasion d'appliquer les principes SDN.

- Le défi consiste à transformer les équipements réseaux (OLT, Optical Line Terminals) en leurs équivalents *barre métal*, afin qu'ils puissent être contrôlés par un logiciel.
- Dans le cas du réseau cellulaire, il existe également deux composants à transformer en barre métal: l'eNodeB (la station de base RAN) et l'Enhanced Packet Core (EPC).
- Les SD-RAN conduiront à la 5G Edge Cloud.



❑ Eléments de réseaux modernes : cas d'utilisation

(6) Télémétrie réseau

L'idée de l'INT (In-Band Network Telemetry) est de programmer le pipeline d'acheminement pour collecter l'état du réseau au fur et à mesure que les paquets sont traités. Dans l'approche INT, les « instructions » de télémétrie sont encodées dans les champs d'en-tête des paquets, puis traitées par les commutateurs de réseau.

- Les paquets traversant un chemin allant du commutateur source *S1* au commutateur de destination *S5* en passant par le commutateur de transit *S2*.
- *Exemple :* J'ai visité les commutateurs *S1* @780ns, *S2* @1.3µs et S5 @2.4µs.
- Ces informations peuvent être utilisées, pour détecter les délais de mise en file d'attente de l'ordre de la milliseconde.