MODULE :
Le Cloud Computing & DevOps

Pr. F. Benabbou
Master DSBD
Faculté des Sciences Ben M'Sik Casablanca

TABLE OF CONTENTS

01

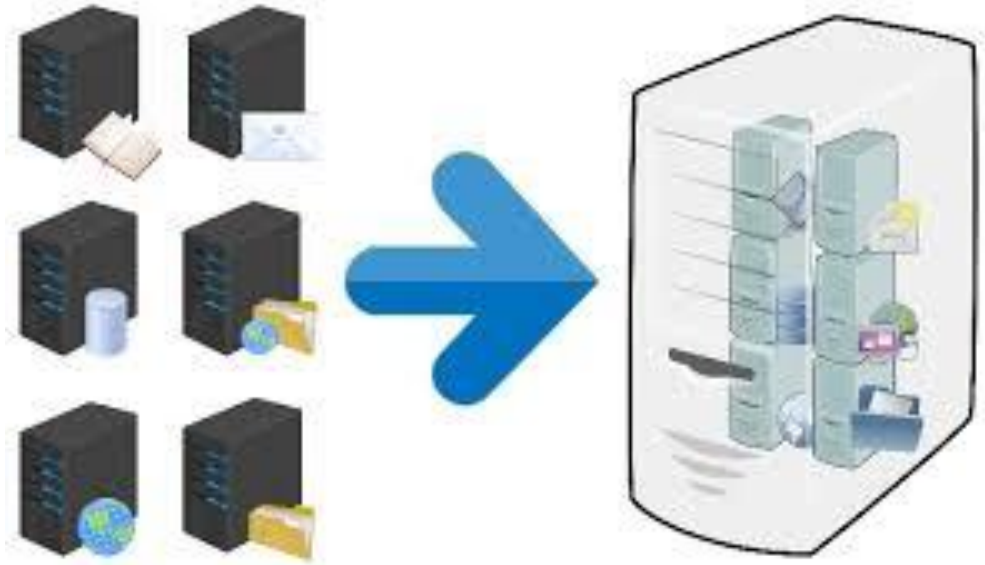
LE CLOUD COMPUTING

Domaines de Virtualisation

- Serveurs
- Réseaux
- Stockage
- postes de travail
- Applications
- etc.

Virtualisation de serveurs

- La virtualisation de serveur permet de regrouper plusieurs serveurs physiques sous-employés sur un seul hôte qui exécute des systèmes virtuels.

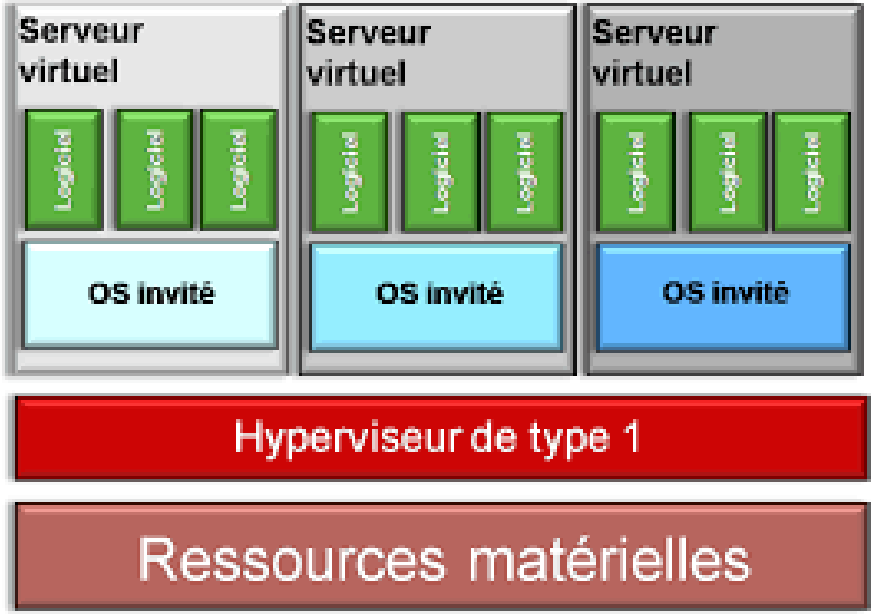


Virtualisation de serveurs

- La virtualisation de serveur permet de d'optimiser la consommation de la capacité des machines physiques

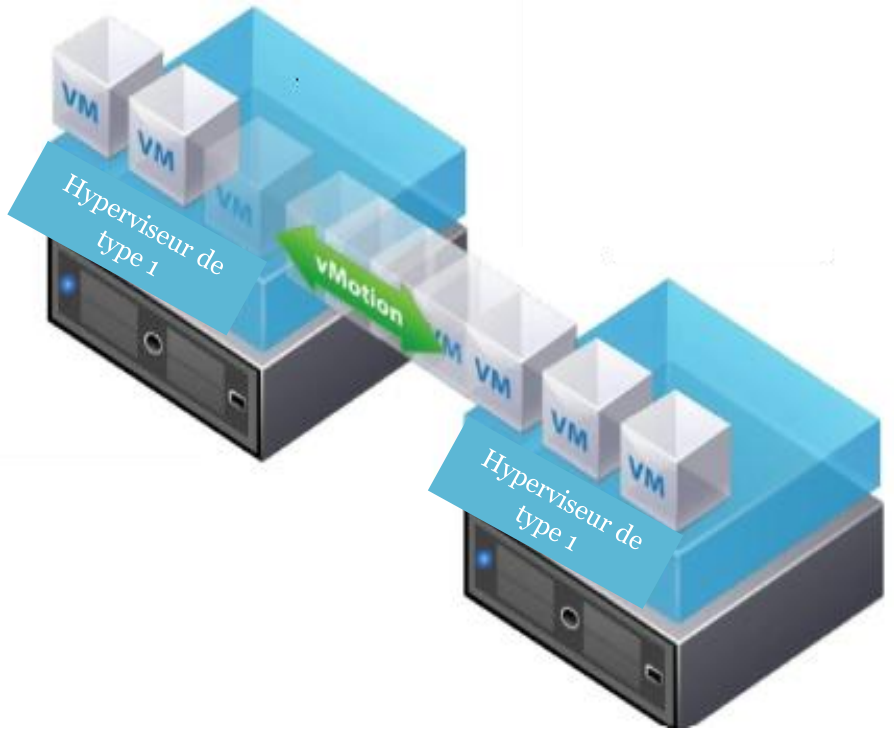
Avantages de la virtualisation de serveurs

- Assurer une meilleure disponibilité grâce à la facilité de déploiement
- Le cloisonnement des serveur sur le serveur physique assure une meilleure sécurité des applications
- Réduire la surface au sol, la consommation électrique, le besoin de climatisation et le nombre d'administrateurs.
- Réaliser des économies (locaux, consommation électrique, personnel).



Avantages de la virtualisation de serveurs

- Meilleures performances grâce à la migration des MVs



Virtualisation de serveurs

- Des outils de P2V (physique vers virtuel) permettent de transformer la plupart des serveurs physiques en machines virtuelles.
- Des outils de conversion de serveur P2V
  - **VMware vCenter Converter :**
    - c'est un outil gratuit fourni par VMware, qui permet de convertir des machines physiques Windows et Linux en machines virtuelles
    - Supporte les conversions à chaud (sans arrêter la machine source) et à froid.
    - Compatible avec vSphere, ESXi, et VMware Workstation.Permet la conversion de formats de machines virtuelles non-VMware (comme Hyper-V, KVM).

Virtualisation de serveurs

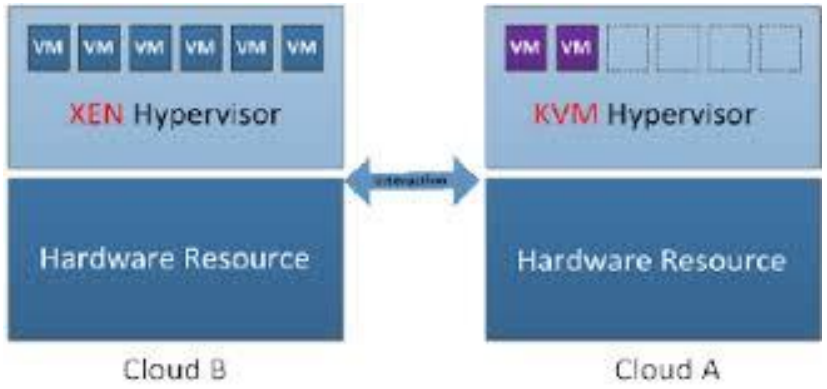
- Des outils de conversion de serveur P2V
  - **Microsoft Virtual Machine Converter :** c'est un outil développé par Microsoft qui permet de convertir des serveurs en machines virtuelles Hyper-V.
  - **Citrix XenConvert :** c'est un outil développé par Citrix qui permet de convertir des serveurs en machines virtuelles XenServer.
  - **Paragon Go Virtual** : c'est un outil de conversion physique vers virtuel qui supporte plusieurs types de formats de machines virtuelles, y compris VMware, VirtualBox, et Microsoft Hyper-V.
  - **Red Hat Virtualization (RHV)** : c'est un outil de Red Hat pour convertir des machines physiques en machines virtuelles dans des environnements Red Hat Virtualization et prend en charge la conversion des systèmes Linux et Windows.

Open Virtualization Format(OVF)

- C’est un format ouvert pour l'emballage et la distribution des systèmes virtuels qui été proposé par l'organisation de normalisation DMTF (Distributed Management Task Force) Reconnu par l'ISO/IEC comme un premier standard international sur la portabilité des systèmes virtuels entres les infrastructures de plateformes IaaS cloud.
- La norme Open Virtualization Format(OVF) est une première étape vers une standardisation des formats de machines virtuelles.
- Elle prend en charge la distribution de machines virtuelles multiplateforme
- Le but est de pouvoir exécuter l’image sur plusieurs plateformes de virtualisation

Portabilité : Open Virtualization Format(OVF)

- Le fichier OVF encapsule :
  - des données nécessaires au fonctionnement d'une machine virtuelle dans le format1 utilisé par chaque éditeur (ex. les images disque au format VHD (Virtual Hard Disk) chez Microsoft ou VMDK[1] chez VMWare)
  - des métadonnées au format XML qui décrivent les caractéristiques de la VM comme ses ressources processeurs, sa quantité de RAM ou encore son espace de stockage, le type de carte réseau utilisé, etc.
- De plus les fichiers OVF contiennent une signature numérique qui permet d'assurer que les machines virtuelles n'ont pas été modifiées depuis leur conception.



- le packaging de machine virtuelle portable et indépendant de la plateforme de Virtualisation et le choix de l'Hyperviseur

[1] format de fichier utilisé pour enregistrer le contenu d'un disque dur virtuel.

