



# AUTOMATISATION ET VIRTUALISATION DES RÉSEAUX

1

- SDN (Software Defined Networks)
- NFV (Network Function Virtualization)
- OpenFlow

# INTRODUCTION




- Avec la révolution des numériques, le secteur des télécommunications est au cœur des transformations technologiques :
  - Virtualisation des services : les ressources informatiques deviennent accessibles sous forme de services
  - Cloud : data center, cloud-based storage : sont devenus des éléments courants du réseau, qui offrent plus de services et de ressources informatiques

 créer, organiser et gérer de très grands volumes de données

- Pour Supporter le besoins croissants en termes de gestion de trafic et de services : Migrer vers d'autres solutions tels que SDN et NFV

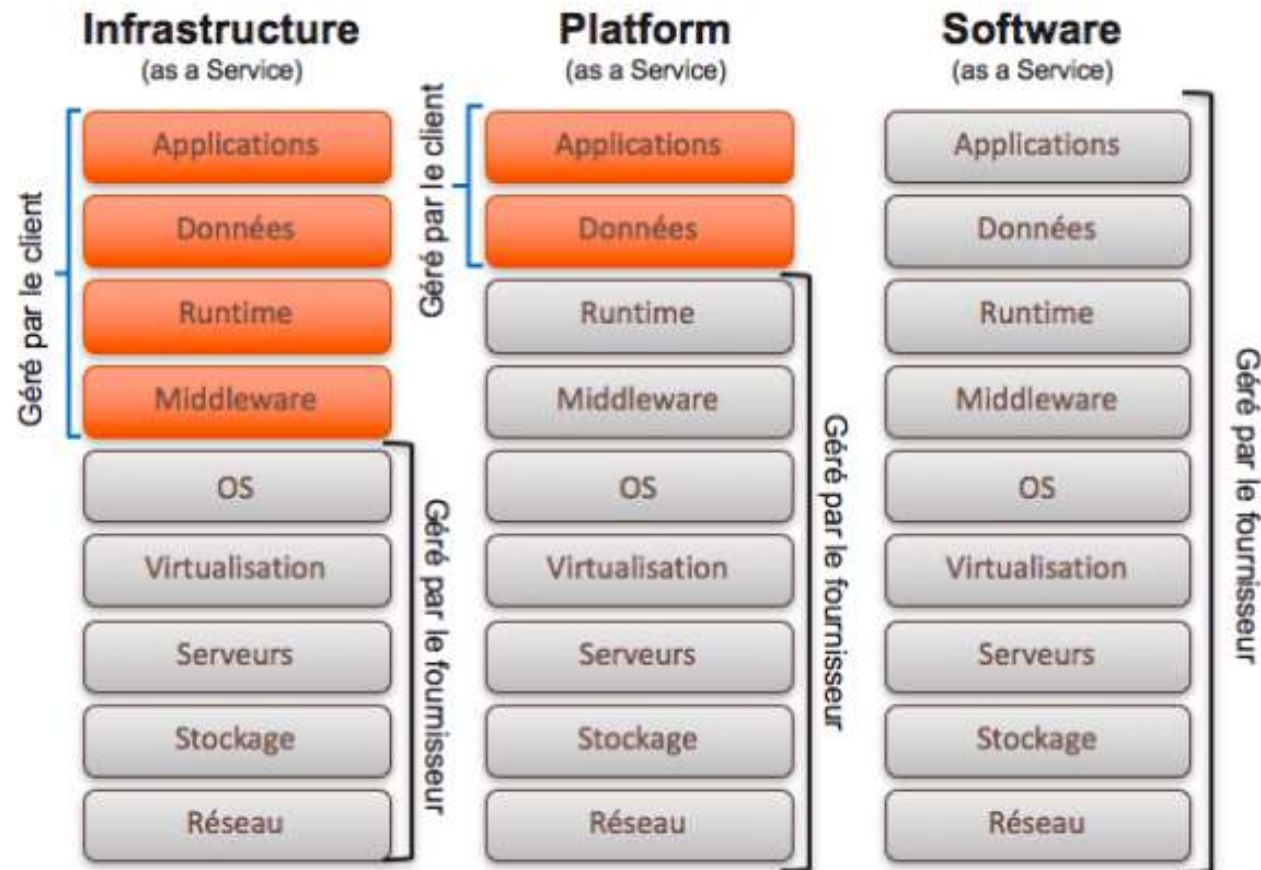
# CLOUD COMPUTING

- Le Cloud Computing est basé sur 5 caractéristiques

	<b>Service à la demande :</b> Tout est automatisé et à disposition en libre-service
	<b>Accessible partout :</b> Les données sont disponibles via le réseau et accessibles depuis un équipement (PC, tablette...)
	<b>Elasticité/Extensibilité rapide :</b> Augmentation ou diminution de la capacité selon les besoins
	<b>Utilisation quantifiable :</b> L'utilisation des ressources est mesurée et rapportée, assurant la transparence du service utilisé au client et au fournisseur
	<b>Le partage des ressources :</b> Les ressources sont mutualisées et mises à disposition des clients par le fournisseur de Cloud sur un modèle multi-tenant

