Software-Defined Networking, Network Function Virtualization et Network Slicing

Loïc Desgeorges - Thomas Begin

Université Claude Bernard Lyon 1 / Laboratoire LIP

loic.desgeorges@univ-lyon1.fr

Sources de ce cours

- Ces transparents sont basés sur :
  - Des supports de cours de Jennifer Rexford (Professor at Princeton) http://www.cs.princeton.edu/courses/archive/spr12/cos461/
  - De la présentation "*Making SDN Work*" de Nick McKeown au sommet *Open Networking* en Avril 2012
  - *SDN & NFV. OpenFlow and ForCES. IETF-93,* de Yaakov Stein, Evangelos Haleplidis.
  - D. Lopez Telefonica I+D, NFV
  - *Tutorial 2 :: Network Functions Virtualization NFV - Perspectives, Reality and Challenges* de Cesar Marcondes et Christian Esteve Rothenberg, 2015
  - Des supports de cours de Francesco Bronzino (Ass. Prof. at ENS Lyon)
- Pour en savoir plus :
  - *OpenFlow: Enabling Innovation in Campus Networks.* McKeown et al., 2008.
  - *The Road to SDN: An Intellectual History of Programmable Networks.* Feamster, Rexford and Zegura, 2014.
  - *Network Functions Virtualization for Dummies,* de Balamurali Thekkedath, Willey Brand. *https://h20195.www2.hpe.com/V2/getpdf.aspx/4AA6-6386ENW.pdf*
  - *Specification OpenFlow : https://opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.3.0.pdf*

Plan

1. Introduction
2. Plan de contrôle & Plan de données
3. SDN
4. OpenFlow et P4
5. Applications SDN
6. NFV
7. Network slicing
8. Défis restants

Internet : un énorme succès

- Initialement une plateforme expérimentale
  - Projet ARPANET (1967-1972)
  - Entre 4 sites aux US
- Devenu une infrastructure de communication
  - multi-usage
    - Web, P2P, VoIP, réseaux sociaux, jeux en-ligne, e-commerce, impôt…
    - Convergence des réseaux
  - dimension planétaire
    - 3.6 milliards d'utilisateurs (2017)
    - 20 à 50 milliards de noeuds (2017)

Des fortes innovations en périphérie

- Terminaux
  - Plus hétérogènes (sans fil, mobiles, capteurs…), nombreux, puissants, petits …
- Applications
  - Web (forums, presse, wiki, e-commerce, e-learning…), courrier électronique, VoIP, streaming, VoD, réseaux sociaux, e-gaming,…
- Cloud computing
  - Synchronisation des données depuis partout
  - Accès à des ressources depuis partout (datacenters)
- Internet of Things (IoT)
  - Capteurs, objets connectés (télé, enceinte, thermostat…)
  - Industrie du futur, domotique, télémétrie, surveillance…
  - Technologies réseaux d'accès : LoRa, Sigfox, BLE, Li-Fi…

 Ces innovations concernent la périphérie de réseaux

… mais peu dans les coeurs de réseau

- Des progrès quantitatifs
  - Ex : Capacité des réseaux optiques Mbps → Tbps
- Une complexification des architectures
  - Proxy,…
- Mais assez peu d'innovations de ruptures
  - Encore en commutation de paquets
    - Même si MPLS (~2000)
  - Encore des algorithmes de routage dynamique (OSPF, BGP)
    - Pas de routage QoS
  - Toujours pas (ou très peu) d'ingénierie de traffic
    - Pas d'optimisation d'un réseau en analysant son trafic

Gestion complexe des réseaux

- Dimension gigantesque
  - En taille et nombre de noeuds
- Hétérogénéité des équipements
  - Inter-opérabilité entre équipementiers différents
  - Bugs/incompatibilités dans les logiciels
    - Jusqu'à 20 millions de lignes de code pour certains routeurs
  - Interfaces de contrôles propriétaires et donc différentes
- Algorithmes/protocoles distribués
  - Difficile d'anticiper ou de forcer des décisions (Ingénierie de trafic)
- Middleboxes
  - Boîtes noires (fermés et propriétaires)
- Erreurs commises par les opérateurs
  - Configuration des équipements

Coût élevé de déploiement et d'exploitation

- Un marché trop étroit
  - Nombre limité d'équipementiers
  - Environ une dizaine d'acteurs
- Equipements peu modulaires et évolutifs
  - Fermés
  - Logiciels livrés avec le hardware
  - Code source fermé et propriétaire

3 défis pour les coeurs de réseau

- Au début des années 2000, des chercheurs jugent urgent de
  - Lever les freins à l'innovation
  - Simplifier la gestion des réseaux
  - Baisser leurs coûts
- Et proposent comme réponse à ces 3 défis
  - Le SDN, le NFV et le network slicing

Feamster, N., Rexford, J., & Zegura, E. (2014). The road to SDN: an intellectual history of programmable networks. *ACM SIGCOMM Computer Communication Review*, 44(2), 87-98.

3 défis pour les coeurs de réseau

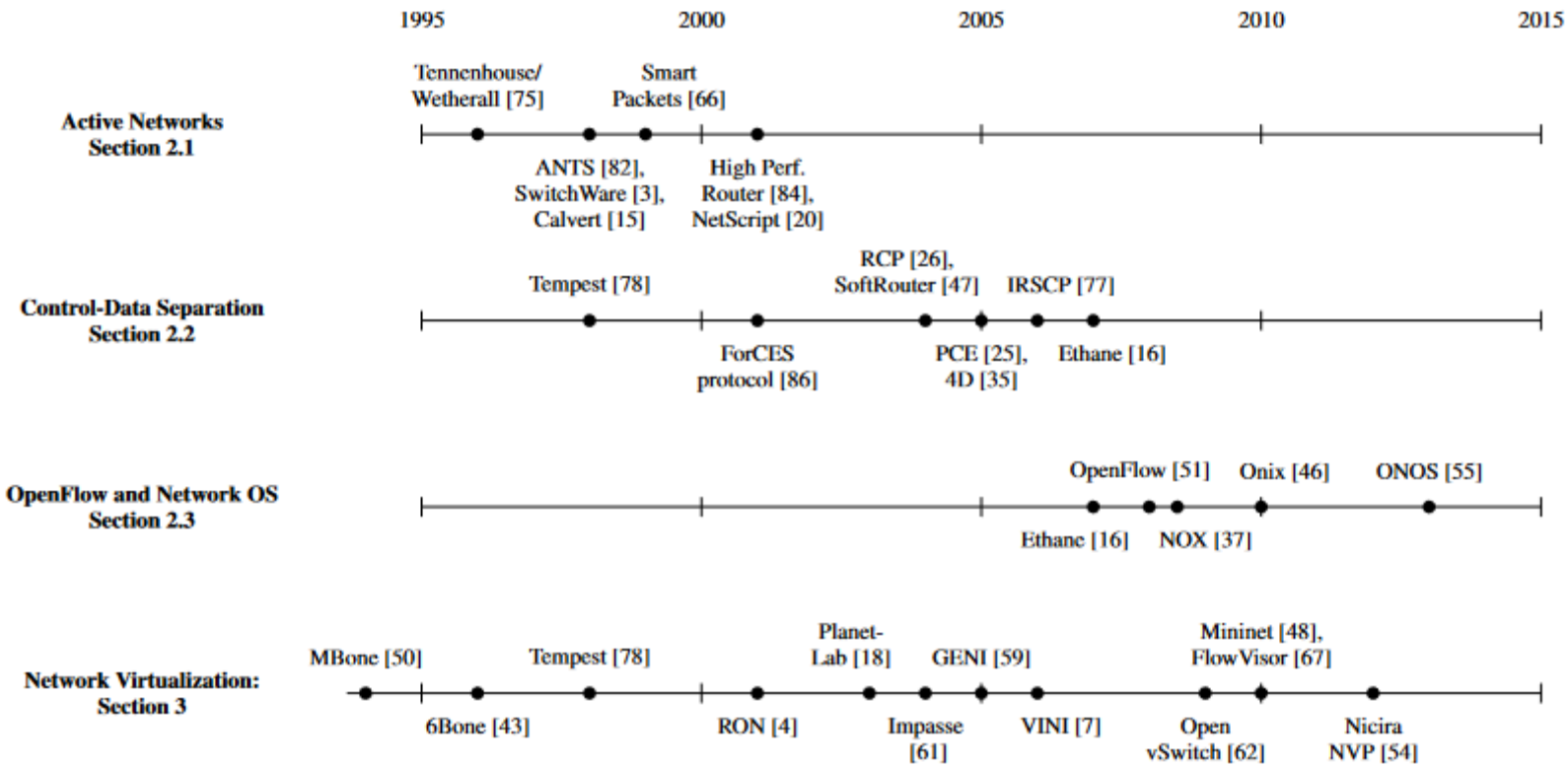


Figure 1: Selected developments in programmable networking over the past 20 years, and their chronological relationship to advances in network virtualization (one of the first successful SDN use cases).

Feamster, N., Rexford, J., & Zegura, E. (2014). The road to SDN: an intellectual history of programmable networks. *ACM SIGCOMM Computer Communication Review*, 44(2), 87-98.

Plan

1. Introduction
2. Plan de contrôle & Plan de données
3. SDN
4. OpenFlow et P4
5. Applications SDN
6. NFV
7. Network slicing
8. Défis restants

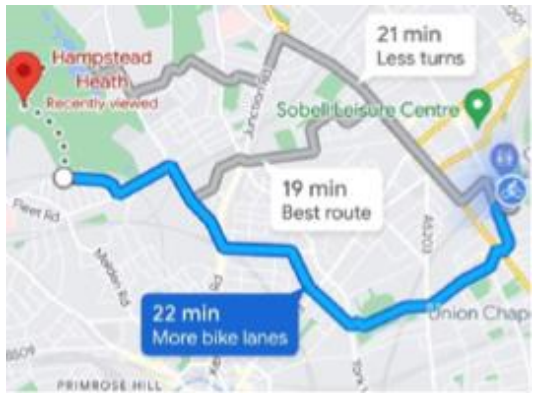
Plan de données & plan de contrôle

- Paquets de données
  - Transporte les données des applications
- Paquets de contrôle
  - Pour le fonctionnement du réseau
- Paquets de gestion
  - Généré par l'administrateur
- Plan de données
  - Achemine, filtre et modifie les paquets
- Plan de contrôle
  - Décide comment acheminer les paquets (calcul des routes, surveillance de la topologie, configuration automatique des équipements réseaux)
- *Le plan de données achemine les paquets selon les règles du plan de contrôle*

Plan de gestion

- Plan de gestion
  - Décide de politiques (QoS, ACL)
    - Analyse les mesures
    - Configure manuellement les équipements réseaux
    - Fixe le poids des liens
    - Ingénierie de trafic
- *Le plan de gestion agit sur le plan de contrôle par l'intervention de l'admin*