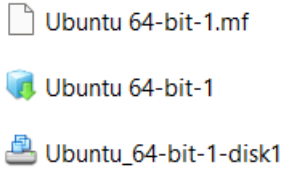
Open Virtual Appliance(OVA)

- OVA est un format de fichiers utilisés pour distribuer des applications virtualisées sous forme d'appliance.
- Une appliance virtuelle, est une :
  - machine virtuelle préconfigurée, qui inclut un système d'exploitation et des applications spécifiques préinstallées et préconfigurées.
  - solution logicielle prête à l'emploi, qui inclut tout ce dont l'utilisateur a besoin pour exécuter une tâche spécifique.
- Les appliances sont souvent utilisées dans des environnements d'entreprise pour déployer rapidement des applications et des services, sans avoir à effectuer une installation et une configuration manuelles,
- OVA est un format de fichier de type archive qui contient un fichier OVF et tous les fichiers associés à la machine virtuelle, tels que les disques durs virtuels, les images ISO, les scripts, etc.

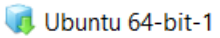
OVF vs OVA

- OVF est utilisé pour la distribution de machines virtuelles individuelles et pour la création d'appliances personnalisées répondant aux besoins de l'utilisateur.
- OVA est une archive utilisée pour distribuer des appliances virtualisées complètes.
- OVF utilise plusieurs fichiers et Ova un seul

Répertoire pour OVF



Répertoire pour OVA



- Ils peut être utilisés avec différentes plateformes de virtualisation, telles que VMware, Microsoft Hyper-V, Xen, KVM,...

La virtualisation de réseaux

- Deux approche pour construire des réseaux virtuels
  - Approches classiques ne se basant pas sur la virtualisation
    - VLAN, VPN
  - Approches basées sur le virtualisation
    - Software-Defined Networking
    - Network Function Virtualization
    - …

La virtualisation de réseaux

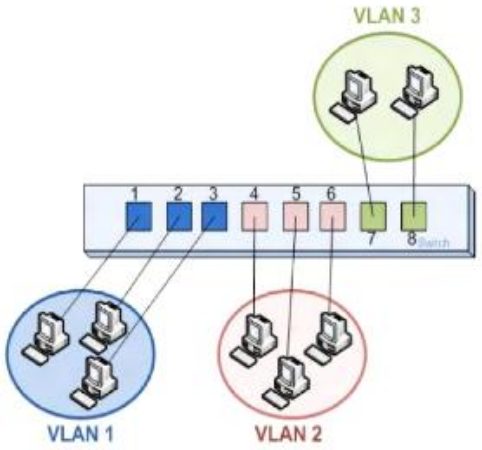
- De manière générale, la virtualisation des réseaux consiste à partager une même infrastructure physique (débit des liens, ressources CPU des routeurs,...) au profit de plusieurs réseaux virtuels isolés.
- Plusieurs techniques ont été utilisées pour créer des réseaux virtuels comme les VLANs (réseaux locaux virtuels) et les VPNs (réseaux privés virtuels).
- Un VLAN est un réseau local regroupant un ensemble de machines de façon logique et non physique.
- Les VPN sont généralement utilisés pour fournir un canal de communication sécurisé entre plusieurs sites géographiquement distants

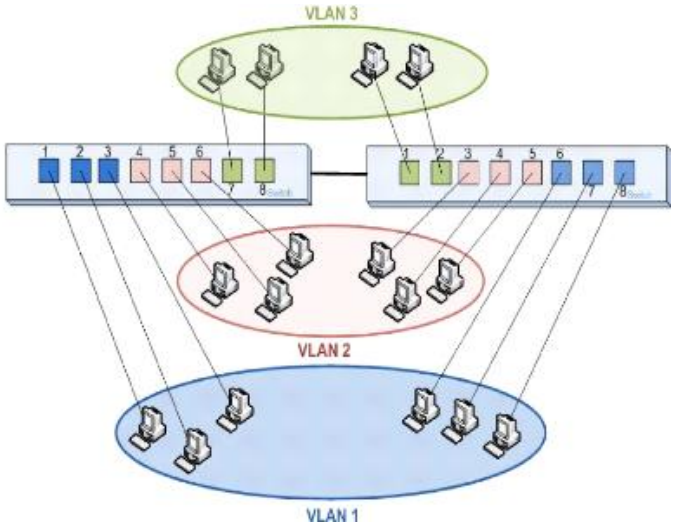
La virtualisation de réseaux

- On distingue plusieurs types de réseaux virtuels :
  - Les réseaux virtuels de niveau 1
  - Les réseaux virtuels de niveau 2
  - Les réseaux virtuels de niveau 3

La virtualisation de réseaux

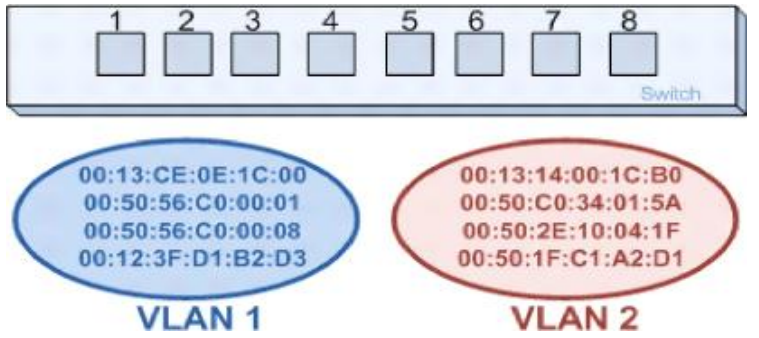
- Les réseaux virtuels de niveau 1, sont appelés réseaux virtuels par port (port-based VLAN)
- ils définissent un réseau virtuel en fonction des ports de raccordement sur le commutateur (switch).
- On associe un port physique de ce commutateur à un numéro de VLAN
- Le principal inconvénient d'un VLAN de niveau 1 est sa rigidité
- si une station se raccorde physiquement au réseau par l'intermédiaire d'un autre port du commutateur, alors il est nécessaire de reconfigurer ce commutateur afin de réintégrer la station dans le bon réseau virtuel.





La virtualisation de réseaux

- Les réseaux virtuels de niveau 2, sont appelés réseaux virtuels par adresse MAC (MAC address-based VLAN)
- ils consistent à définir un réseau virtuel sur la base des adresses MAC des stations.
- Une adresse MAC est un identifiant unique implémenté dans chaque adaptateur réseau.
- Ce type de VLAN est beaucoup plus souple que le précédent car il est indépendant de la localisation de la machine.

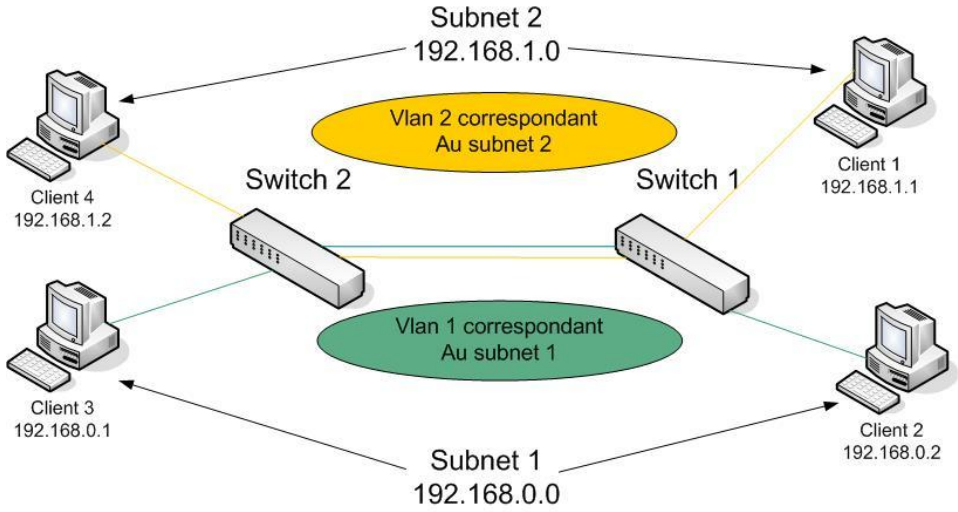


La virtualisation de réseaux

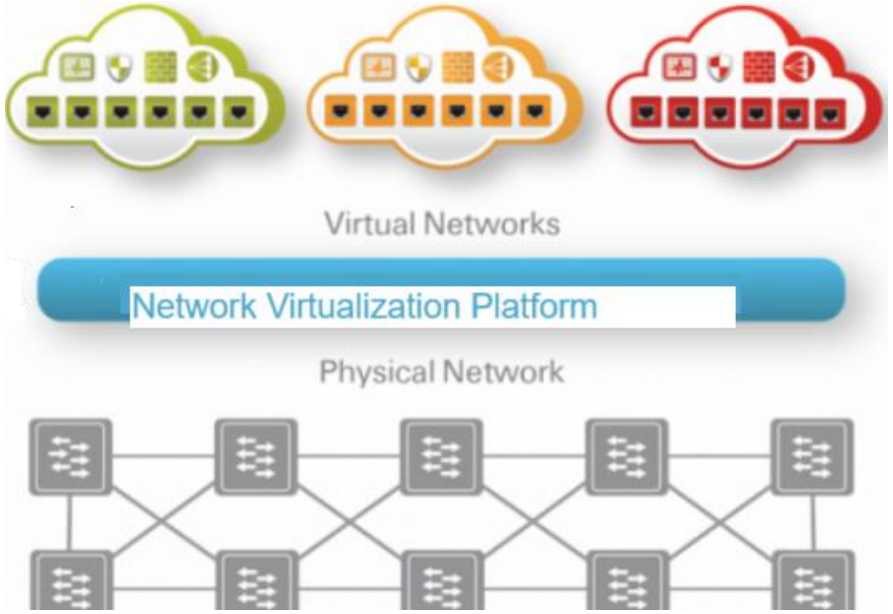
- On distingue principalement deux types de VLAN de niveau 3:
  - Les réseaux virtuels par adresse de sous-réseau (Network address-based VLAN)
  - Les réseaux virtuels par protocole (Protocol-based VLAN):