# CLOUD – MODÈLES DE CONSOMMATION

- Le Cloud computing se décompose en trois grands modèles

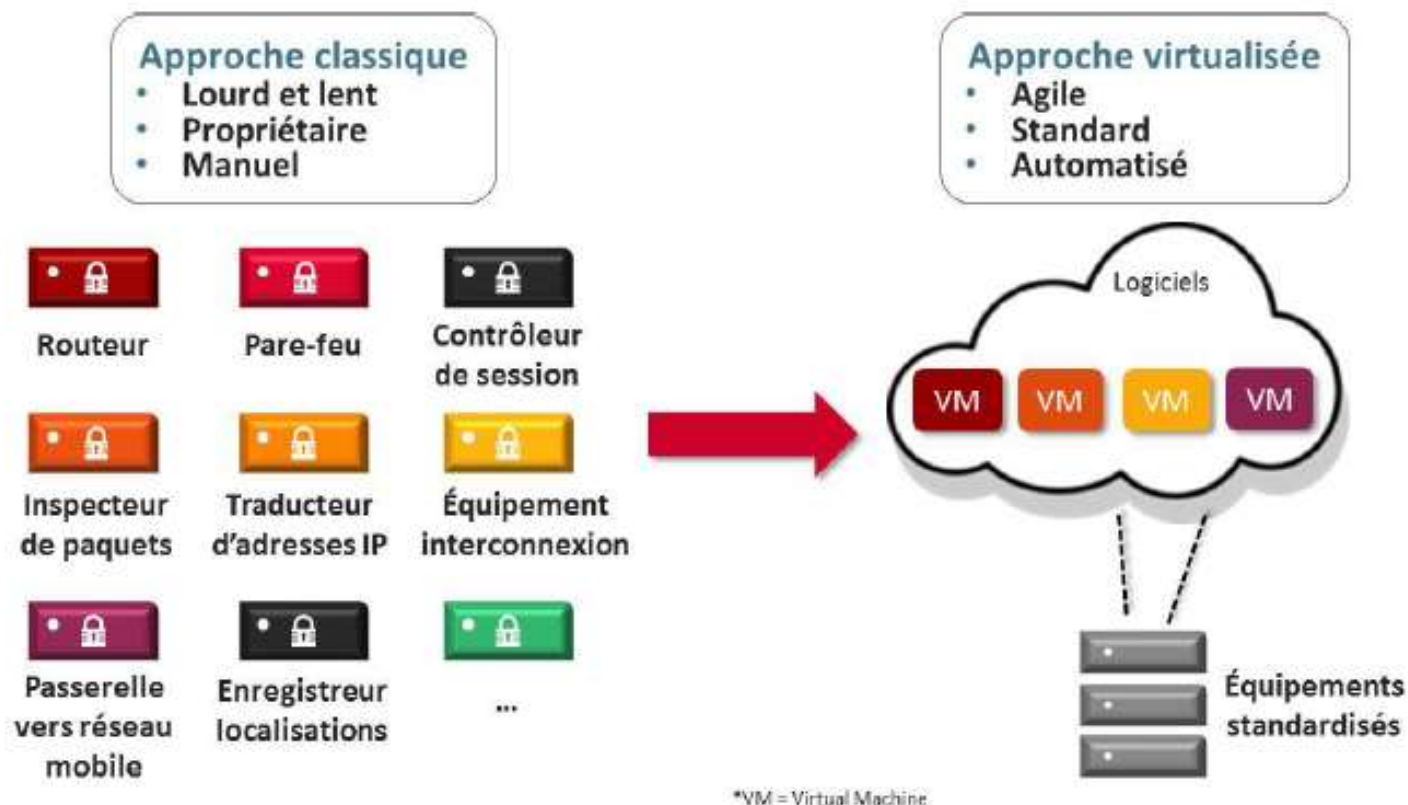


## CLOUD – MODÈLES DE CONSOMMATION

- Le SaaS (Software As A Service) met à disposition des utilisateurs des applications sans avoir la nécessité de gérer le réseau, les serveurs, les systèmes d'exploitation, le stockage.
- Le PaaS (Platform As A Service) permet au client de bénéficier d'une plateforme de développement hébergé par un fournisseur, sans avoir à gérer le réseau, les serveurs, les systèmes d'exploitation ni le stockage.
- L'IaaS (Infrastructure As A Service) apporte aux entreprises une infrastructure virtualisée en leur fournissant, à la demande, une capacité de traitement et de stockage sans avoir à gérer le réseau, les serveurs et le stockage localisés dans des datacenters.

# NETWORK FUNCTIONS VIRTUALIZATION (NFV)

- Le NFV consiste à faire assurer les fonctions réseau non plus par du matériel dédié mais par des logiciels s'exécutant sur du matériel banalisé façon « datacenter ».



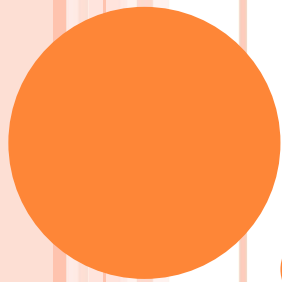
# NFV

- La virtualisation des fonctions réseau permet d'extraire des fonctions du matériel, et ainsi d'utiliser des serveurs standard pour d'autres fonctions qui nécessitaient auparavant un équipement propriétaire coûteux.