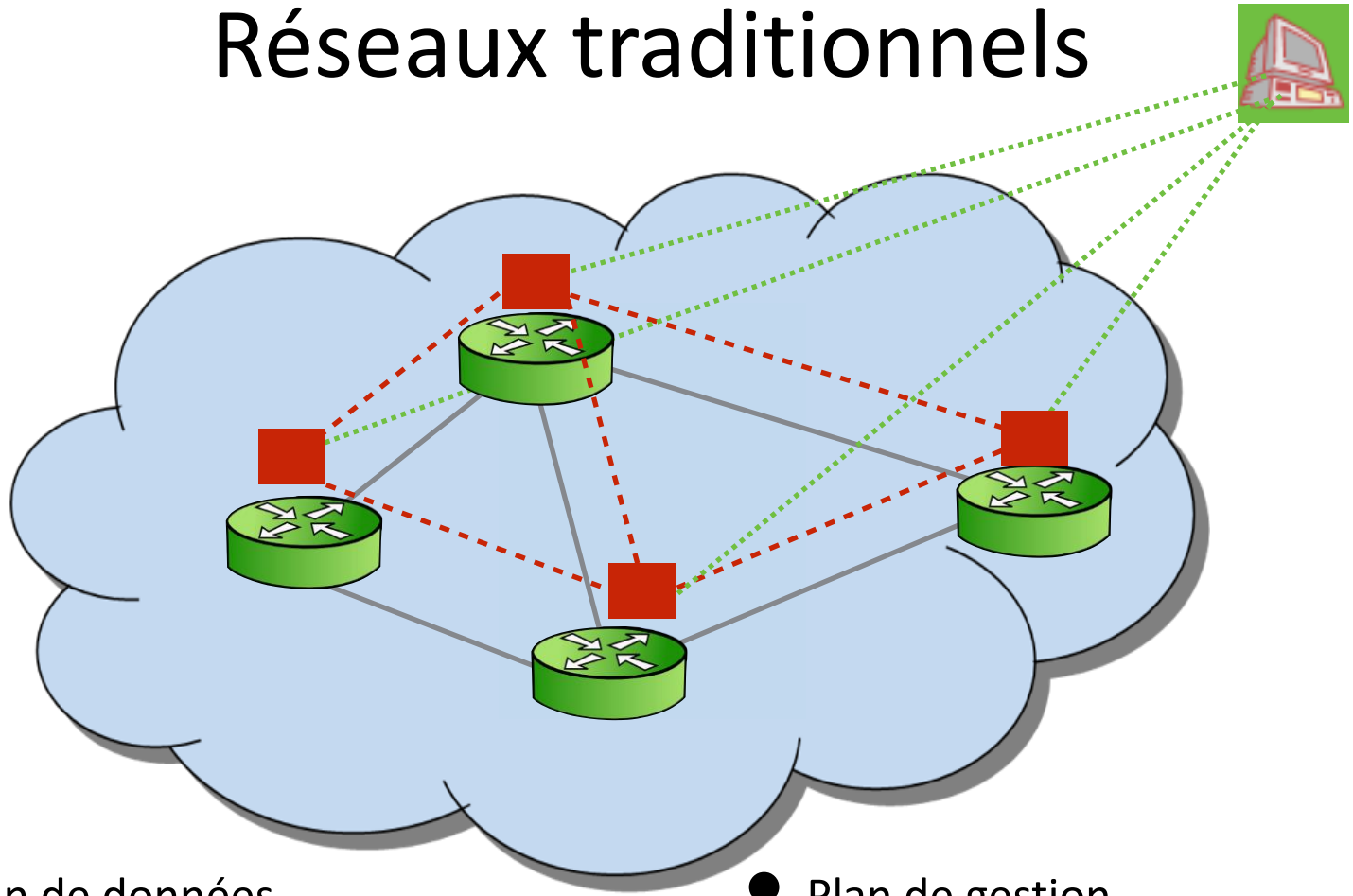
Plan de données



Plan de contrôle

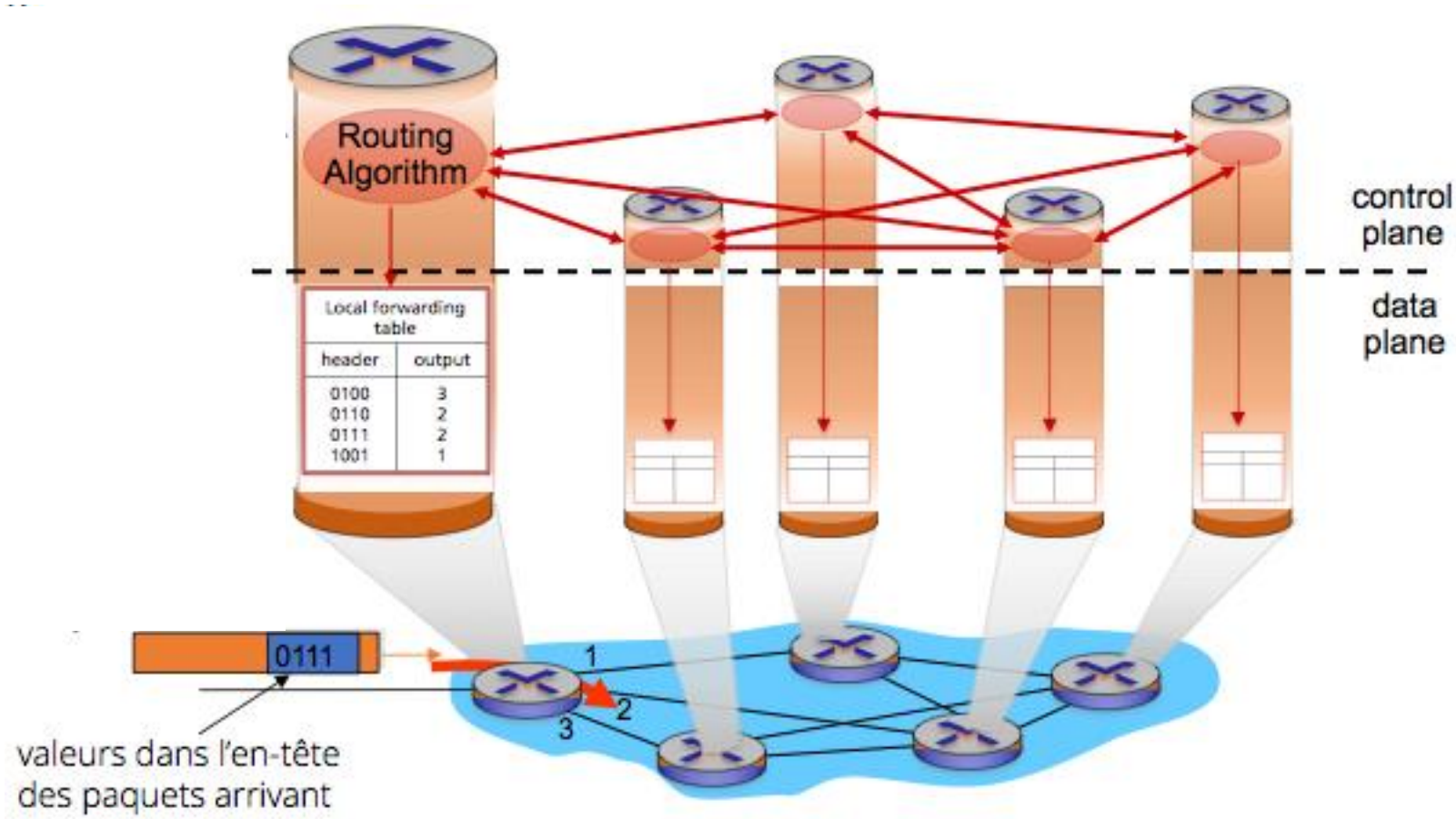
Plan de gestion

Réseaux traditionnels



- Plan de données
  - Distribué ou ~~Centralisé~~ sur les noeuds ?
- Plan de contrôle
  - Distribué ou ~~Centralisé~~ sur les noeuds ?
- Plan de gestion
  - ~~Distribué ou~~ Centralisé sur les noeuds ?
- À quel plan appartiennent les routeurs ? Et les commutateurs ?

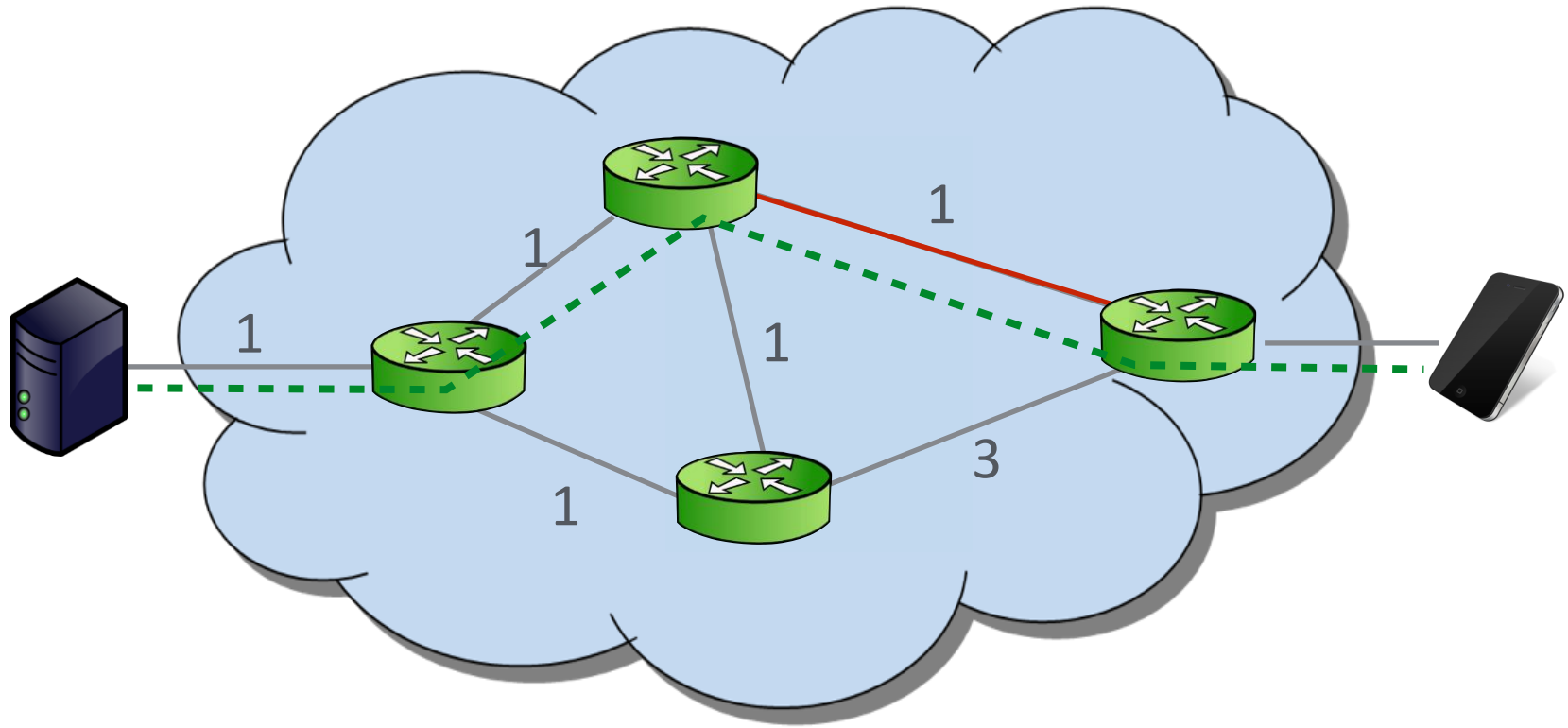
Plan de données & plan de contrôle



Le plan de contrôle

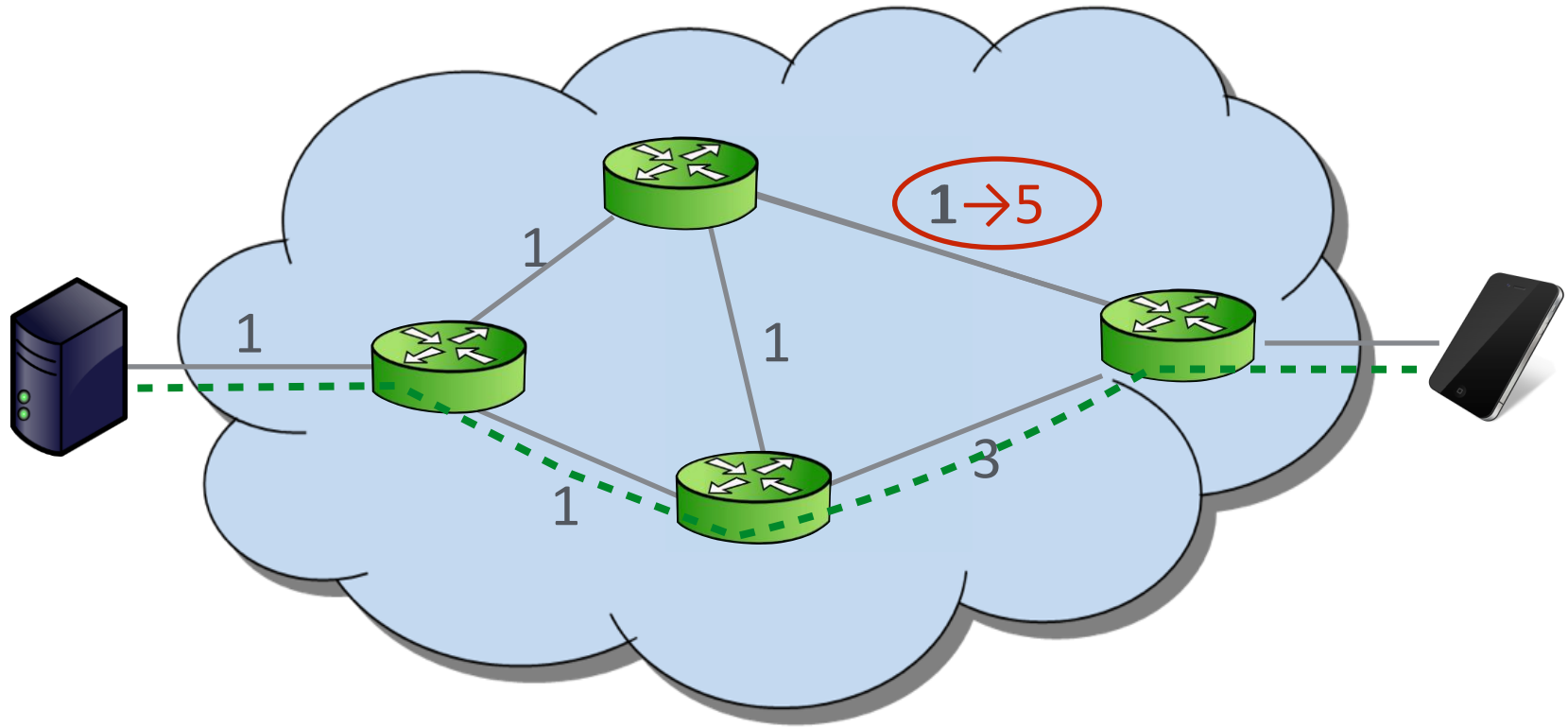
- Souvent mis en oeuvre par des algorithmes distribués
- Avantage
  - Robustesse et tolérance aux pannes
- Inconvénients
  - Nécessite un niveau élevé d'inter-opérabilité entre les équipements réseaux
  - Complexe de "forcer" des opérations du plan de contrôle