La virtualisation de réseaux

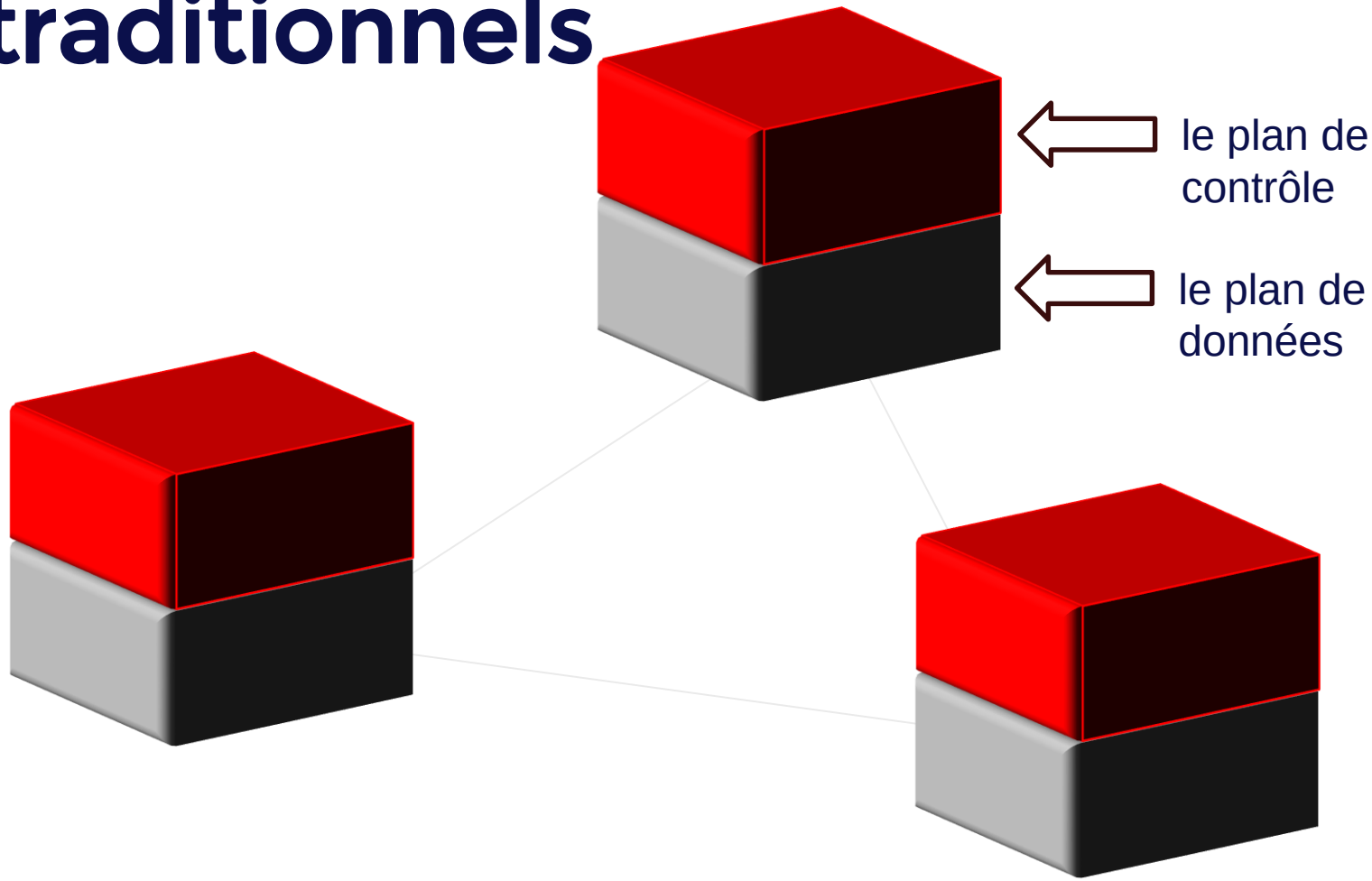
- Les réseaux virtuels par adresse de sous-réseau (Network address-based VLAN):
  - Ils permettent de regrouper plusieurs machines suivant le sous réseau auxquels elles appartiennent. L'adresse va déterminer à quel Vlan appartient la machine
  - Ce type de réseau virtuel est très flexible puisque les commutateurs adaptent automatiquement leur configuration lorsqu'une station est déplacée.
  - Les Vlans de niveau 3 souffrent de lenteur, le switch est obligé de décapsuler le paquet jusqu'à l'adresse IP pour pouvoir détecter à quel Vlan il appartient.
- Les réseaux virtuels par protocole (Protocol-based VLAN): les réseaux virtuels sont créés sur la base des protocoles utilisés (TCP/IP, IPX,...) et les stations sont regroupées en réseaux virtuels suivant le protocole qu'elles utilisent.



Techniques de virtualisation des réseaux



Les réseaux traditionnels



Le réseau traditionnel utilise des dispositifs matériels fixes et dédiés tels que des routeurs et des commutateurs pour contrôler le trafic du réseau.

Les réseaux traditionnels

Les Inconvénients des réseaux traditionnels

1. Approvisionnement Lent

Les composants réseaux se charge du contrôle et les données

2. Complexité & Risque d'erreur

Difficulté de surveiller et de configurer manuellement chaque appareil.

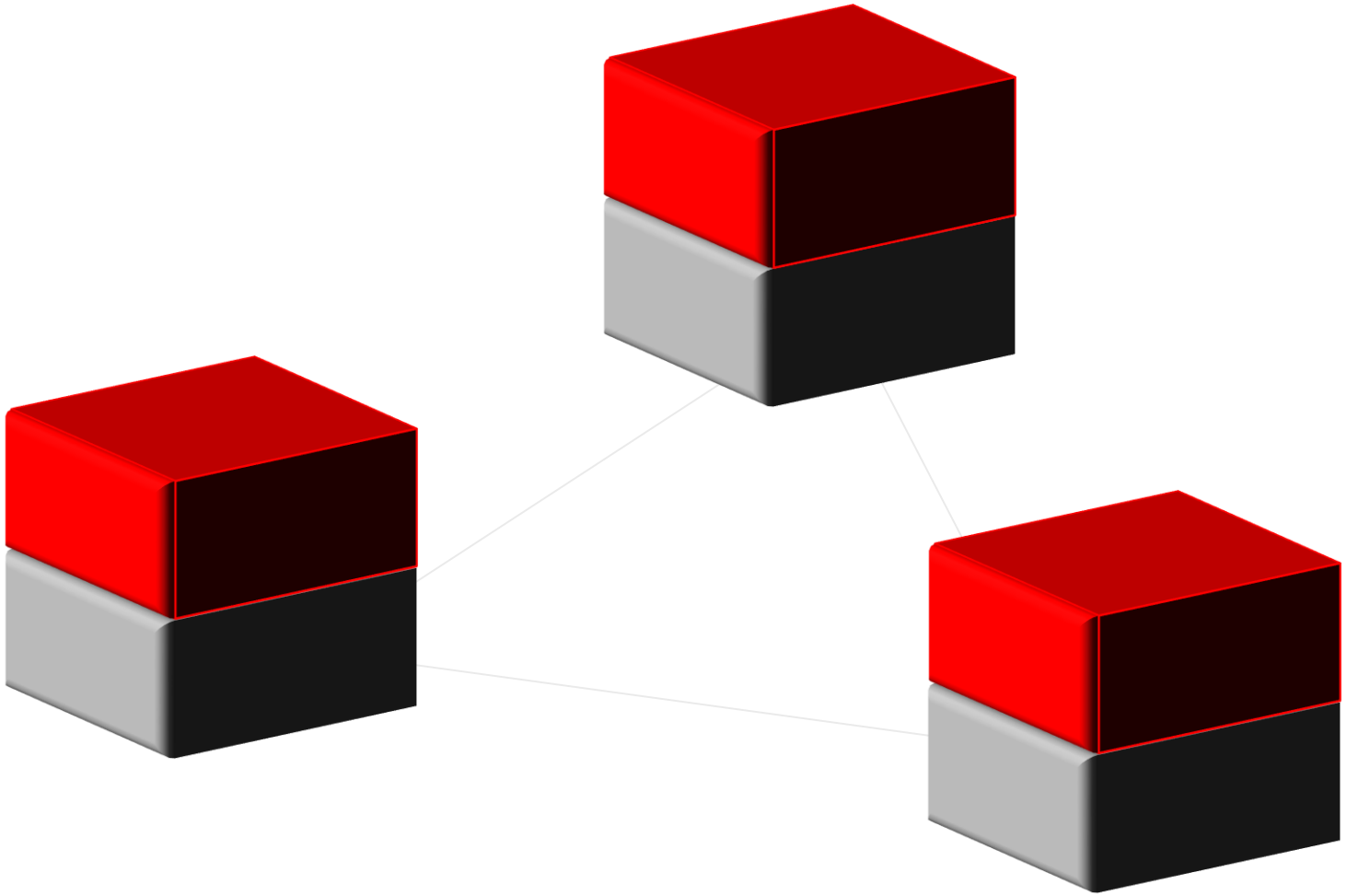
3. Manque de flexibilité

Les périphériques possèdent une configuration matérielle statique. Les modifications, telles que l'ajout ou la suppression d'appareils, nécessitent des interventions manuelles complexes.

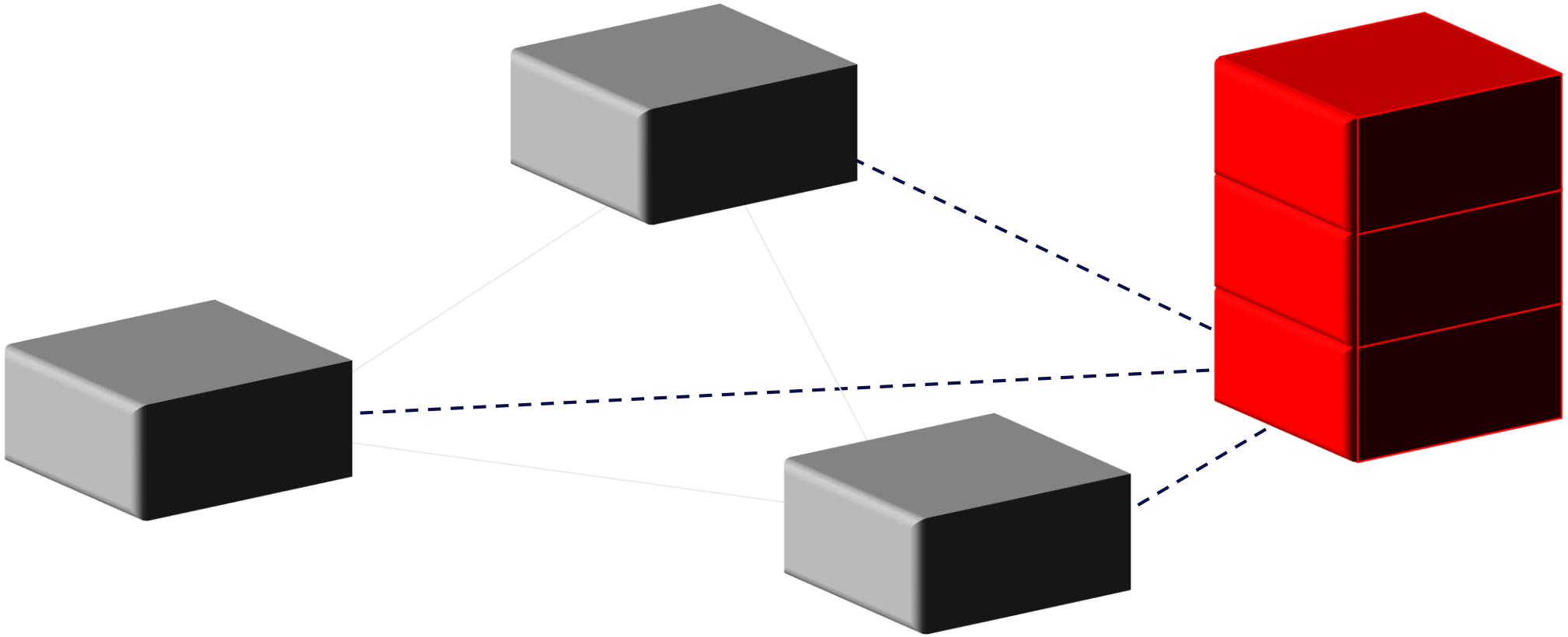
4. Scalabilité limité

Difficulté de répondre aux besoins croissants. Tout ajout nécessite souvent des ajustements de l’infrastructure physique