- Exemples :
  - Niveau 2 OSI « Switch virtualisé » : logiciel OpenVSwitch
  - Niveau 3 OSI « Router virtualisé » : OpenVSwitch+IPTables
  - Niveau 4 OSI « virtual Load Balancer »: Ex Apache Load Balancer

## AVANTAGES DE L'ARCHITECTURE NFV

- Diminution des dépenses d'investissement et des dépenses d'exploitation de l'opérateur grâce à la réduction des coûts d'équipement et de la consommation d'énergie.
- Réduction des délais de mise sur le marché des nouveaux services de réseau
- De nouveaux services pour des revenus accrus
- Évolution des services, ou augmentation ou diminution de l'échelle grâce à une meilleure flexibilité
- Moins de risques pour l'essai et le déploiement de nouvelles opportunités de services





# SDN

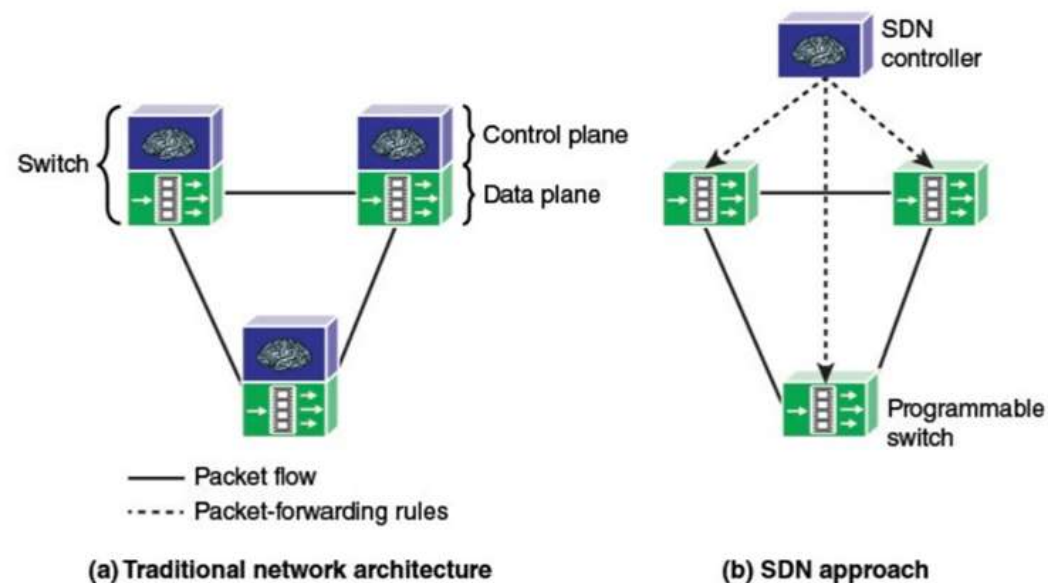
## Software Defined Networks

# INTRODUCTION

- Le SDN (Software-Defined Networking) est une approche de gestion et de contrôle des réseaux qui permet aux administrateurs réseau :
  - de gérer et de configurer des réseaux de manière plus flexible,
  - De centraliser et automatiser le fonctionnement de réseau.
- Le SDN est basé sur un contrôleur et sur le protocole OpenFlow (OF), qui communique avec les Open vSwitch (OVS).