Exemple d'ingénierie de trafic (1)



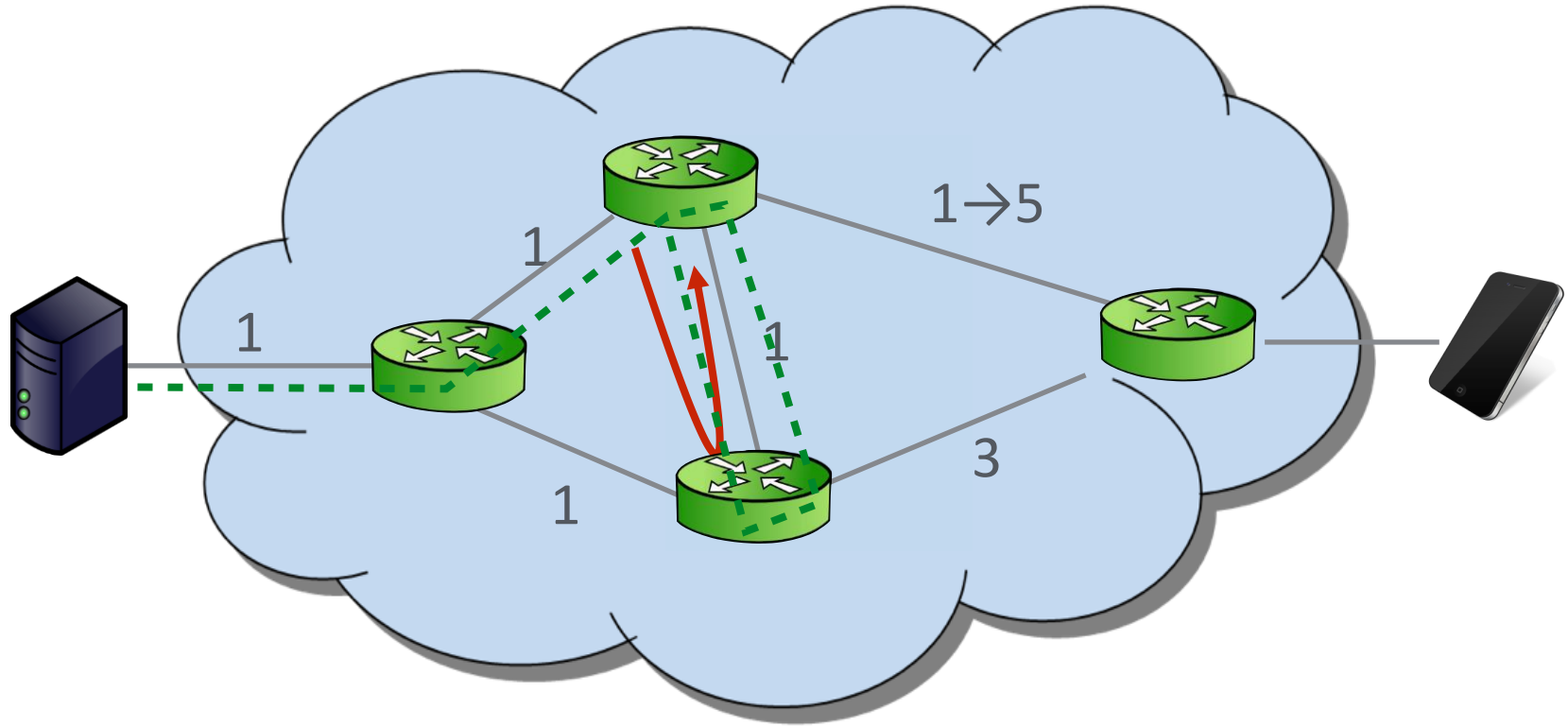
- Action de l'administrateur sur le plan de contrôle
  - pour forcer un changement
- Scénario
  - Le lien Nord-Est sature
  - Comment re-router le trafic pour éviter la congestion ?

Exemple d'ingénierie de trafic (2)



- L'administrateur augmente "manuellement" le poids du lien Nord-Est
  - Ce qui agira sur le routage dynamique
  - Et re-routera le trafic par le sud
- Ça fonctionne mais …

Exemple d'ingénierie de trafic (3)



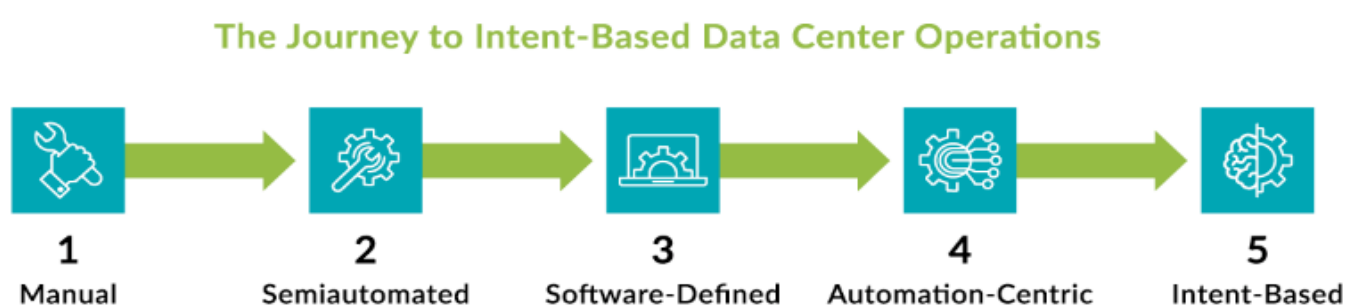
- Inconvénients
  - Non-automatique → lent et propice aux erreurs humaines
  - Complexe (pas sur cet exemple très simple)
  - Incohérence (temporaire) entre les noeuds → boucle de routage
- Peut on penser des réseaux sans plan de contrôle distribué ?
  - Avec un contrôle centralisé dans un contrôleur ?

Plan

1. Introduction
2. Plan de contrôle & Plan de données
3. SDN
4. OpenFlow et P4
5. Applications SDN
6. NFV
7. Network slicing
8. Défis restants

Software-Defined Networking

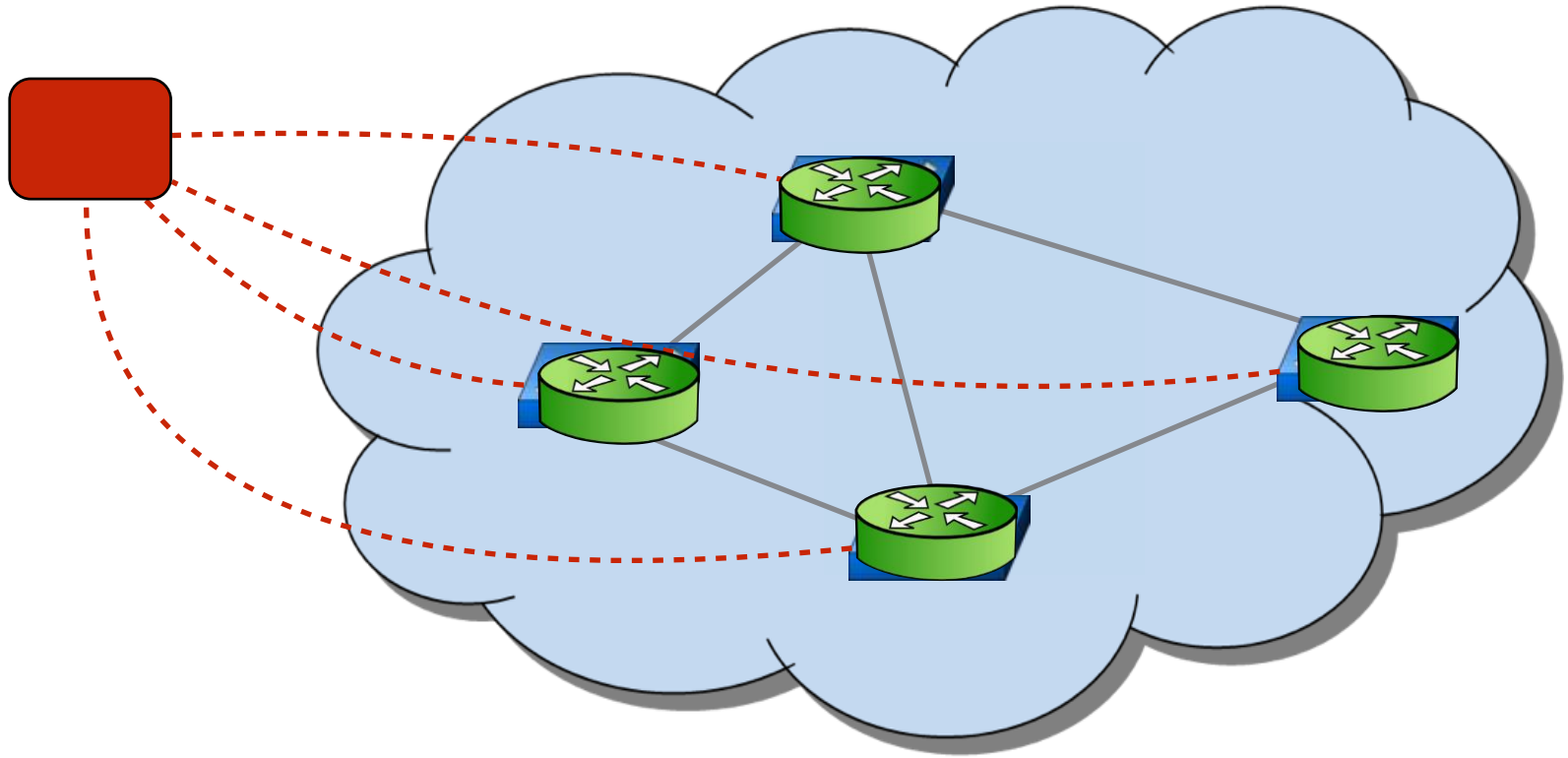
- Propriétés
  - Un plan de contrôle centralisé dans un ou plusieurs contrôleurs
  - Une interface ouverte et universelle pour programmer le plan de données
  - Des commutateurs plus simples remplacent les routeurs complexes
- Fin de l'algorithmie distribuée dans les réseaux mais
  - Réseaux agiles et programmables
  - Interface de contrôle simplifiée et universelle
  - Développement de chaînes de traitement des paquets
  - Vérification formelle de la politique d'un réseau (absence de boucles, conformité à un SLA, chemin sûrs…)
  - Intention déclarative : déclaration de politiques (exemple : accès à des services) et mise en oeuvre automatique (et non plus configuration individuelle des équipements)



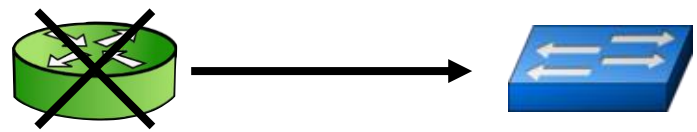
Source : https://www.juniper.net/us/en/research-topics/what-is-intent-based-networking.html

Software-Defined Networking

Contrôleur SDN



Contrôleur
- Intelligent
- Vue globale
- Décide de tout



Fin des routeurs (et du routage dynamique)

Commutateurs (de niveau 3)
- Simples et rapides
- Plan de données seulement
- Ne sont plus des routeurs