Software-Defined Networking (SDN)



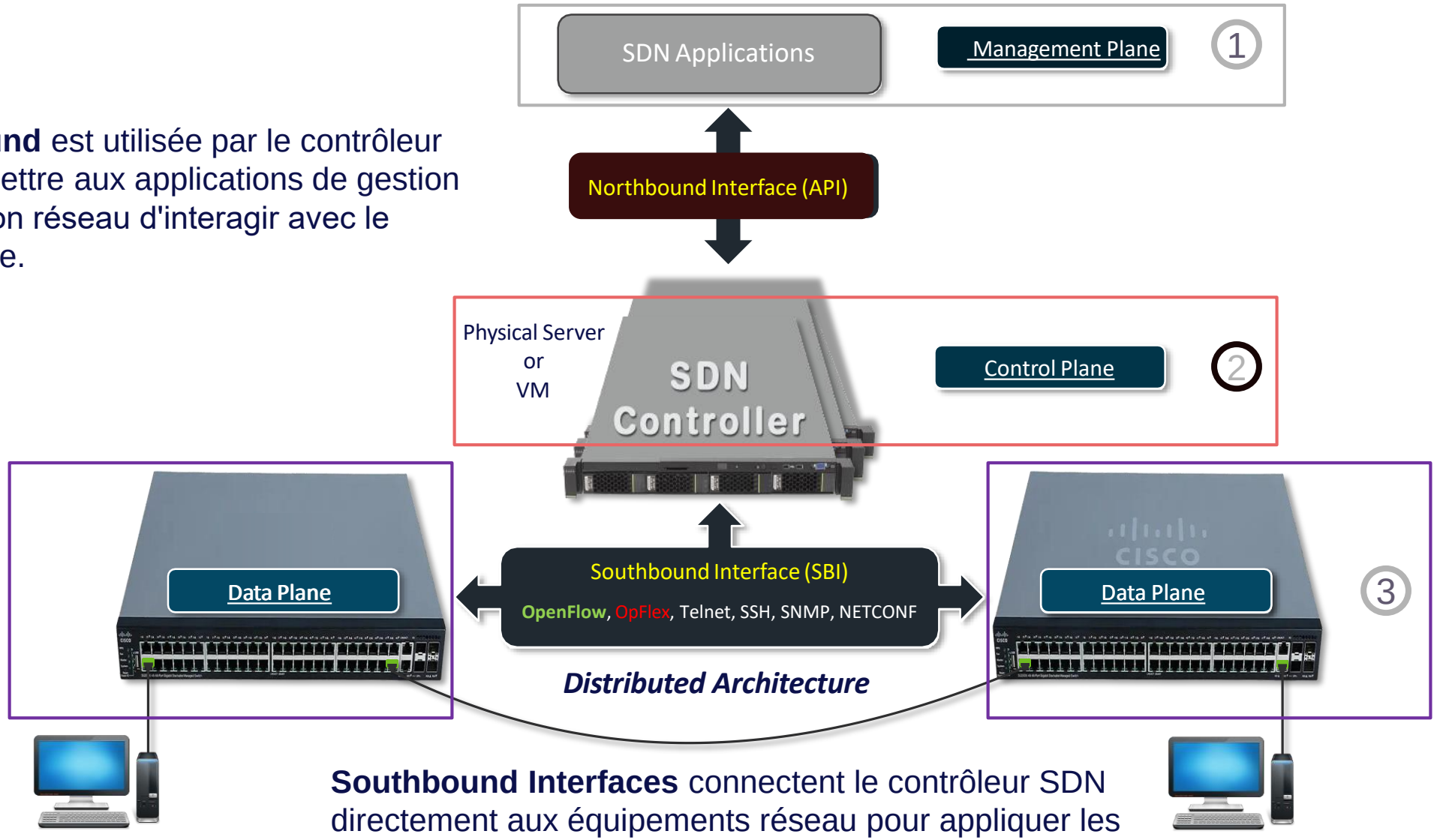
Software-Defined Networking (SDN)



- SDN est une approche de conception et de gestion des réseaux informatiques
- Un réseau défini par logiciel consiste à séparer la couche de gestion des flux de la couche de données qui transmet le trafic réseau.
- La gestion du réseau est centralisée en utilisant un contrôleur SDN

L’Architecture de SDN

L'API **northbound** est utilisée par le contrôleur SDN pour permettre aux applications de gestion et d’orchestration réseau d'interagir avec le réseau lui-même.



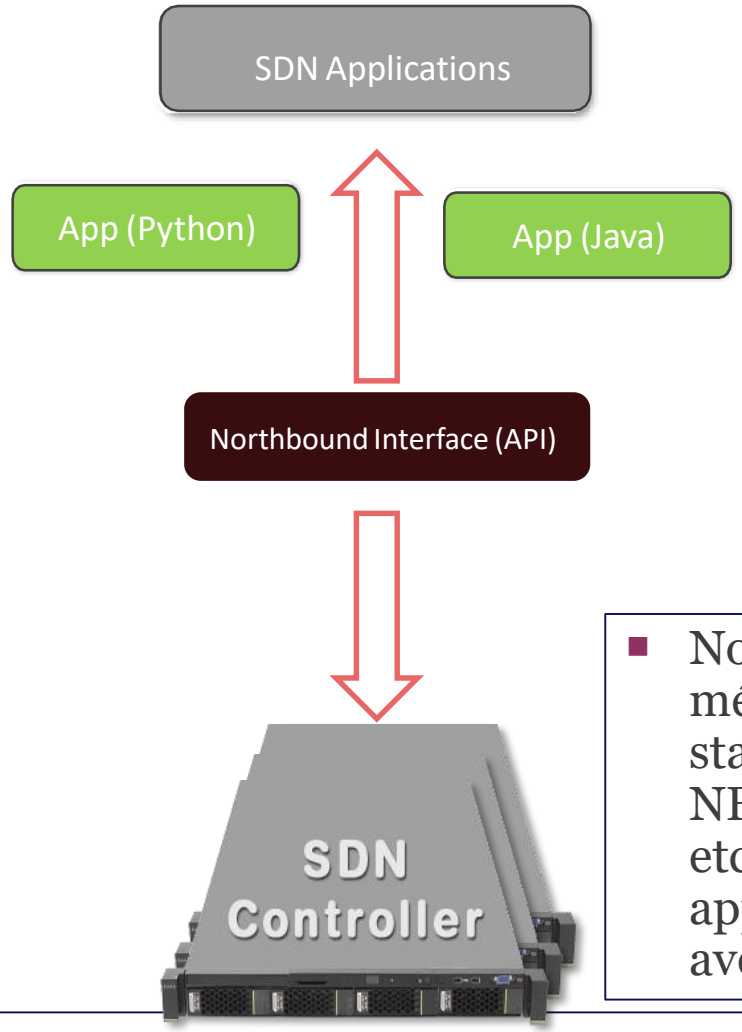
Southbound Interfaces connectent le contrôleur SDN directement aux équipements réseau pour appliquer les politiques et configurations décidées au niveau supérieur

L'Architecture de SDN

1 Management Plane

- La couche d'application fait référence aux applications et services qui s'exécutent au-dessus du contrôleur SDN.

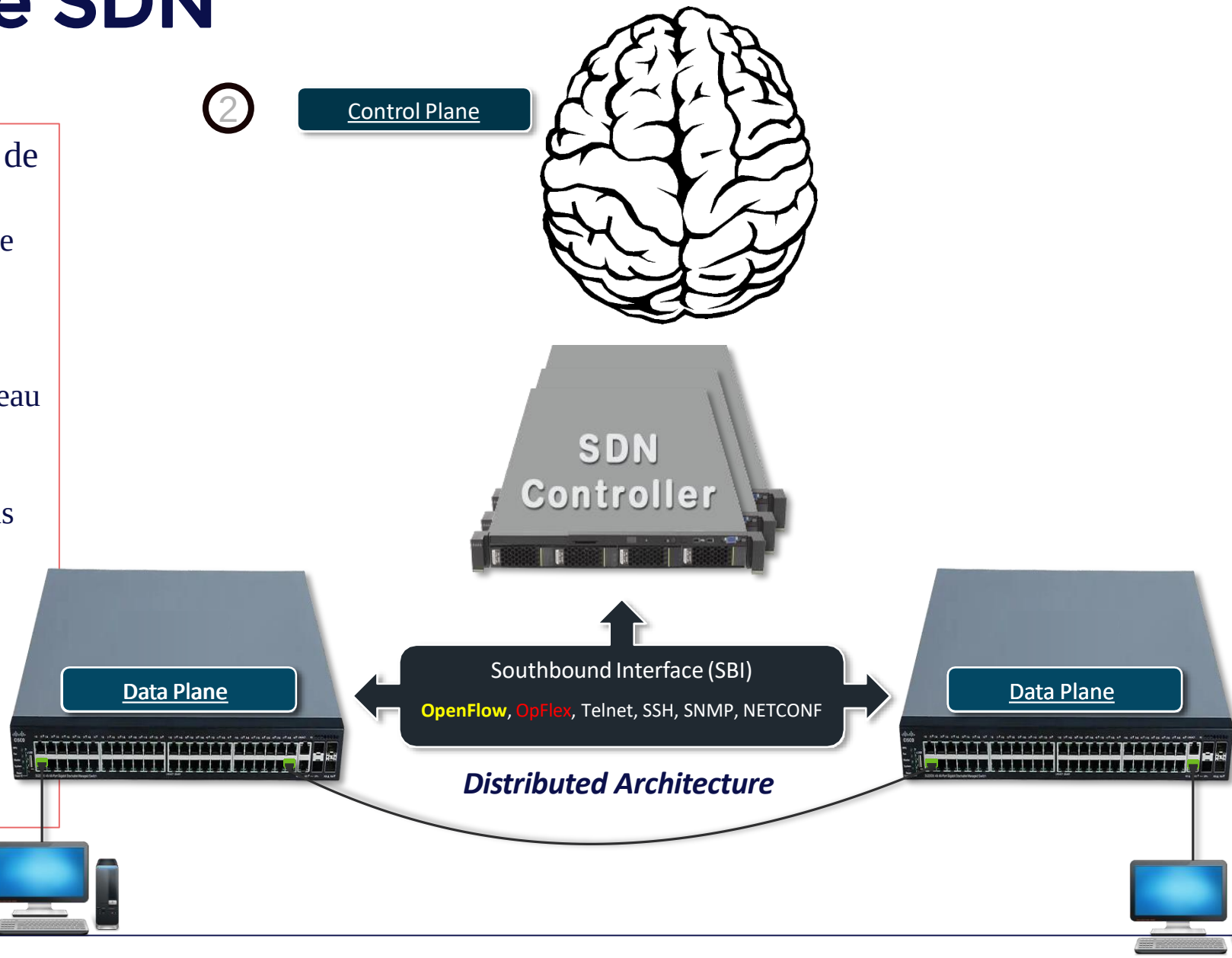
- Responsable de la configuration initiale des équipements et de l'application des politiques réseau.
- Permet aux administrateurs de définir des règles et des stratégies globales pour la sécurité, le routage et la priorisation du trafic.
- Surveillance et collecte de données
- configurer et appliquer les règles de sécurité, telles que les politiques d'accès, les pare-feu, et les systèmes de détection d'intrusion.