# COMPARAISON ENTRE RÉSEAU TRADITIONNEL ET SDN

- Réseau Traditionnel :
  - Plan de contrôle (indépendant) : prise de décision distribué
- SDN :
  - Plan de contrôle centralisé : prise de décision centralisé

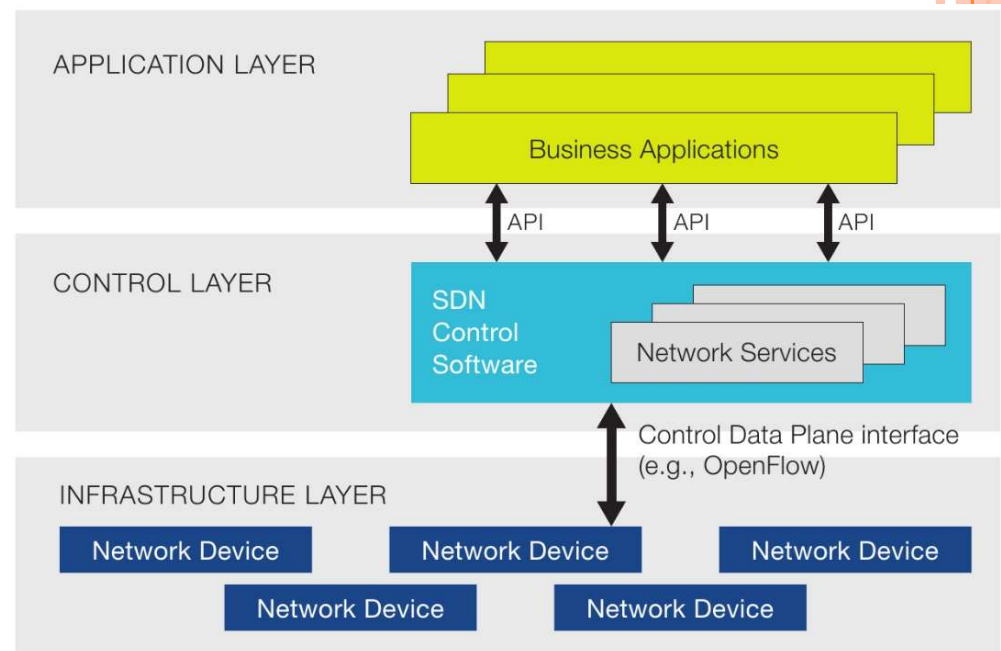


## SDN : DÉFINITION

- SDN est un concept qui sépare le plan de contrôle du plan de transfert de données, et où un plan de contrôle contrôle plusieurs dispositifs.
- Cette architecture sépare les fonctions de contrôle et de transfert du réseau, permettant ainsi au contrôle réseau de devenir directement programmable et l'infrastructure sous-jacente d'être abstraite pour les applications et les services réseau