Routeurs et commutateurs

- Les routeurs des réseaux IP traditionnels ont 2 fonctions
  - Commutation
    - Lire l'en-tête des paquets
    - Consulter la table d'acheminement (routage)
    - Commuter le paquet

    Plan de données
  - Routage
    - Echanger avec les autres routeurs
    - Exécuter un protocole de routage
    - Remplir les tables d'acheminement

    Plan de contrôle
- Les commutateurs des réseaux SDN ont 1 seule fonction
  - Commutation
  - Mais ils sont programmables

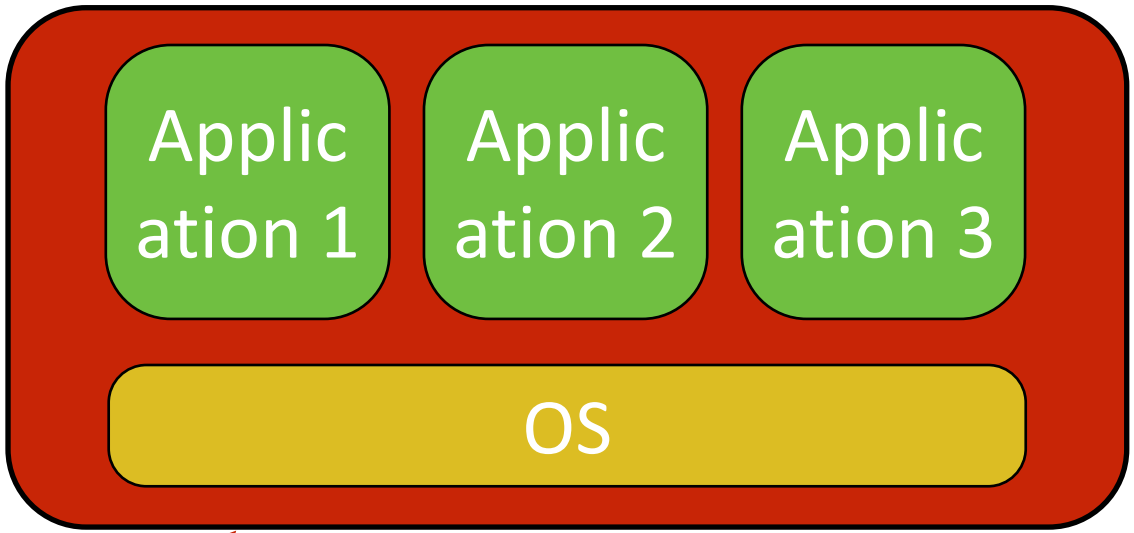
  Plan de données

Comment instruire les commutateurs SDN ?

- Mode Réactif
  - 1er paquet d'un flot : le comm. interroge le contrôleur
  - Le contrôleur décide et en informe les commutateurs concernés
    - Ajoute d'une nouvelle règle dans les tables d'acheminement
  - Réduit la taille des tables mais surcoût additionnel
- Mode Pro-actif
  - Le contrôleur pré-remplit les tables d'acheminement dans les commutateurs
  - Suppose des règles agrégées pour traiter tous les cas possibles
  - Mise à jour fréquente
- Souvent les 2 modes co-habitent
  - Ensemble de règles pré-établies + exceptions

Contrôleur SDN

Contrôleur SDN



Application monolithique remplacée par des modules spécialisés

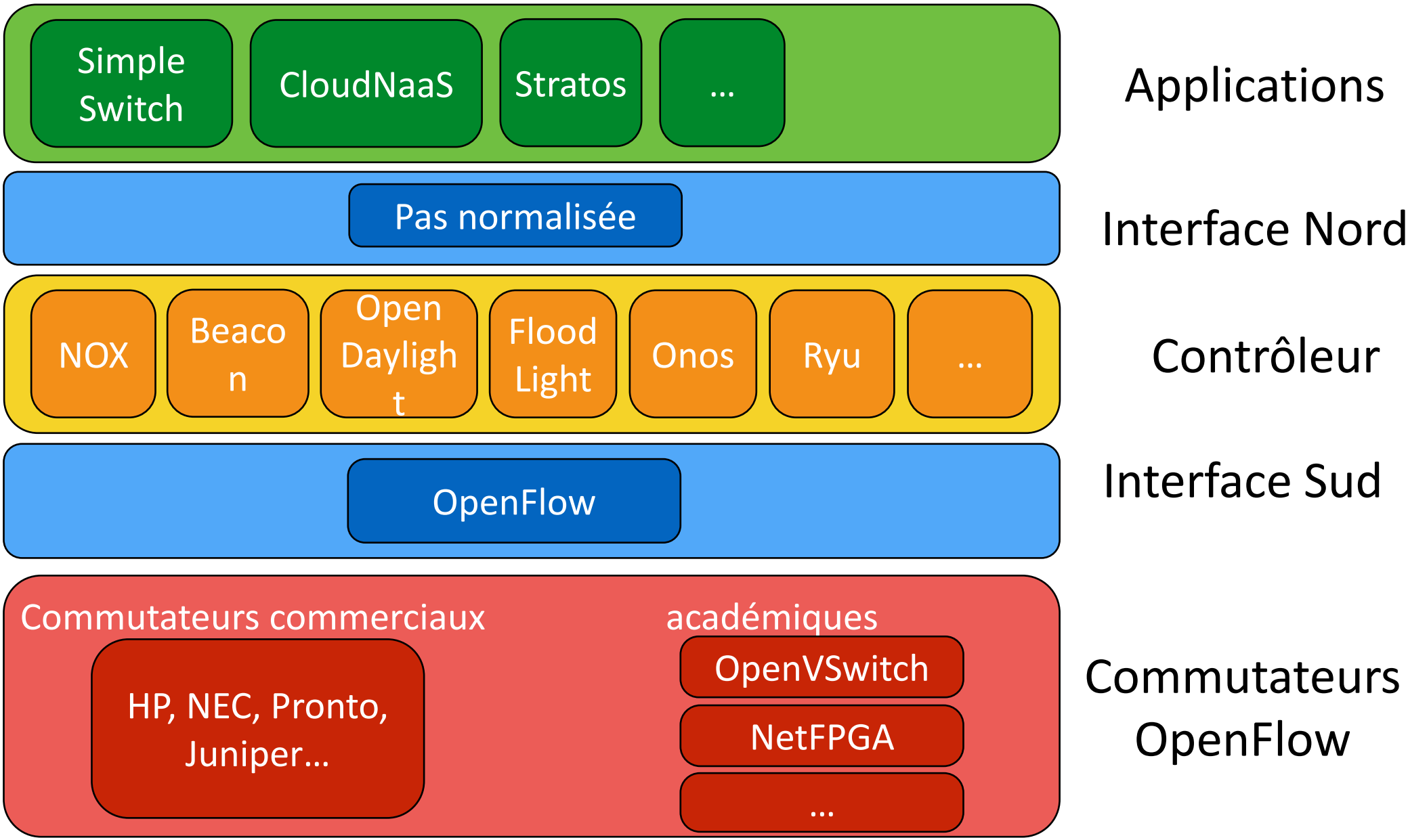
Entrées

- Topologie du réseau (changements)
- Statistiques sur le trafic
- 1er paquets des flots (mode réactif)

Sorties

- Instructions/Règles à instaurer/révoquer pour l'acheminement des données destinées aux commutateurs

La pile SDN


Simple Switch
CloudNaaS
Stratos
…
Applications
Pas normalisée
Interface Nord
NOX
Beacon
Open Daylight
Flood Light
Onos
Ryu
…
Contrôleur
OpenFlow
Interface Sud
Commutateurs commerciaux
HP, NEC, Pronto, Juniper…
académiques
OpenVSwitch
NetFPGA
…
Commutateurs OpenFlow

Plan

1. Introduction
2. Plan de contrôle & Plan de données
3. SDN
4. OpenFlow et P4
5. Applications SDN
6. NFV
7. Network slicing
8. Défis restants

- Format des règles pour le traitement des paquets (plan de données)
  - correspondance : selon les en-têtes des paquets
  - action : supprimer, expédier, modifier ou transmettre au contrôleur
  - priorité : arbitrer si plusieurs correspondances possibles
  - compteur : #octets and #paquets pour chaque règle

```
1.  src=1.2.*.*, dest=3.4.5.* → drop
2.  src=*.*.*.*, dest=3.4.*.* → forward(2)
3.  src=10.1.2.3, dest=*.*.*.* → send to controller
```

2 langages de programmation

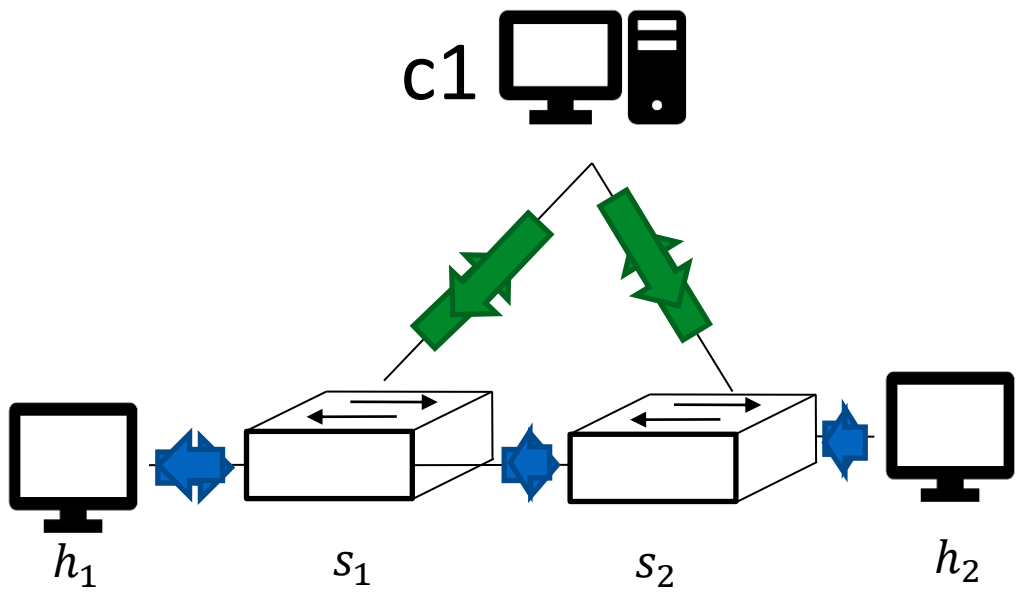
- OpenFlow : programmation du plan de contrôle

- P4 : programmation du plan de données

Unifie différents types d'équipements

- Routeur
  - correspondance: plus long préfixe IP partagé (BPM)
  - action: réexpédier sur un lien
- Commutateur ("Switch")
  - correspondance: adresse MAC destination
  - action: réexpédier ou innonder
- Pare Feu ("Firewall")
  - correspondance: adresses IP et #ports (TCP/UDP)
  - action: autoriser ou refuser
- NAT
  - correspondance: adresse IP et #port
  - action: réécritr les adresses et ports
- Equilibreur de charges
  - …

SDN en pratique : construction de la table des flux des switchs



- Packet In
  - Correspondance : Destination depuis
  - **Requête du switch**
- Flow Mod
  - Correspondance : Destination depuis
  - Action : transmettre à
  - **Direction du contrôleur**