- Northbound API fournit les mécanismes de communication standardisés, tels que REST API, NETCONF, OpenFlow Java API, etc..., pour permettre aux applications externes d'interagir avec le contrôleur SDN.

L'Architecture de SDN

- Control Plane de (SDN) permet de gérer et de contrôler le flux de trafic du réseau.
  - prend les décisions concernant la gestion, le routage et la configuration du réseau
  - détermine le meilleur chemin pour les données
  - Programme et automatise la gestion du réseau via des API.
  - applique les règles et les politiques réseau, comme les priorités de trafic, les limitations de bande passante, et les règles de sécurité
- Cette centralisation :
  - permet une vue d'ensemble du réseau et simplifie la gestion des configurations et politiques réseau.
  - permet aux équipements hétérogènes de fonctionner ensemble.

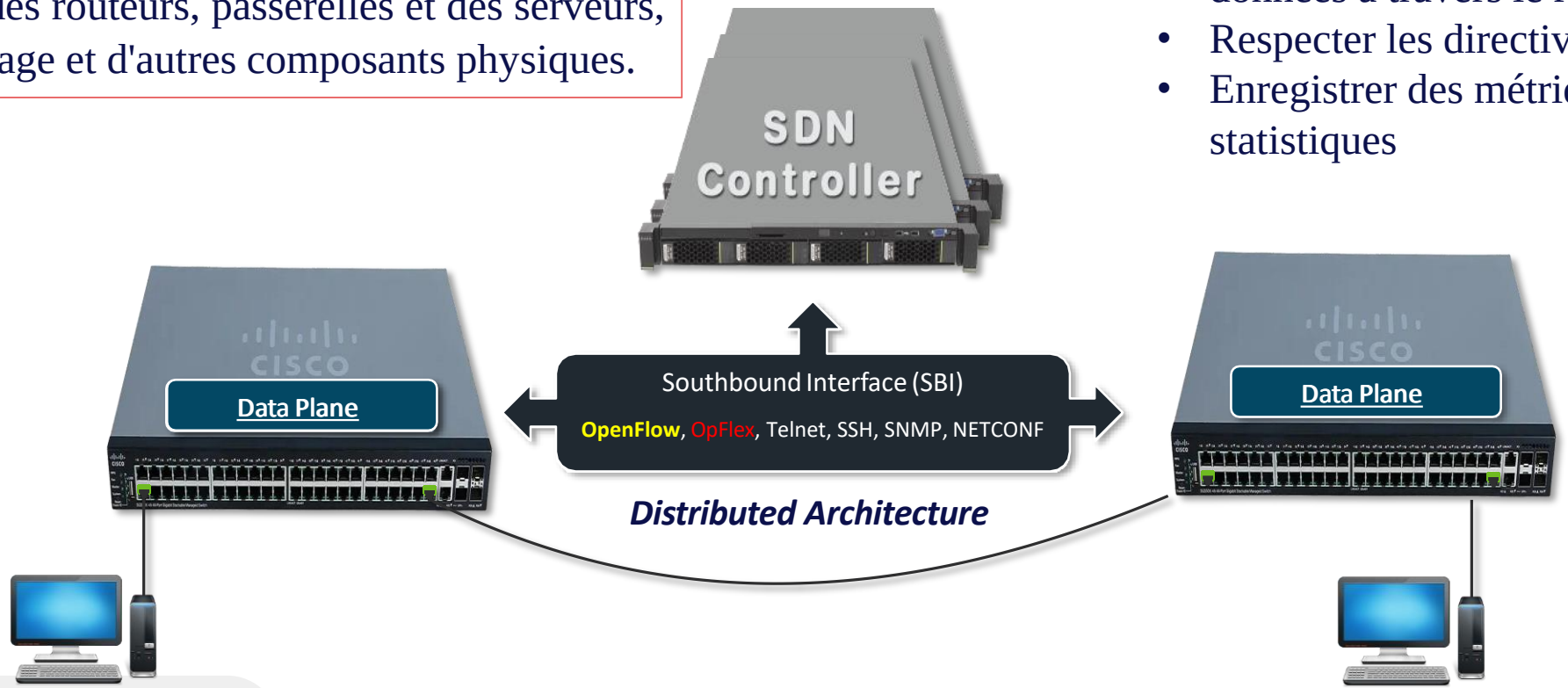


L'Architecture de SDN

③ Data Plane

Data Plane dans (SDN) est constituée des équipements physiques de l'infrastructure réseau comme commutateurs, des routeurs, passerelles et des serveurs, ainsi que le câblage et d'autres composants physiques.

- Le rôle de Data plane :
  - Gérer le transfert réel des paquets de données à travers le réseau
  - Respecter les directives du Controller
  - Enregistrer des métriques et statistiques



L'Architecture de SDN

1 Management Plane:

- Il assure l'enregistrement, la configuration initiale et l'inventaire des équipements réseau
- Il collecte et stocke des statistiques de performance (bande passante, taux de perte de paquets, temps de latence)
- Il gère le déploiement des mises à jour logicielles et des correctifs de sécurité sur les équipements réseau
- Il gère les comptes des utilisateurs et leurs droits d'accès
- Il fournit des fonctions de reporting, de journalisation, et d'audit pour assurer la conformité aux réglementations et politiques internes.

2 Control Plane:

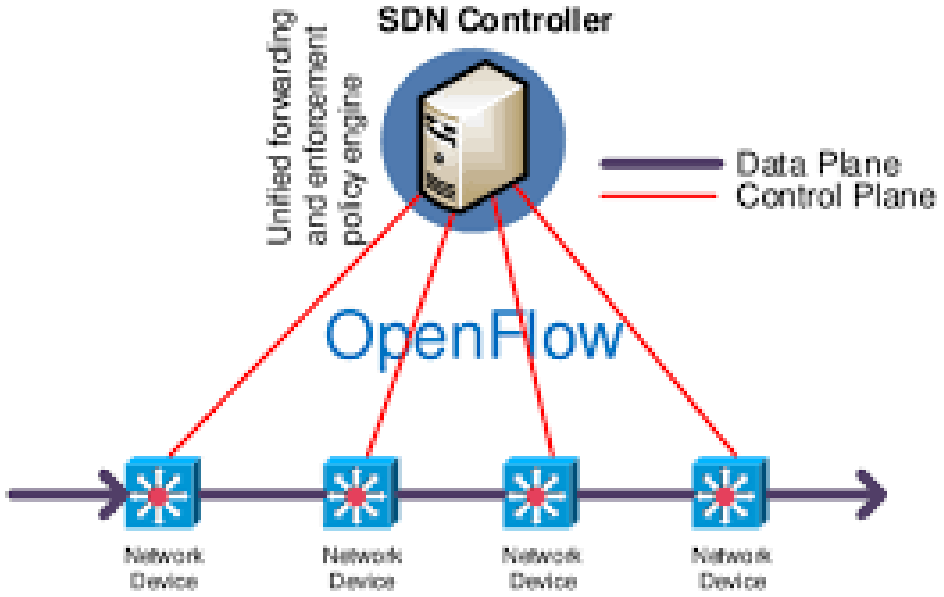
- Responsable de la prise de décisions en matière de routage et de commutation.
- Permet la configuration, la surveillance et la gestion des périphériques réseau

3 Data Plane (Forwarding Plane):

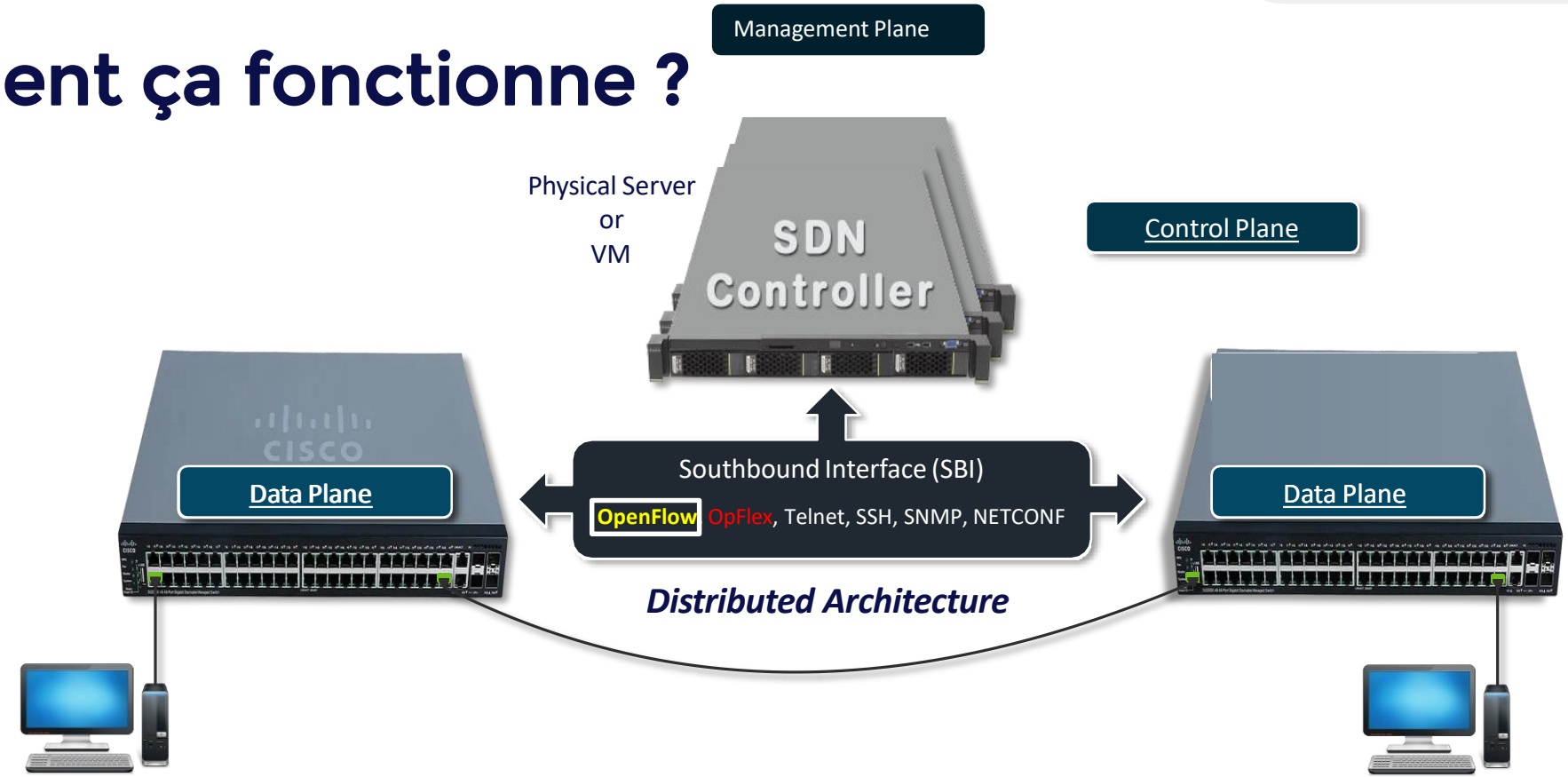
- Utilisé pour acheminer les données entre les périphériques.