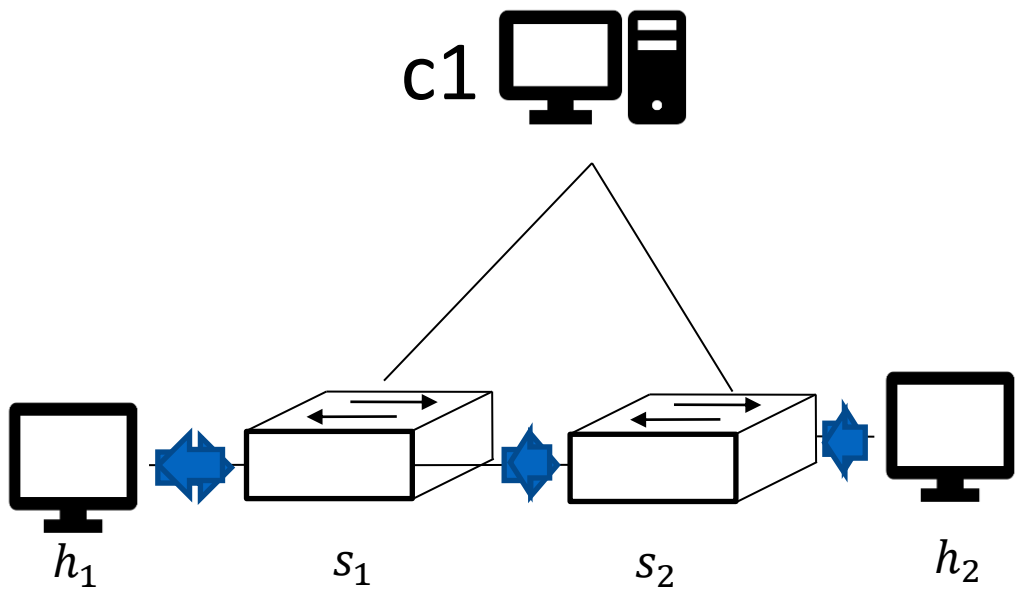
Src	Dst	Action
H1	H2	S2
H2	H1	H1

Partie Correspondance pour identifier le flux

Partie Action pour dire quoi faire avec ce flux

En réalité, l'action correspond au port relié au switch

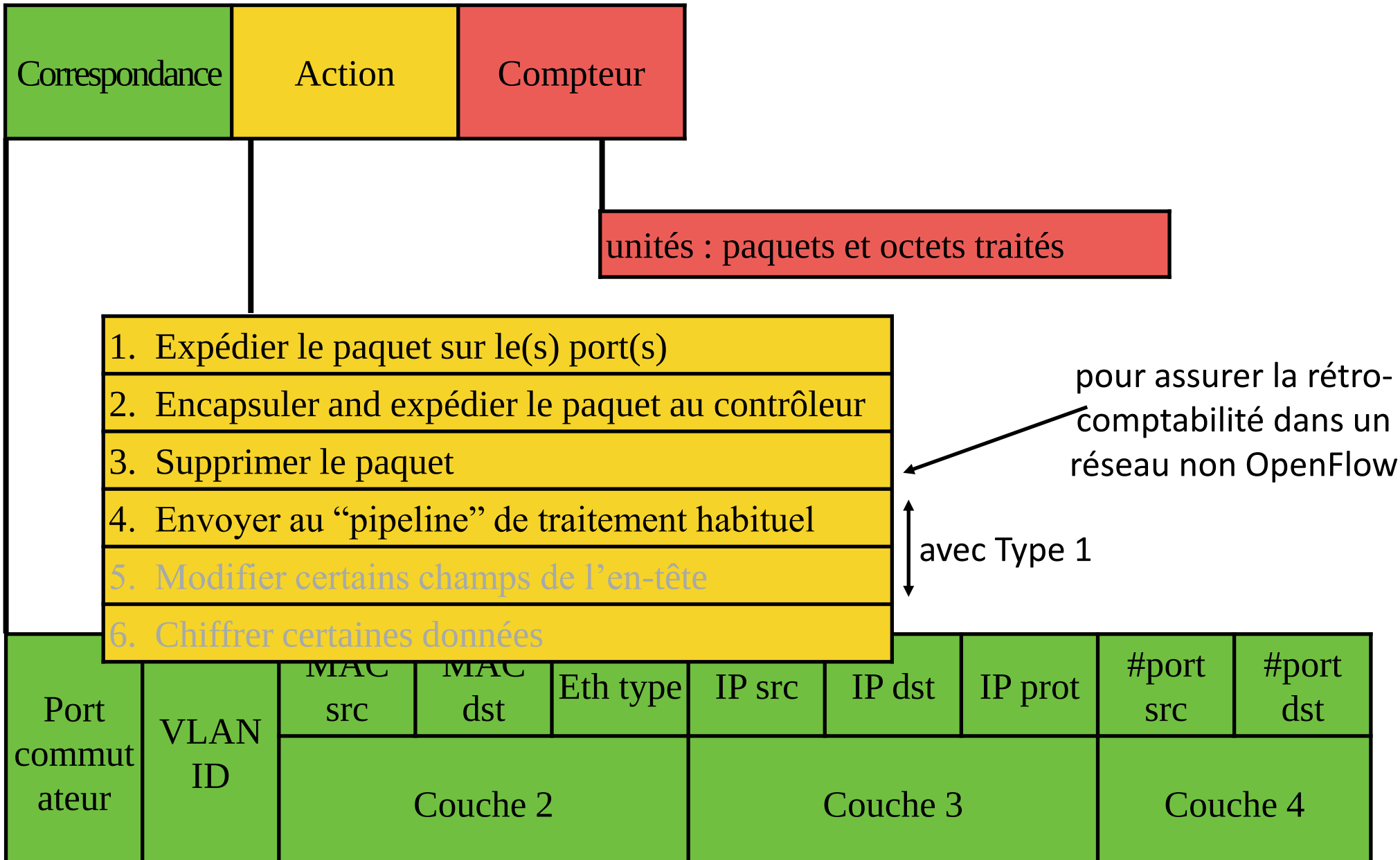
SDN en pratique : utilisation de la table des flux des switchs



Src	Dst	Action
H1	H2	S2
H2	H1	H1

- Le contrôleur avait écrit la règle
  - Application de la règle et pas besoin de passer par une requête
  - En réalité, les règles ne sont pas éternelles (temps de vie ou suppression manuelle par le contrôleur)
  - Paramètre supplémentaire : Idle time

Format d'une règle OpenFlow



Exemple de règles OpenFlow

Fonction	Port entrée	VLAN ID	MAC src	MAC dst	Eth type	IP src	IP dst	IP prot	#port src	#port dst	Action
Routeur	*	*	*	*	*	*	5.6.*.*	*	*	*	Port6
Comm. (paquet)	*	*	*	00:1f..	*	*	*	*	*	*	Port 6
Comm. VLAN	*	Vlan1	*	00:1f..	*	*	*	*	*	*	Port6, Port 7, Port 8
Pare-feu	*	*	*	*	*	*	*	*	*	22	Drop
Comm. flux	Port 3	Vlan1	00:20..	00:1f..	0800	1.2.3.4	5.6.*.*	*	4	17264	Port 6
???	*	*	*	*	*	10.1.2.3	*	*	*	*	Send to controller

Proactives

Réactives

Permet d'émuler les fonctions de presque tous les équipements réseaux

Plan

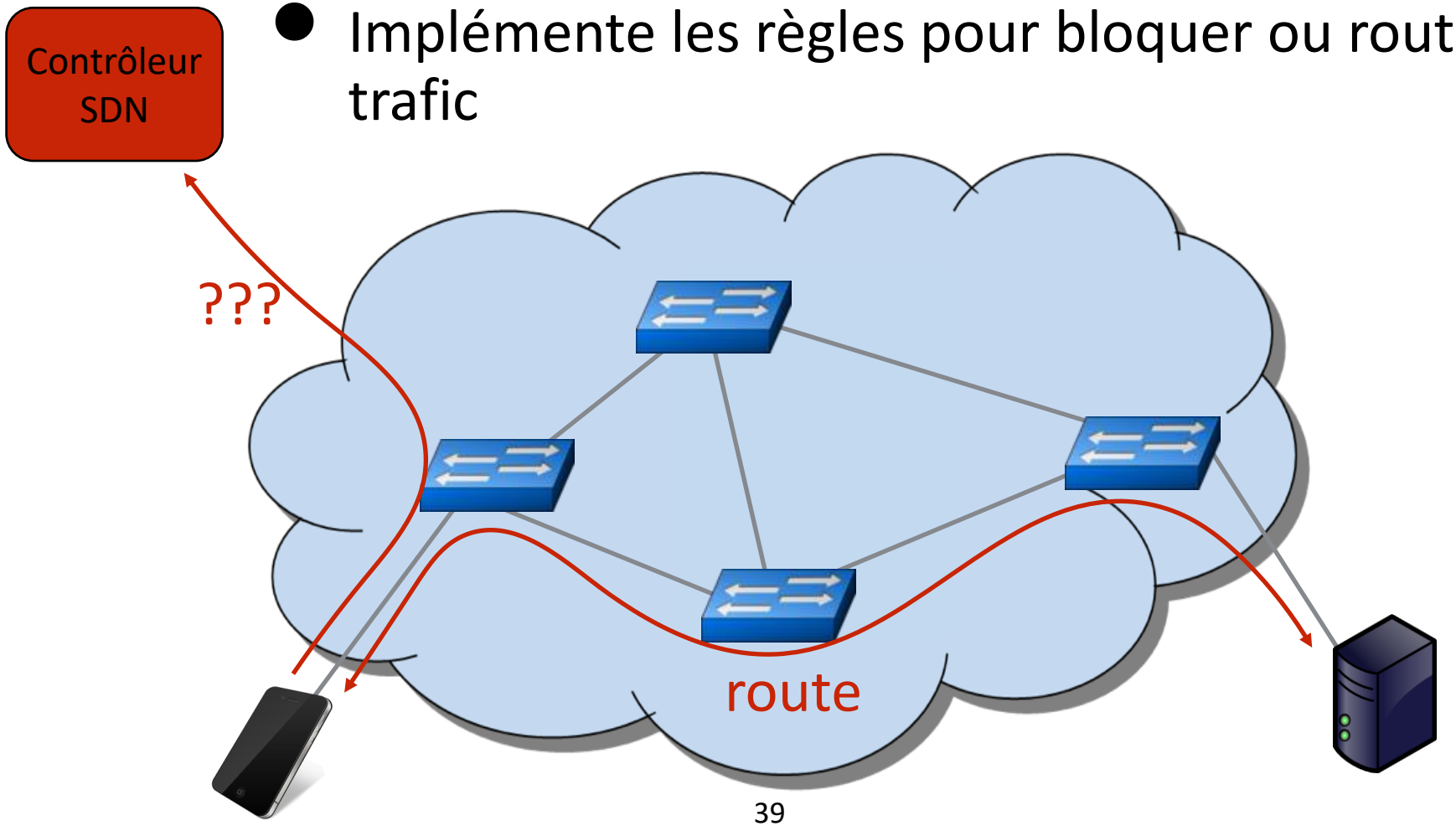
1. Introduction
2. Plan de contrôle & Plan de données
3. SDN
4. OpenFlow et P4
5. Applications SDN
6. NFV
7. Network slicing
8. Défis restants

Exemple d’applications SDN

- Contrôle d’accès dynamique
- Mobilité sans interruption
- Equilibrage de charge des serveurs
- Utilisation de plusieurs points d’accès sans fil

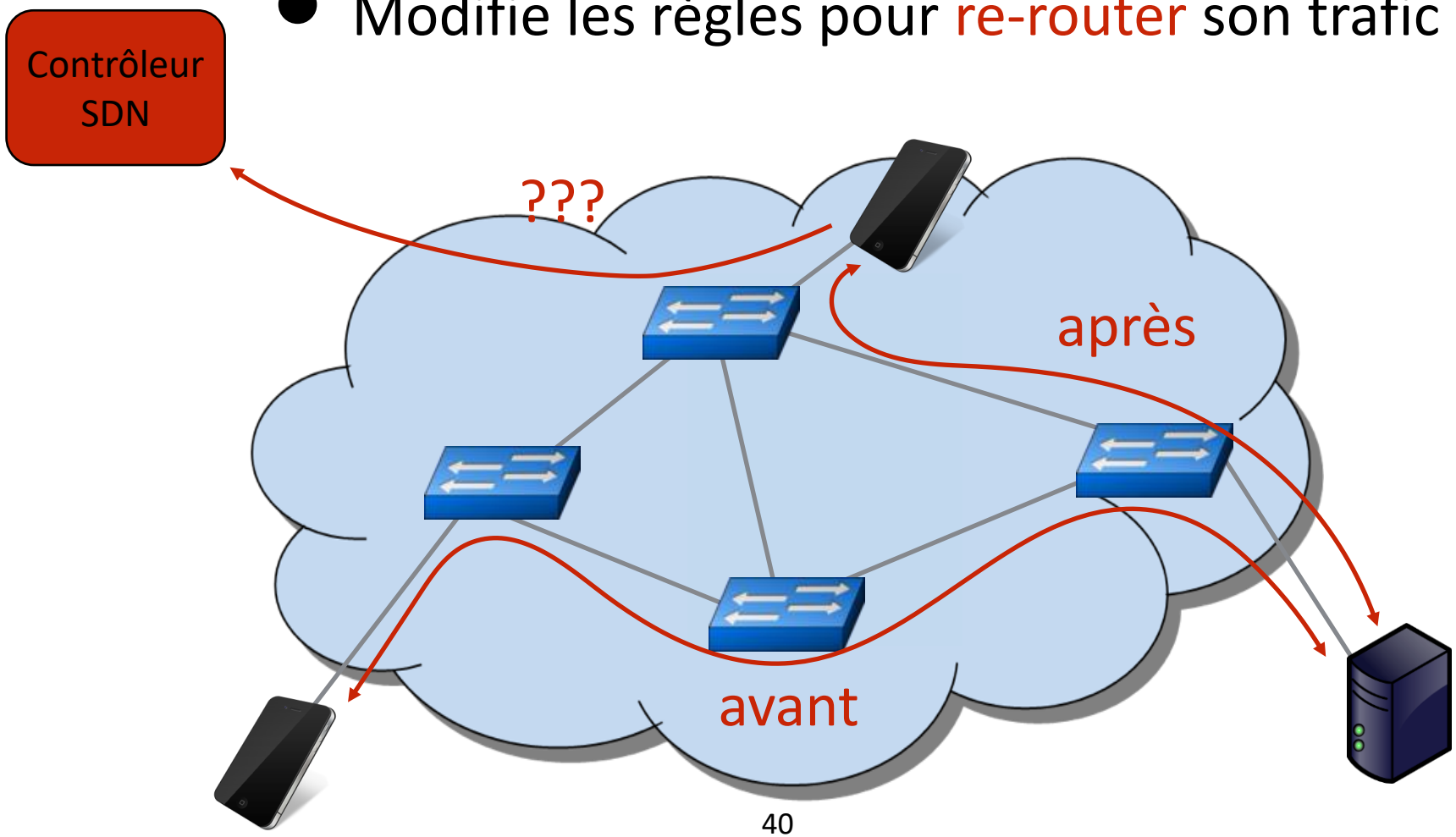
Contrôle d'accès dynamique

- Inspecte le premier paquet d'une connexion (flux)
- Consulte la politique de contrôle d'accès
- Implémente les règles pour bloquer ou router le trafic



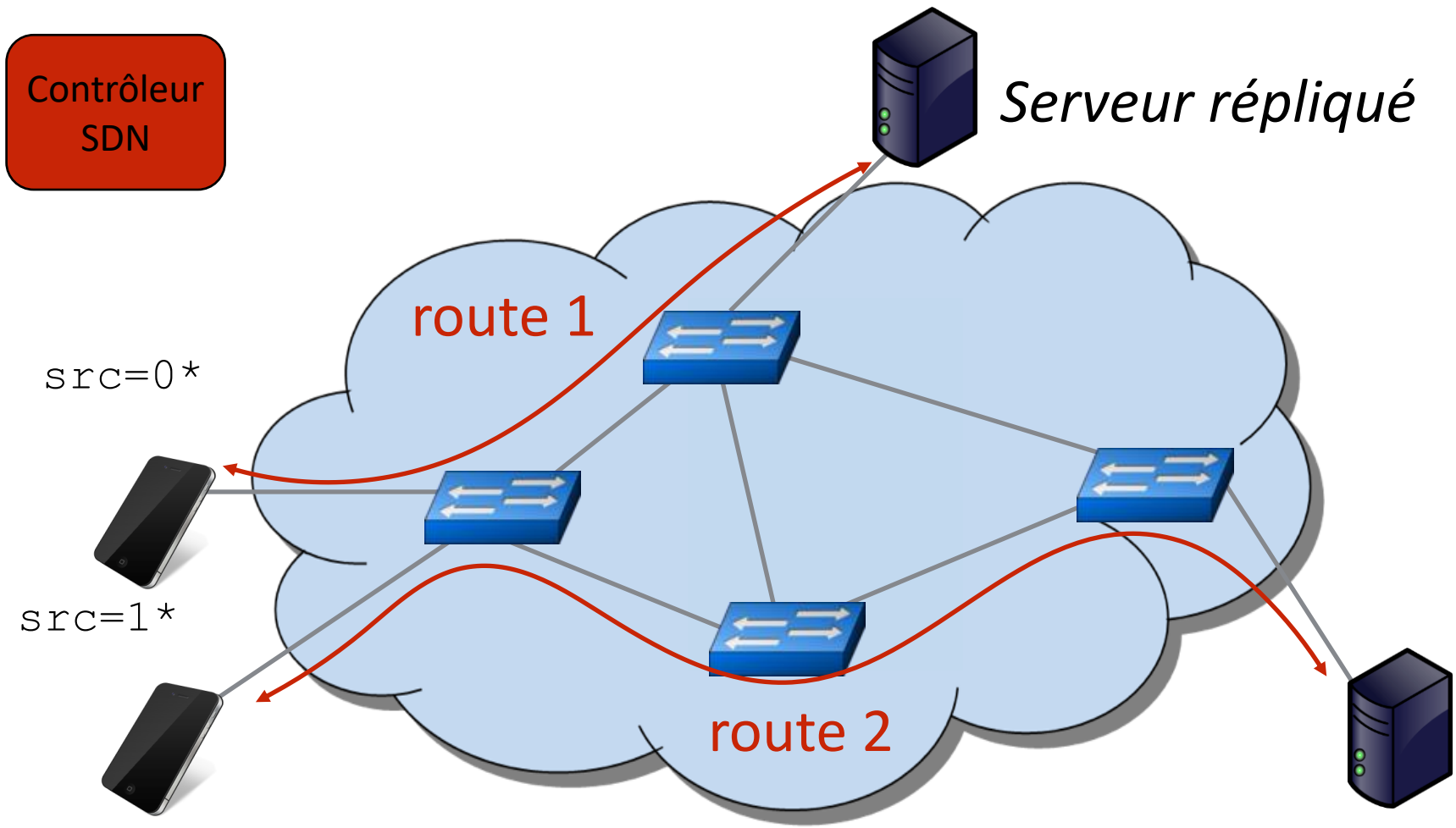
Mobilité sans interruption

- Découvre que l'hôte s'est déplacé
- Modifie les règles pour re-router son trafic



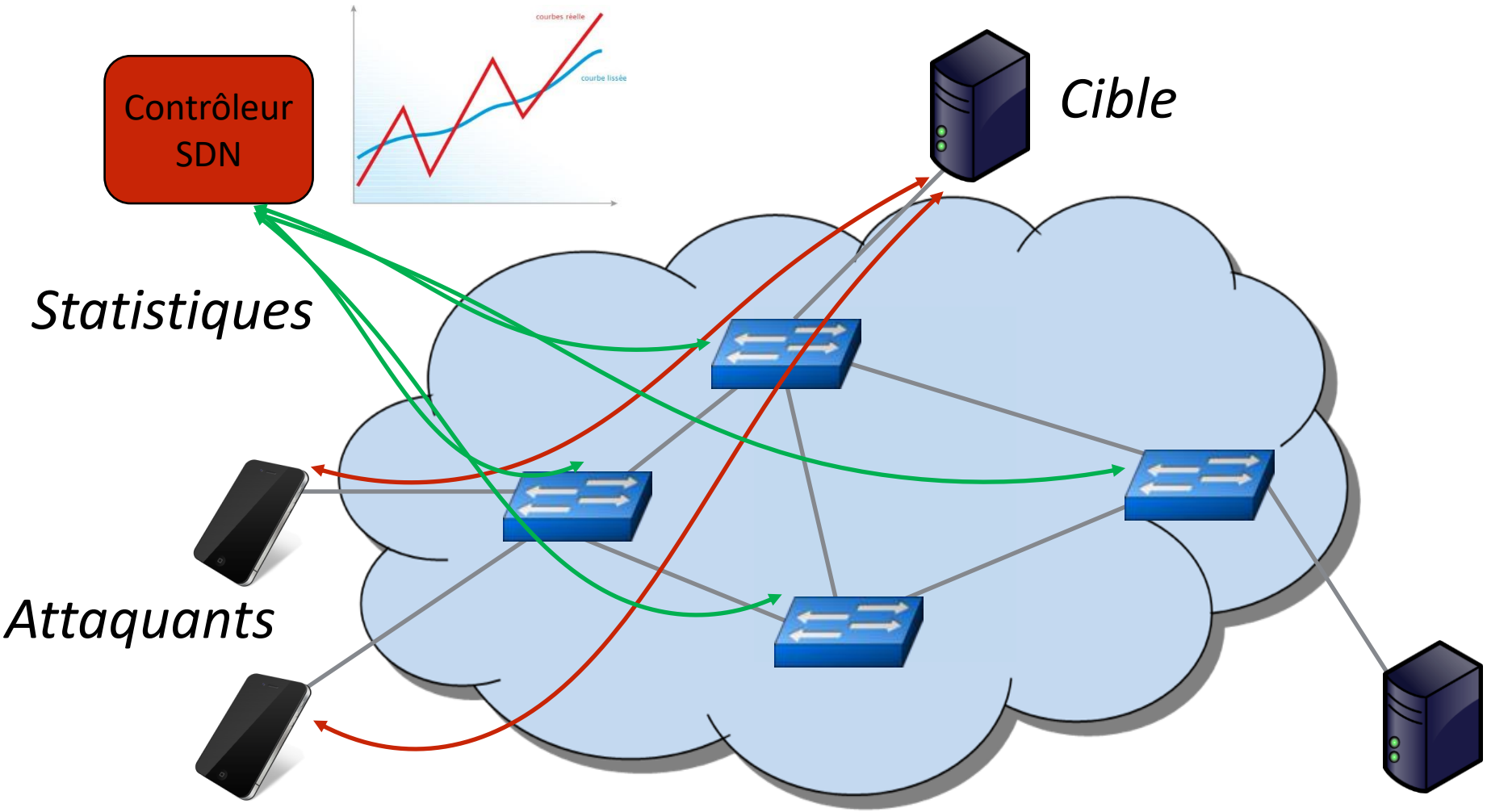
Equilibrage de charge des serveurs

- Pré-implémente les politiques d'équilibrage de charge
- Scinde le trafic en fonction de la @IP source



Détection d'attaque

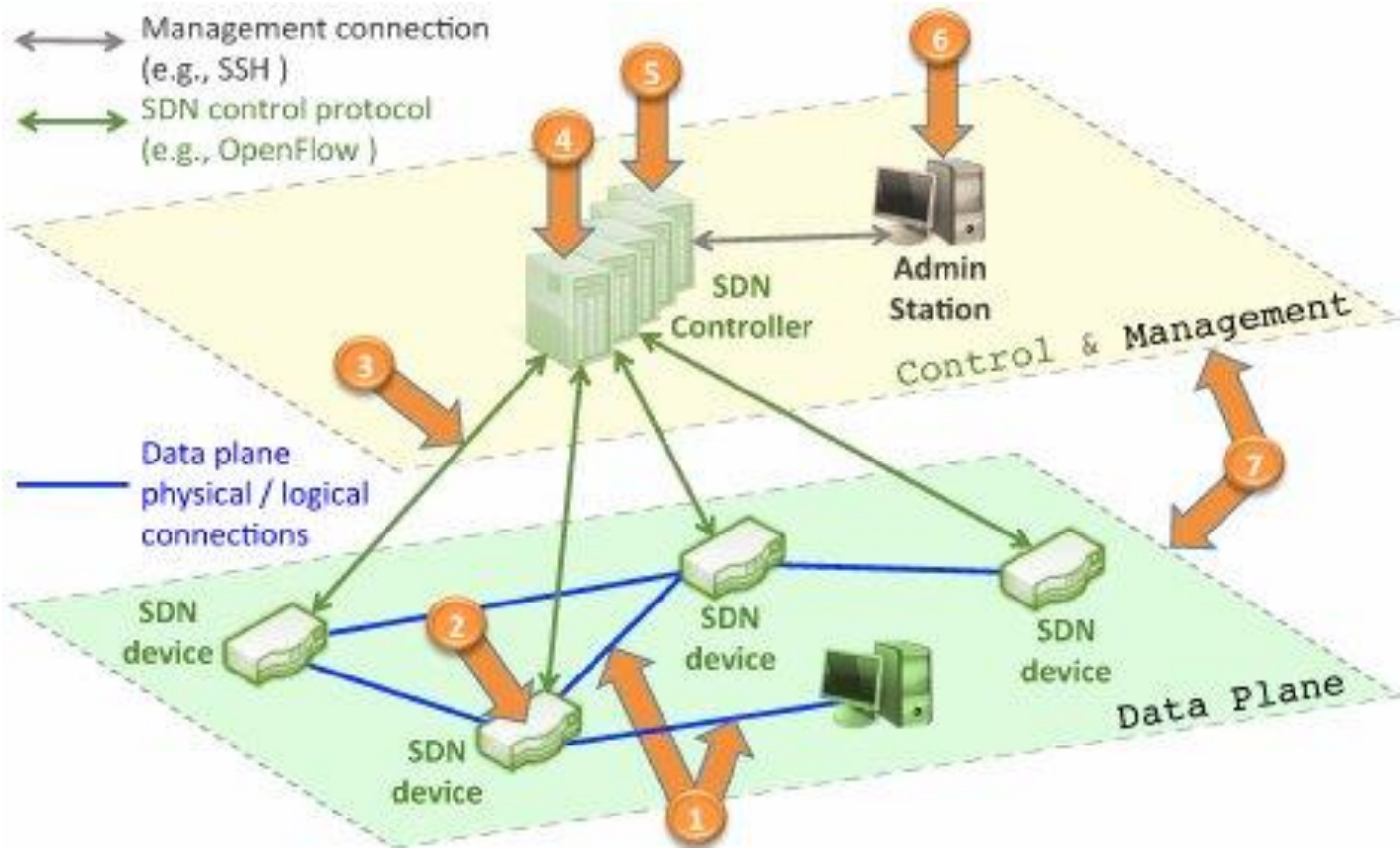
- Analyse des statistiques pour rechercher des anomalies