OpenFlow

- Un périphérique communique avec le contrôleur SDN grâce à openflow .
- OpenFlow est un protocole clé pour les réseaux définis par logiciel (SDN) qui permet aux contrôleurs SDN de gérer directement les équipements réseau (comme les commutateurs et routeurs).
- C'est un standard défini par l'Open Network Foundation (ONF)
- Les instructions fournies par le contrôleur peuvent être exécutées sur n'importe quel équipements propriétaires (routeur, passerelle, etc).



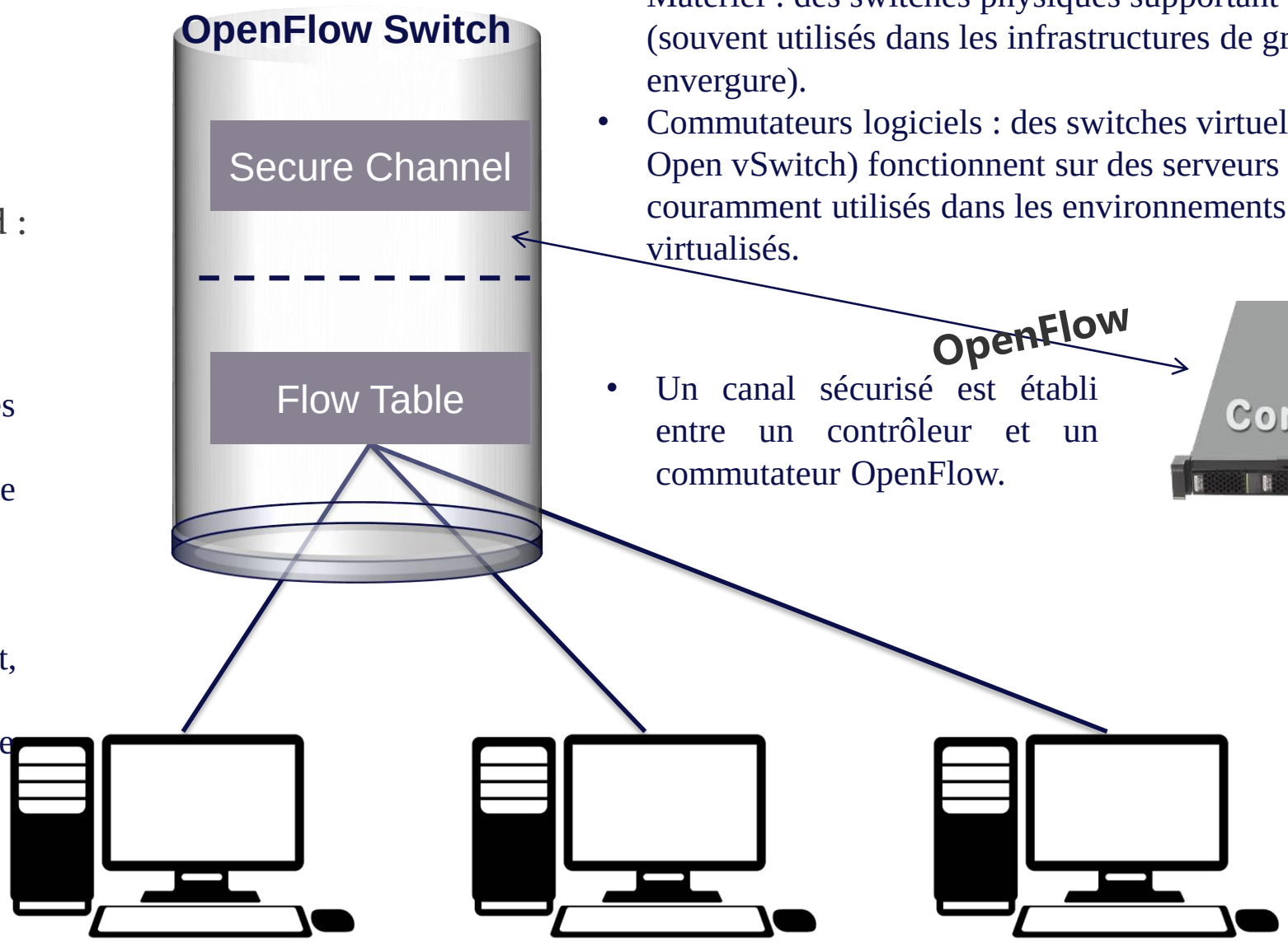
Comment ça fonctionne ?



- Un paquet entre dans le switch.
- Le switch cherche une correspondance dans sa **table de flux** (ou Flow Tables),
  - Si une correspondance est trouvée : le switch applique l'action spécifiée (par exemple, transférer vers un port spécifique).
  - Si aucune correspondance n'est trouvée : le switch interroge le contrôleur SDN pour obtenir les règles relatives à la gestion des paquets grâce à openflow
- le contrôleur SDN décide de la manière dont les paquets de données doivent être acheminés dans le réseau en utilisant des tables de flux.

Fonctionnement d'OpenFlow

- Chaque table de flux contient des règles précises qui indiquent aux appareils comment traiter certains types de paquets.
- Une règle de table de flux comprend :
  - **•Des critères de correspondance** : Comme l'adresse source ou de destination, le protocole, ou les ports. Ces critères permettent d'identifier des paquets spécifiques.
  - **•Une action à exécuter** : Une fois que le paquet correspond aux critères, le commutateur applique l'action indiquée (transférer le paquet, le bloquer, le rediriger vers un autre port, etc.).
  - •des statistiques (comme le nombre de paquets et d'octets traités).



OpenFlow Switch: on a deux types :Commutateurs matériels ou virtuel

- Matériel : des switches physiques supportant OpenFlow (souvent utilisés dans les infrastructures de grande envergure).
- Commutateurs logiciels : des switches virtuels (comme Open vSwitch) fonctionnent sur des serveurs et sont couramment utilisés dans les environnements cloud et virtualisés.

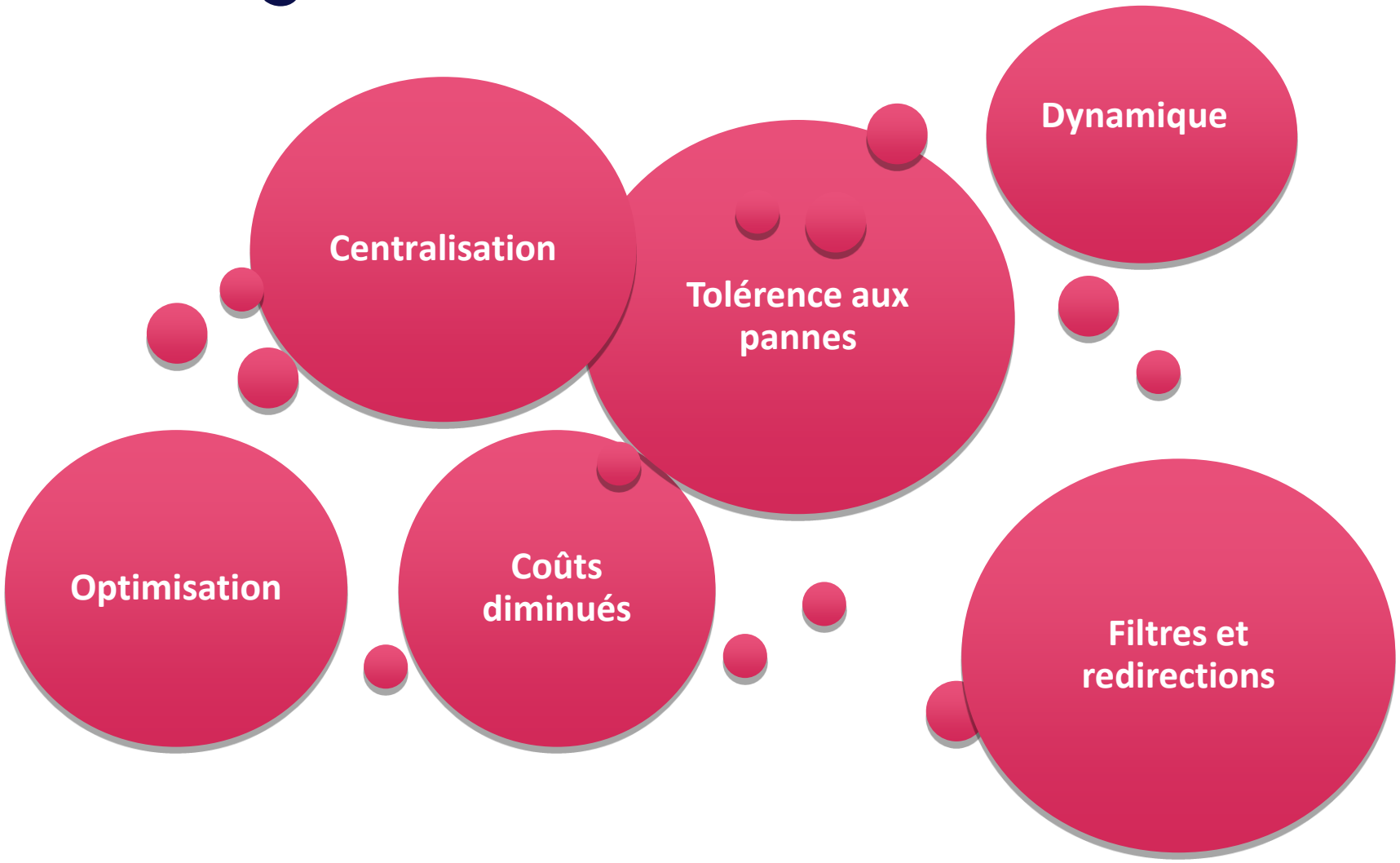
OpenFlow

- Un canal sécurisé est établi entre un contrôleur et un commutateur OpenFlow.