SDN & OpenFlow dans le monde

- Open Networking Foundation
  - Google, Facebook, Microsoft, Yahoo, Verizon, Deutsche Telekom, et beaucoup d'autres
- Commercialisation de commutateurs OpenFlow
  - HP, NEC, Quanta, Dell, IBM, Juniper,…
- Network OS
  - NOX, Beacon, Floodlight, Nettle, ONIX, Frenetic
- Déploiement actuel
  - Plusieurs campus et réseaux commerciaux (2018)
  - Google (2021)
    - Réseau B2 : MPLS accès clients vers ses datacenters
    - Réseau B4 : SDN pour l'interconnexion entre ses datacenters
  - CISCO : solution ACI (Application Centric Infrastructure) pour les datacenters
  - SD-WAN et 5G

Enjeu en SDN : sécurité

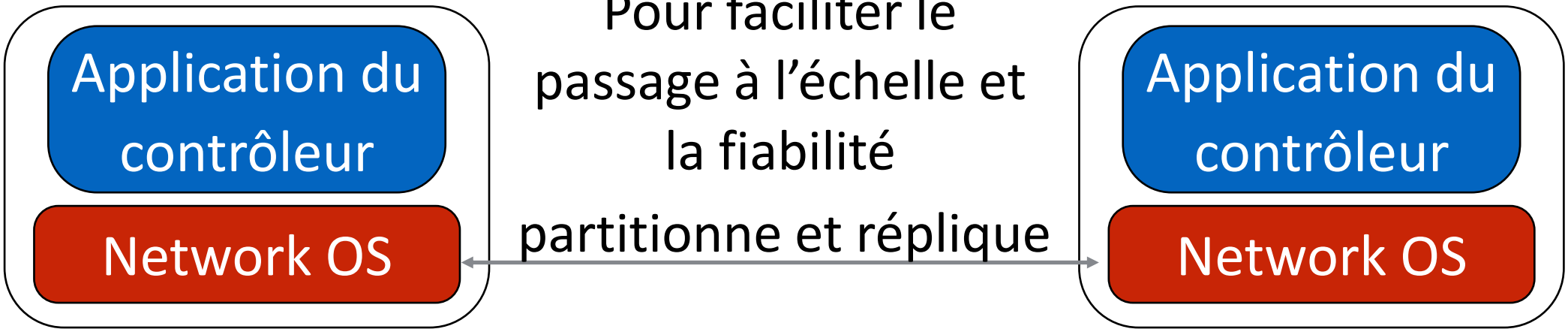


Kreutz, D., Ramos, F. M., & Verissimo, P. (2013, August). Towards secure and dependable software-defined networks. In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking* (pp. 55-60).

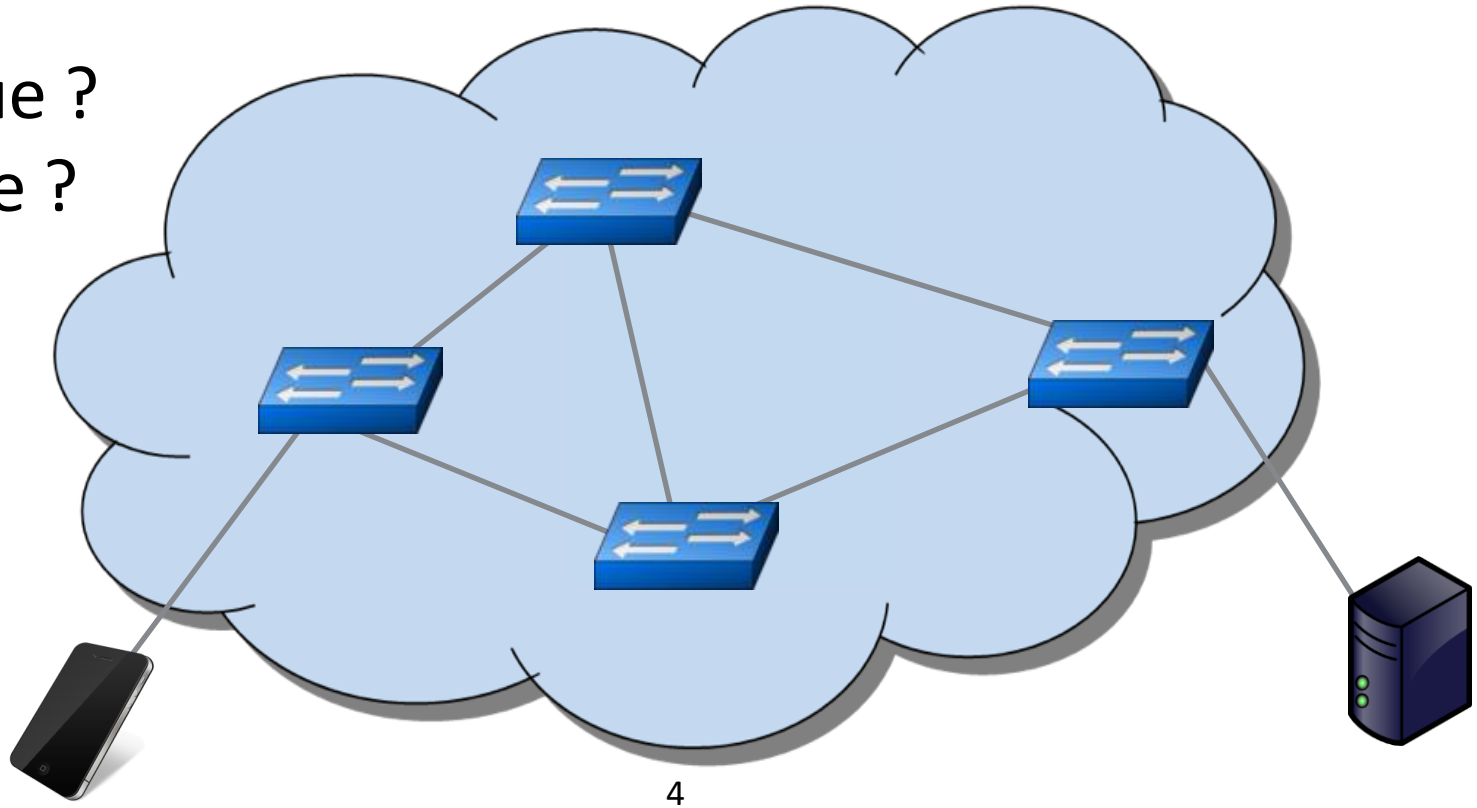
Contrôleur SDN

- Un ou plusieurs ?
  - passage à l'échelle
  - Fiabilité (un unique point de défaillance)
  - Vulnérabilité (cyber sécurité)
- Réplication ou partition (arborescence)
- Où les situer ? Comment les faire communiquer ?
- Comment garantir une qualité de service malgré la latence introduite
- Autant de sujets de recherche

Contrôleur distribué



Hiérarchique ?
Horizontale ?

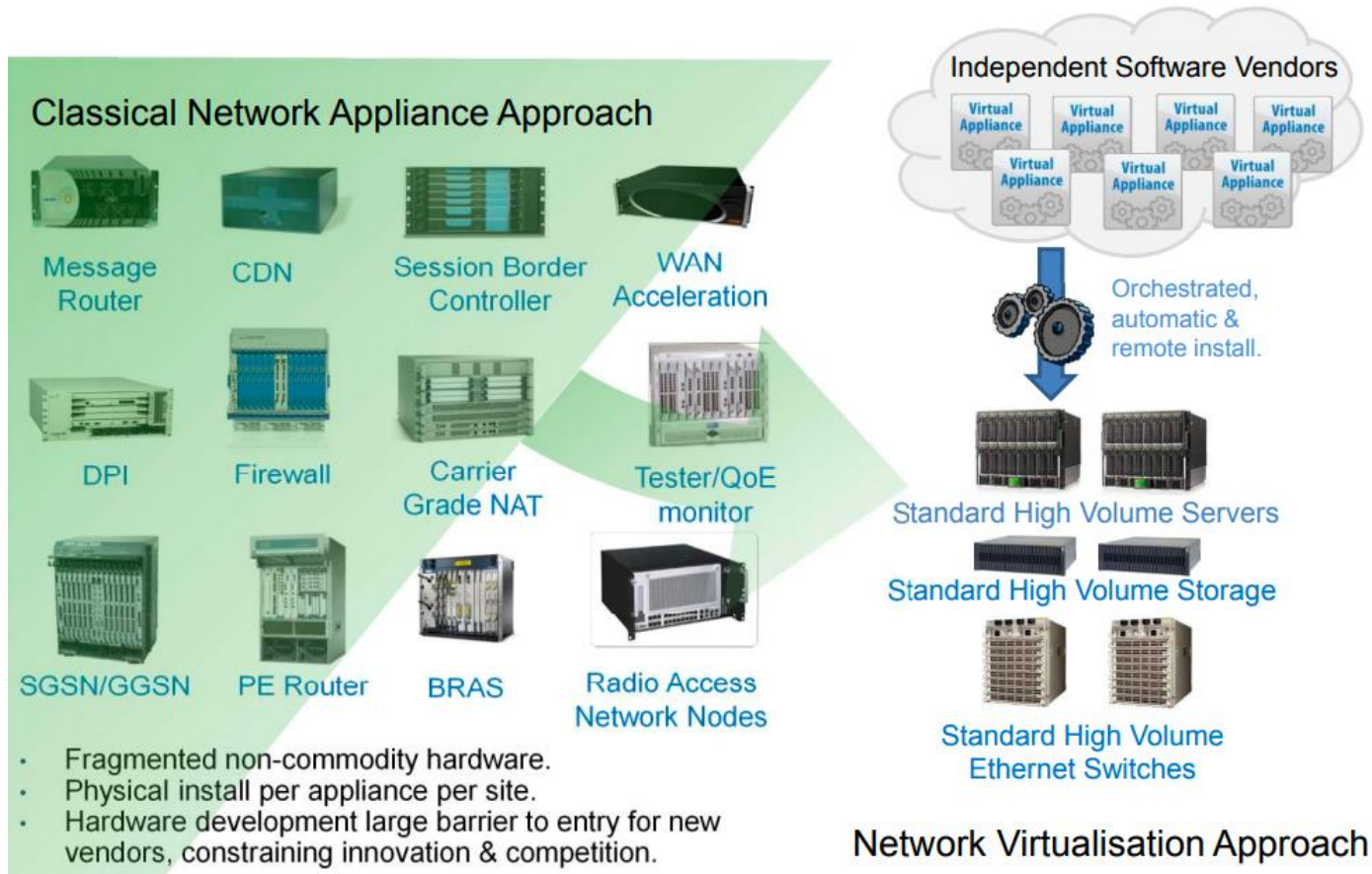


Plan

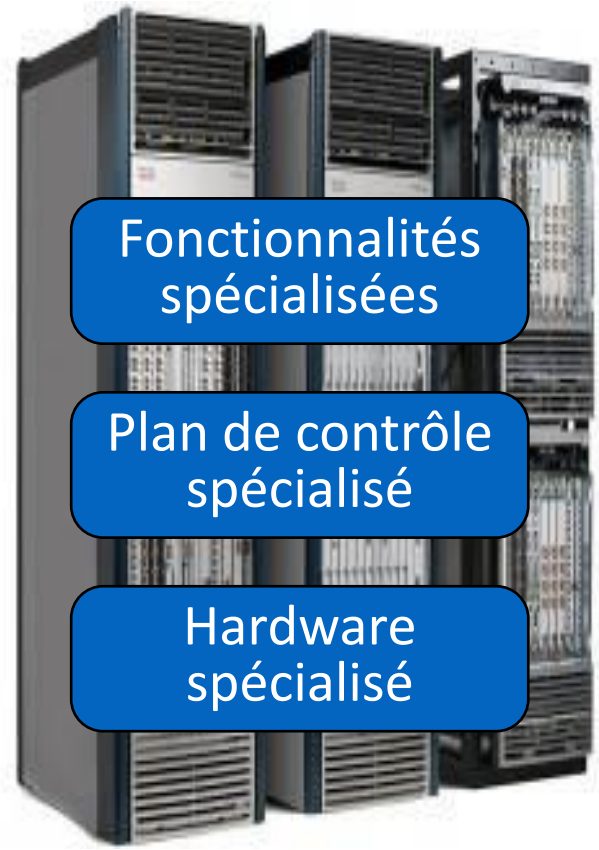
1. Introduction
2. Plan de contrôle & Plan de données
3. SDN
4. OpenFlow et. P4
5. Applications SDN
6. NFV
7. Network slicing
8. Défis restants

Network Functions Virtualization

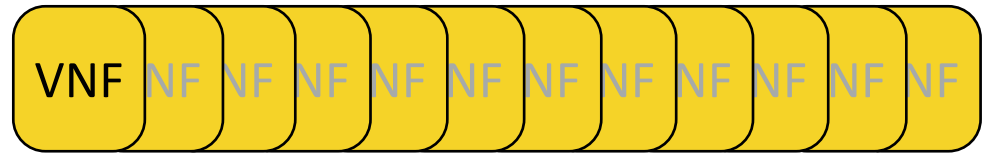
- Remplacer les équipements réseaux matériels (fermés, chers et peu évolutifs)
  - par du logiciel spécialisé s'exécutant sur du matériel standard
- Softwarization du réseau
  - Fonction VNF (Virtualized Network Function) : émule une fonction réseau



Routeurs & Commutateurs



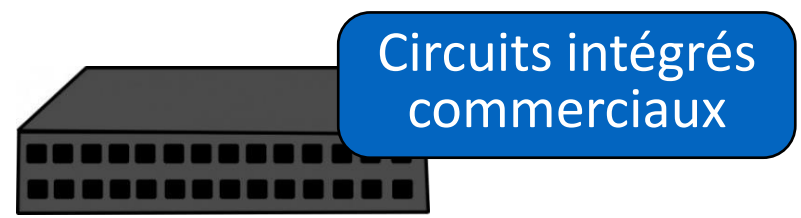
Intégration verticale, fermé, propriétaire, innovation lente



—— Interface ouverte ——

Plan de contrôle ou Plan de contrôle ou Plan de contrôle

—— Interface ouverte ——



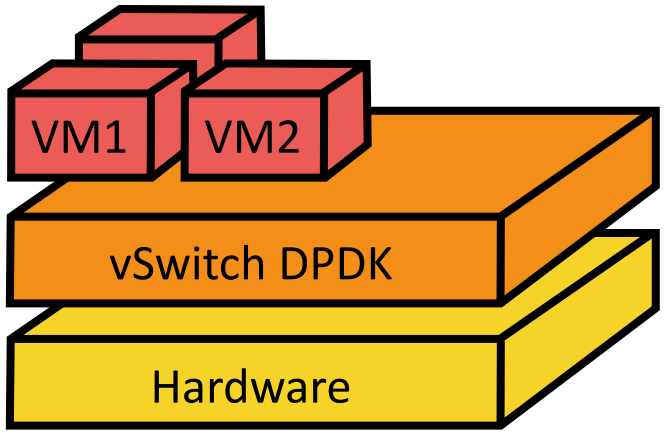
Horizontal interfaces ouvertes, innovation rapide, nombreux acteurs

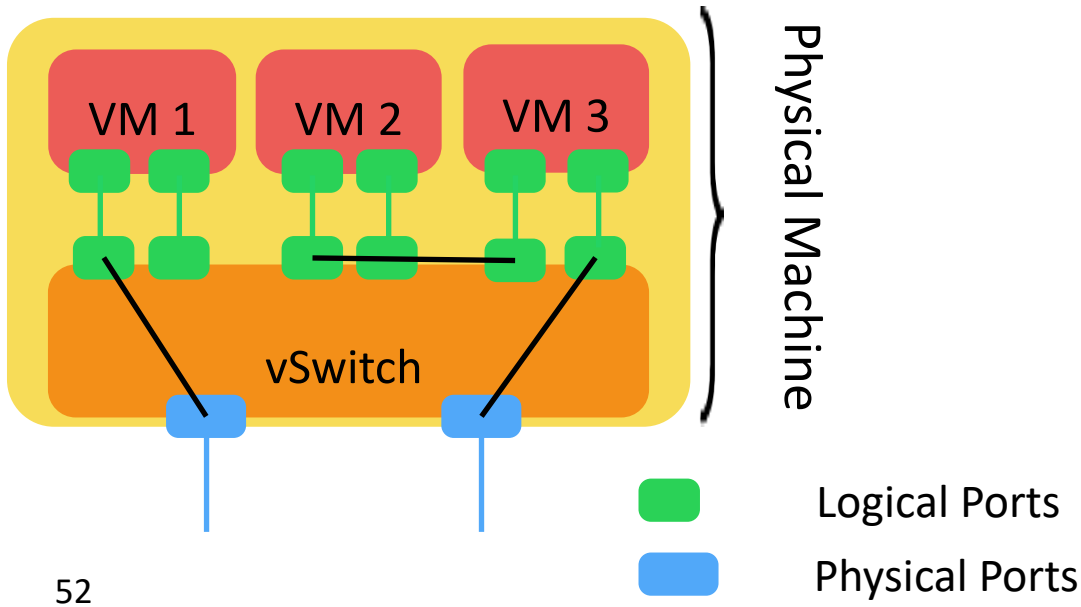
Un réseau plus agile

- Les fonction VNF peuvent être hébergées dans une VM
  - Possible d'allumer/déplacer/éteindre les fonctions selon la demande
    - Migration de VM, Proximité des clients (Folllow-the-sun)
- Exemples de fonctions VNF
  - Commutation: switch, routeur, NAT
  - Noeuds des réseaux mobiles : NodeB, eNodeB
  - Noeuds résidentiels : routeur domestique et box internet
  - Passerelles : IPSec/SSM VPN gateways, IPv4-IPv6 conversion, encapsulation, tunelling
  - Analyse de traffic : DPI, mesure de QoE
  - Converged and network-wide functions : serveurs AAA, policy control, charging platforms
  - Optimisation des applications : CDN, serveur cache, équilibreur de charge, accélérateur applicatif
  - Fonctions de sécurité : firewall, anti-virus, IDS/IPS, filtre anti-spam

Exemples de fonctions

- Commutateur simple
  - Aussi appelé vSwitch
  - Typiquement déployé sur l'hyperviseur (ou une VM)
  - Exemple de logiciel : Open vSwitch
  - Exemple de librairie spécialisée : DPDK, netmap
  - Performances : débit de plusieurs dizaine de Gbps
- Exemple d'un vSwitch avec 3 VMs





Déploiement actuel du NFV

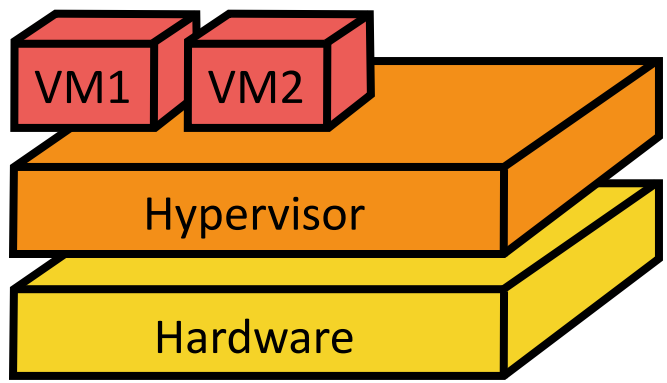
- Réseaux 5G
- Routeurs virtuels
  - OpenvSwitch (OVS)
    - Avec librairie DPDK
- Parefeux
  - pfSense, OPNsense (basés sur FreeBSD)

Plan

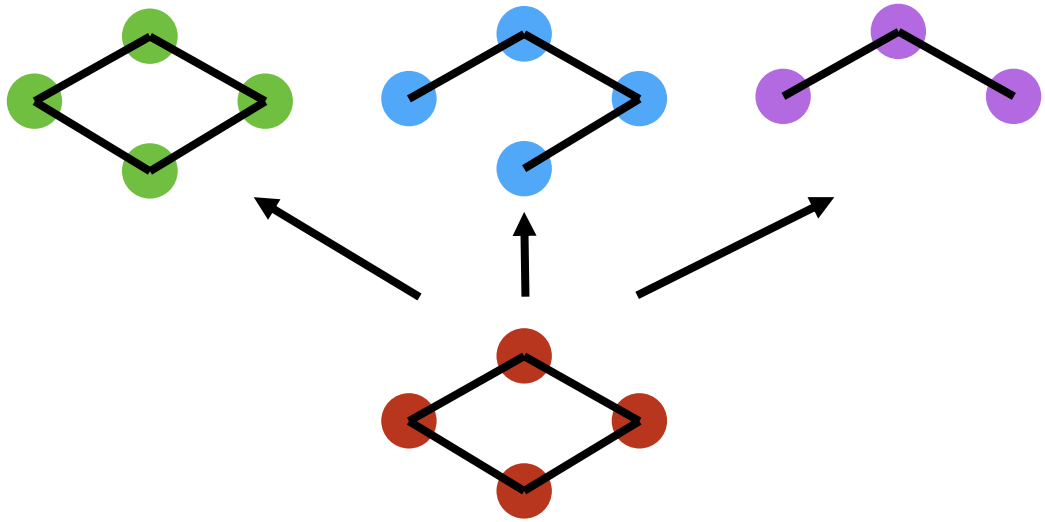
1. Introduction
2. Plan de contrôle & Plan de données
3. SDN
4. OpenFlow et P4
5. Applications SDN
6. NFV
7. Network slicing
8. Défis restants

Virtualisation des serveurs

- Très courant dans les datacenters
- Plusieurs VMs partagent les ressources d'une PM
  - Ressources propres ou partagées
- L'hyperviseur gère la création/destruction des VMs
- Avantage : mutualisation des ressources



Virtualisation des réseaux



3 réseaux virtuels isolés sur une même infrastructure

Network slicing = Faire cohabiter "indépendamment" plusieurs réseaux sur une même infrastructure physique

Network slicing

- 3 techniques principales utilisées
  - Description d'un slice en un ensemble de fonctions réseaux
    - Briques fonctionnelles élémentaires
  - Virtualisation
    - NFV pour s'abstraire des resources physiques
  - Orchestration
    - Contrôleur SDN pour allouer les resources
- Au coeur de la 5G pour permettre le déploiement de réseaux différents (QoS) sur une même infrastructure

Avantages du NFV

- Utiliser du matériel standard (COTS hardware)
  - Réduire les coûts de déploiement et d'exploitation
  - Economies d'échelle
- Réduire les délais / cycles de développement et de déploiement
- Consolidation du parc informatique
  - Réduire consommation électrique
- Développer un réseau plus souple et dynamique
  - Déplacer des fonctions réseaux vers les datacenters, POPs ou selon la demande
- Permettre le Network Slicing
  - Faire cohabiter (indépendamment) plusieurs réseaux sur une même infrastructure physique

Plan

1. Introduction
2. Plan de contrôle & Plan de données
3. SDN
4. OpenFlow et P4
5. Applications SDN
6. NFV
7. Network slicing
8. Défis restants

SDN & NFV

- Ensemble, SDN et NFV permettent
- Un réseau programmable et agile
  - Allocation dynamique des ressources
  - Meilleur contrôle (+ direct et + fin) sur le plan de données
  - Les opérateurs (datacenters, FAI, entreprises…) pourront programmer leurs réseaux
  - Infrastructure as Code (IaC)

Défis restants

- Délai induit par le contrôleur SDN en mode réactif
  - Surcoût du temps de réponse
- Disponibilité du contrôleur SDN
  - Performances si montée en charge
- Fiabilité du contrôleur SDN
  - Tolérance aux pannes (single point of failure)
- Sécurisation du contrôleur SDN
  - Protection aux attaques
- Performances des commutateurs NFV
  - Librairies spécialisées
- Sécurisation du network slicing
  - Réseaux virtuels : différents mais indépendants ?

Fin du Cours