Software-Defined Networking

- Grâce au SDN, l'administrateur réseau peut réaliser certaines opération facilement indépendamment des périphériques qui vont les appliquer:
  - Modifier les règles de routage
  - filtrage, redirection
  - Changer les priorités des paquets,
  - bloquer certains types spécifiques de paquets
  - définir les politiques de sécurité
  - Gérer le QoS (Qualité de Service), bande passante, etc.
  - améliorer l'efficacité du réseau…
- L'idée est de rendre le réseau programmable en permettant aux administrateurs réseau de contrôler et de configurer le réseau de manière dynamique et centralisée.

Avantages et benefices de SDN



Avantages et benefices de SDN

La centralisation de la partie logiciel de tout le réseau dans le controleur

Dynamique et Agile : Les SDN permettent de centraliser le contrôle du réseau, ce qui facilite la modification des règles de routage et des politiques de sécurité en temps réel (en ajoutant, supprimant ou modifiant les règles de manière dynamique).

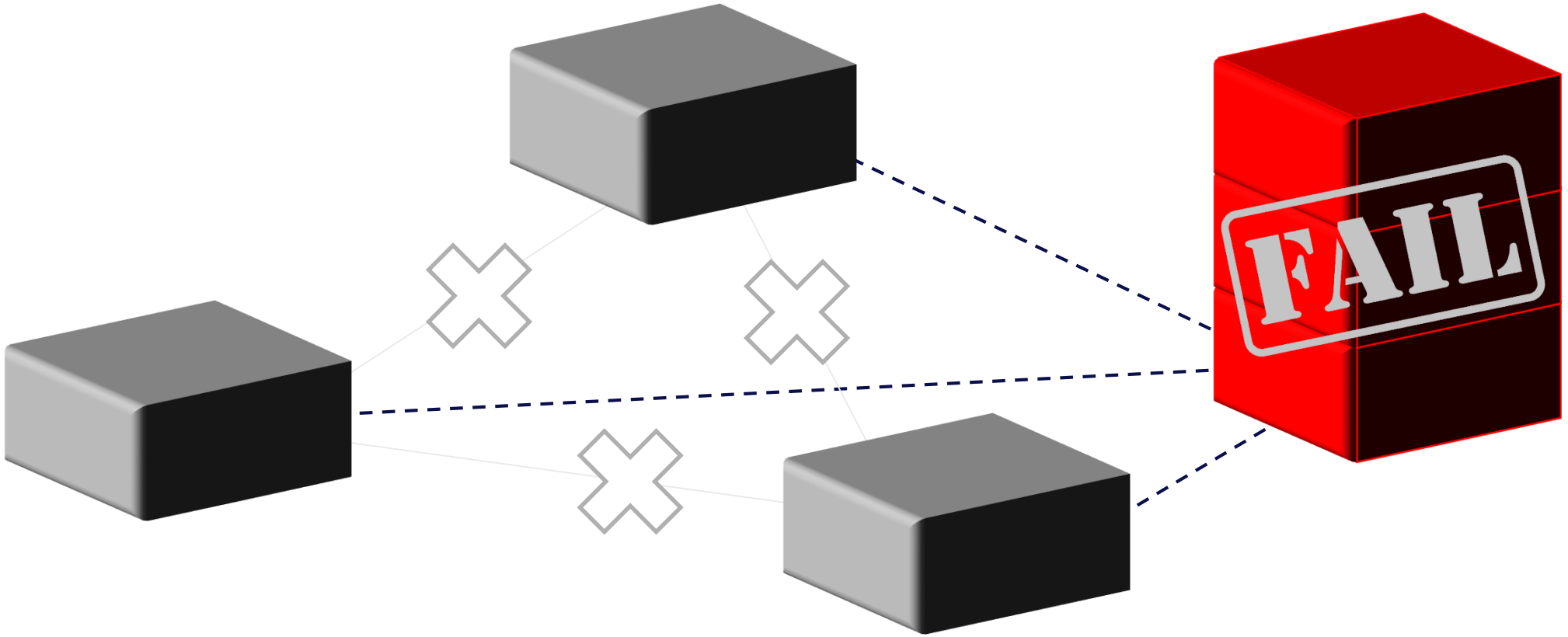
Coûts diminués : En dissociant le Control Plane du Data Plane, les SDN permettent de réduire la complexité et le coût des équipements réseau (on peut utliser des équipement moins cher et peu performants)

Optimisation: Les SDN permettent d'optimiser les chemins de trafic en temps réel, ce qui peut réduire la latence et améliorer l'efficacité des applications sensibles au temps de réponse

Filtres et redirections : on peut définir à travers le formalisme SDN différent fonctionnalités réseaux telles que les filtres ou les redirections

Tolérance aux pannes : Pour cela des configurations de contrôleurs répliqués ou redondants sont souvent mises en place. plusieurs contrôleurs sont déployés pour prendre le relais en cas de défaillance, permettent de minimiser l'impact d'une panne du contrôleur principal.

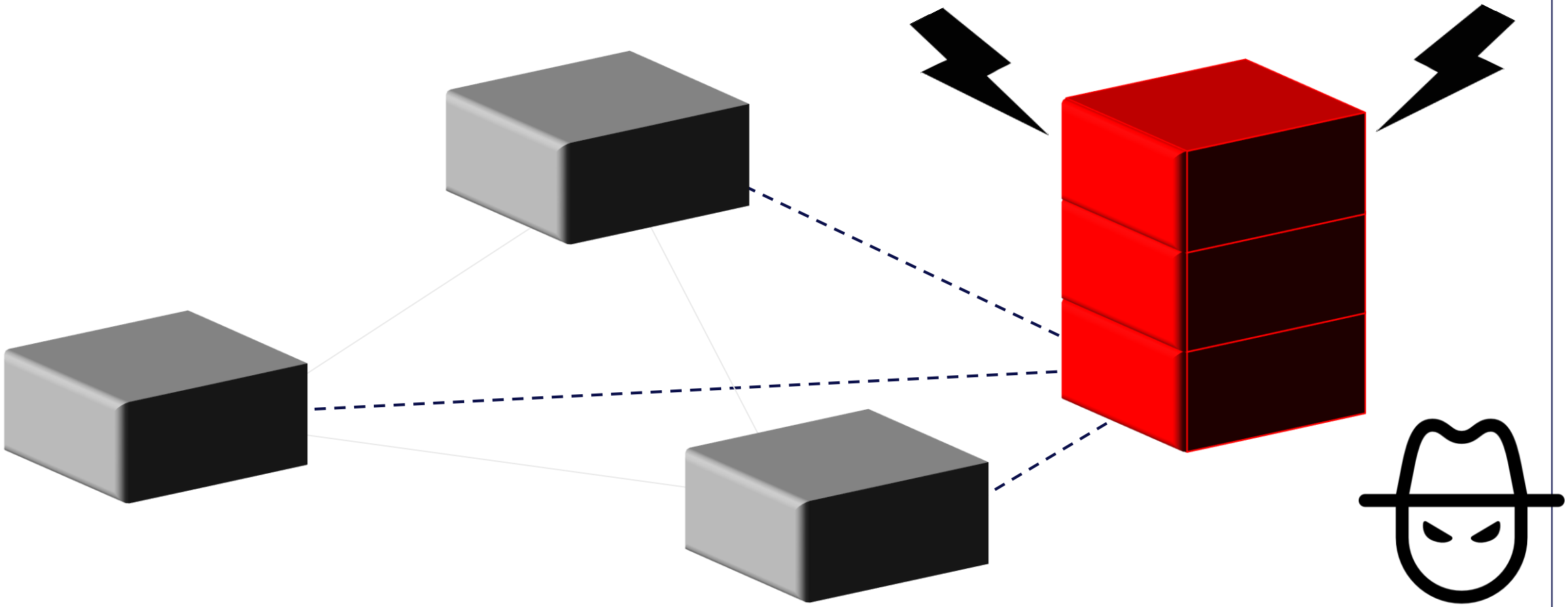
Limites de SDN



1 Point de panne central (Single Point of Failure)

- En cas de défaillance du contrôleur SDN, le réseau peut devenir instable ou même indisponible.
- Bien que des solutions de redondance soient souvent mises en place, ces configurations peuvent être coûteuses et complexes à gérer.

Limites de SDN



2 Point d'attaque unique (Single point of attack)

- Centraliser le contrôle du réseau dans un contrôleur SDN peut introduire un point unique de vulnérabilité.
- Si le contrôleur est compromis, l'ensemble du réseau peut être affecté.

Mininet

- Mininet est un logiciel open source qui permet de créer des réseaux virtuels complets sur un seul ordinateur, en émulant des hôtes (machines virtuelles légères), des commutateurs, des contrôleurs SDN, et des liens réseau.
- Il utilise des technologies de virtualisation au niveau du noyau, comme les namespaces de réseau de Linux, pour isoler les hôtes et les liens, ce qui rend l'émulation efficace en termes de ressources.
- Mininet est compatible avec divers contrôleurs SDN comme OpenDaylight, Ryu, ONOS et POX, permettant de tester différentes architectures SDN et de simuler leur fonctionnement avec des commutateurs OpenFlow.
- Le contrôleur SDN peut être exécuté localeme
interagit avec les switches et hôtes virtuels via

http://mininet.org/download/

Network Function Virtualization : NFV

Les fournisseur réseau fournissent une connectivité de réseau pour les entreprises

Network Function Virtualization : NFV

- Souvent les fonctionnalités réseaux sont déployées sur des équipements propriétaires dans les locaux des clients.
- Elles englobent des fonctionnalité comme :
  - **Serveur NAT** pour la translation des adresses
  - **VPN** (Virtual Private Network)
  - Analyse profonde des paquets (**DPI-Deep Packet Inspection**)
  - Serveur de mise en cache pour distribuer le contenu à proximité des utilisateurs finaux : **(CDN-Content Delivery Network**)
  - **Serveur DNS** permettent de gérer la résolution de noms pour les ressources internes
  - Serveur d'accès à large bande utilisé par les fournisseurs d'accès Internet pour gérer les connexions à large bande des utilisateurs finaux (BRAS - Broadband Remote Access Server))
  - Fonction support du GPRS pour la transmission mobile :**SGSN** -Serving GPRS Support Node et **GGSN** -Gateway GPRS Support Node)) ,
  - Routeur frontière qui qui sert de point d'interconnexion entre le réseau du fournisseur et les réseaux des clients ou d'autres opérateurs(**Provider Edge Router -PE Route**r)
  - **WAN Accelerator** est un dispositif matériel ou logiciel conçu pour optimiser et accélérer les performances du réseau étendu
  - etc.

Fonctionnalités réseaux

Network Function Virtualization : NFV

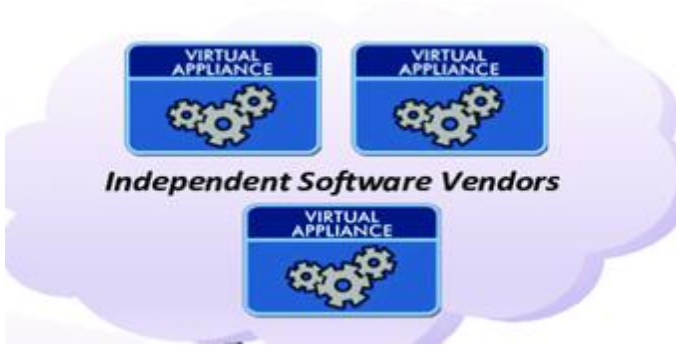
- Plusieurs équipements réseaux propriétaires déployés dans les locaux des clients
- Chaque équipement est conçu pour exécuter une fonction spécifique et ne peut pas être facilement reconfiguré pour effectuer une autre tâche.
- Cela peut être coûteux en termes d'investissement initial et de coûts de maintenance
- Si on a besoin d'une nouvelle fonction dans un équipement , il faut déplacer les techniciens sur place

- Les fournisseurs de service ont commencé à chercher des solutions pour réduire les coûts, et accélérer le déploiement

Vitualisation des Fonctions Réseau (NFV)

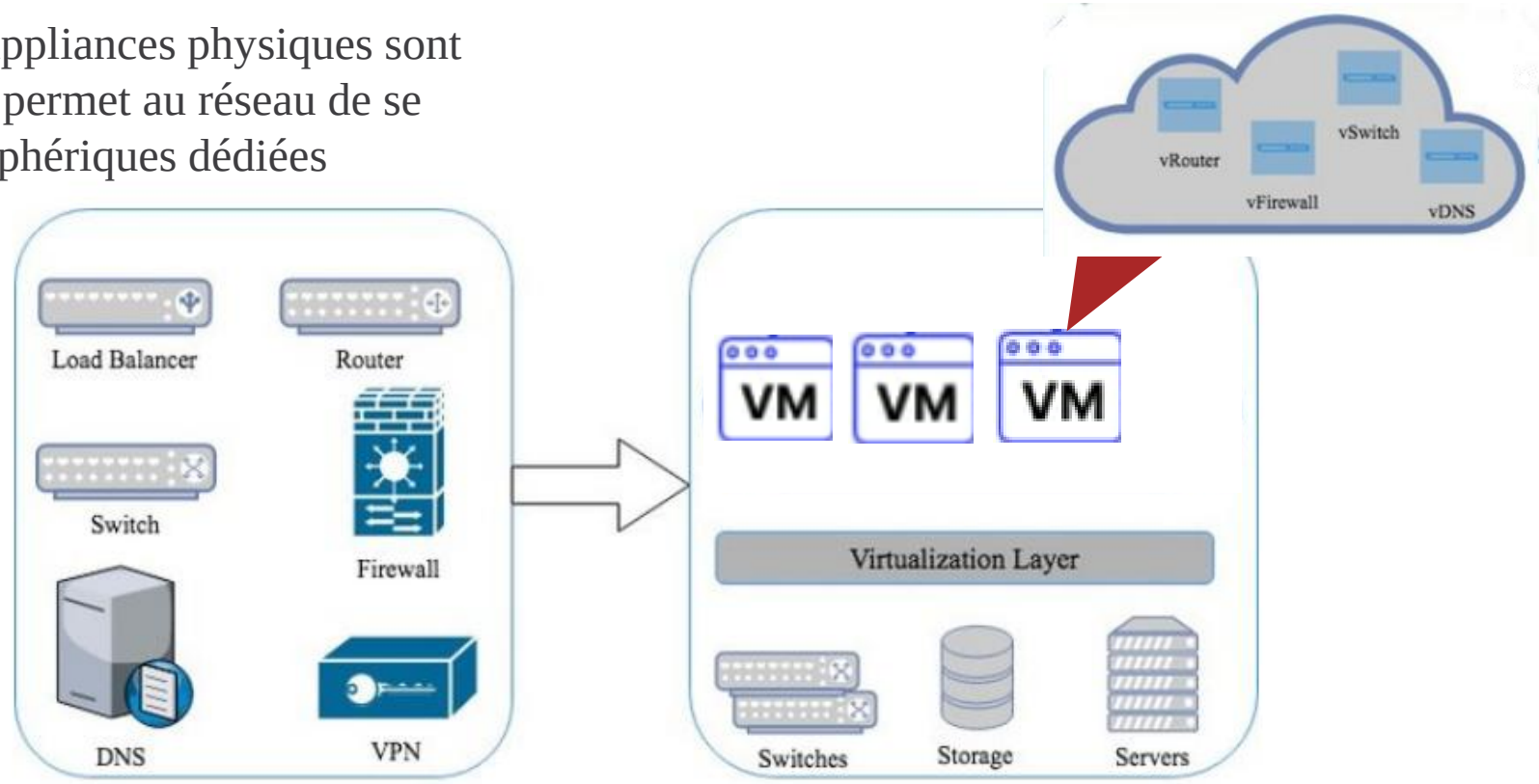
Network Function Virtualization : NFV

- A l'origine de ce concept sont les opérateurs Telecom, ensuite standardisé par l'ISG (Industry Specification Group) de l'ETSI (European Telecommunicatons Standards Institute)
- Le principe du NFV consiste à virtualiser les services réseaux pour les abstraire du matériel dédié en les transférant vers des serveurs virtuels.
- Cela consiste à remplacer des équipements de réseau propriétaires et spécialisés, tels que des routeurs, des pare-feu et des commutateurs, par des logiciels virtualisés s'exécutant sur des serveurs standardisés et des infrastructures cloud.



Network Function Virtualization

Les fonctions réseaux basées sur des appliances physiques sont virtualisées via un hyperviseur, ce qui permet au réseau de se développer sans devoir ajouter de périphériques dédiées



Approche traditionnelle **Approche NFV**

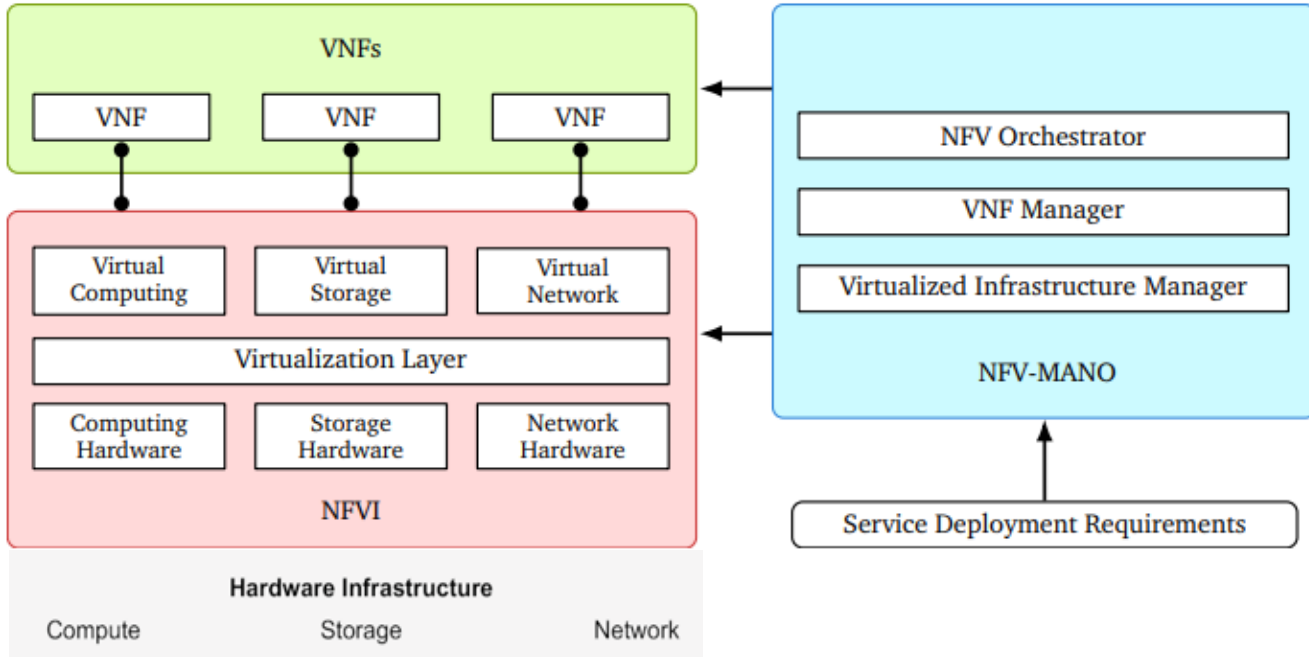
Les serveurs standard COTS

- Les serveurs COTS sont des serveurs standard, prêts à l'emploi, qui peuvent être achetés auprès de différents fournisseurs.
- Ils sont beaucoup moins chers que les équipements réseaux propriétaires.
- Ils sont conçus pour exécuter diverses tâches, et s'adaptent aux exigences spécifiques des différentes applications NFV.
- Cela permet de réunir plusieurs fonctions sur un seul serveur physique, ce qui réduit les coûts et le nombre d'interventions sur le terrain au minimum.
- Les serveurs COTS peuvent être optimisés en utilisant la virtualisation des serveurs, chacun exécutant une fonction spécifique.

ETSI NFV architecture framework

- Les **VNFs** (Virtual Network Functions) remplacent les fonctions des nœuds réseau physiques
- **NFVI** fournit les ressources virtuelles nécessaires pour supporter l'exécution des VNFs (capacité réseau, la puissance de calcul, l'espace mémoire)
- Le **VIM** contrôle et gère les ressources (calcul, stockage et réseau) de la NFVI au sein de l'infrastructure d'un opérateur en maintenant un inventaire de l'allocation des ressources virtuelle aux ressources physiques.
- **VNF Manager** (VNFM) gère le cycle de vie des VNFs (création et allocation des VMs, mise à jour, mise à l'echelle, fin, etc,).
- **Le NFV Orchestrator** (NFVO) garantit qu'une VNF reçoit, une quantité adéquate de ressources de calcul, de stockage et de réseau de la NFVI.

MANO (*Management and orchestration*)



Network Function Virtualization : NFV

- Avantages:
  - Abstraction des d'équipements matériels propriétaires et dédiés.
  - Réduire les coûts
  - Déployer plus rapidement de nouveaux services réseau
  - Mise à l'échelle en fonction des besoins des utilisateurs
  - Offrir une meilleure qualité de service
  - Une sécurité accrue,
  - Sans que le hardware soit une contrainte limitante.

SDN VS NFV

- NFV se concentre sur la virtualisation des fonctions réseau.
- NFV permet de rendre les fonctions réseau plus flexibles et évolutives en les virtualisant.
- En virtualisant ces fonctions, elles peuvent être déployées et adaptées facilement en fonction des besoins.
- Abstraction des d'équipements matériels propriétaires et dédiés.

VS

- SDN se concentre sur la centralisation de la gestion et du contrôle du réseau.
- SDN vise à rendre la gestion du réseau plus efficace et automatisée en séparant le plan de contrôle du plan de données
- Les administrateurs réseau peuvent gérer et configurer les dispositifs réseau de manière centralisée.

NFV et SDN sont des technologies différentes mais peuvent être combinées