# ARCHITECTURE SDN

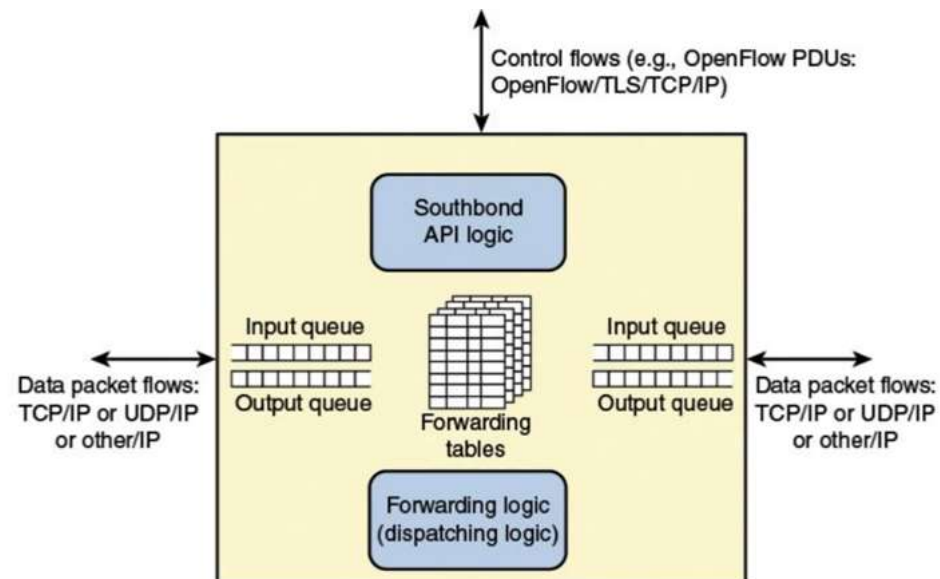
- Composée de 3 couches
- NorthBound Interface:
  - REST API
  - Entre Application et le plan de Contrôle
- SouthBound Interface:
  - Protocole OpenFlow
  - Entre le plan Contrôle et le plan de transfert de données
- Exemple de contrôleur :
  - RYU, OpenDayLight, ONOS, FloodLight, POX, etc.



# ARCHITECTURE SDN

## ○ Plan de Données :

- Éléments Matériels : Switchs, routeurs, Firewalls
- **Flow Tables** : tables détenues par les switchs, qui contiennent des règles et qui déterminent comment traiter le trafic réseau en fonction des politiques définies



# ARCHITECTURE SDN

- Plan de Contrôle (Control Plane) :

- **Contrôleur SDN** : Un logiciel centralisé qui prend en charge la logique de contrôle du réseau.

Il communique avec les éléments matériels du réseau pour définir les politiques de routage, gérer les flux de données et répondre aux changements dans la topologie du réseau.

- **Base de Données de Réseau** : Stocke les informations sur l'état du réseau, la topologie, les adresses IP, etc. Le contrôleur utilise ces informations pour prendre des décisions.

# ARCHITECTURE SDN

- Interface de Programmation Applicative (API) :
  - **Interface Nord (Northbound Interface)** : Permet aux applications ou aux services au-dessus du contrôleur d'interagir avec le plan de contrôle.

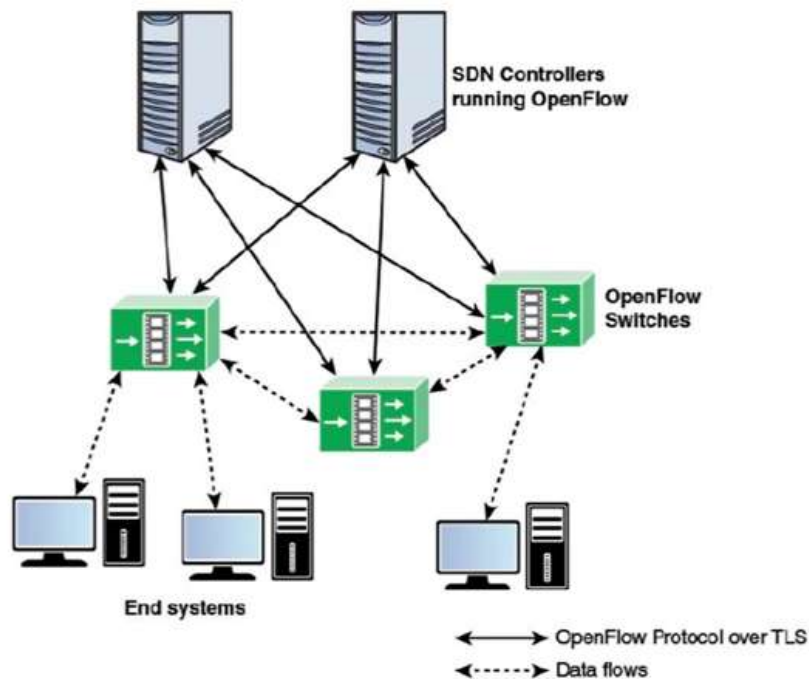
Les développeurs peuvent utiliser cette interface pour créer des applications personnalisées qui contrôlent le réseau en fonction des besoins spécifiques.

- **Interface Sud (Southbound Interface)** : Permet au contrôleur de communiquer avec les éléments matériels du réseau, généralement via des protocoles comme OpenFlow. Cela permet au contrôleur de dicter comment les composants réseau doivent traiter le trafic.



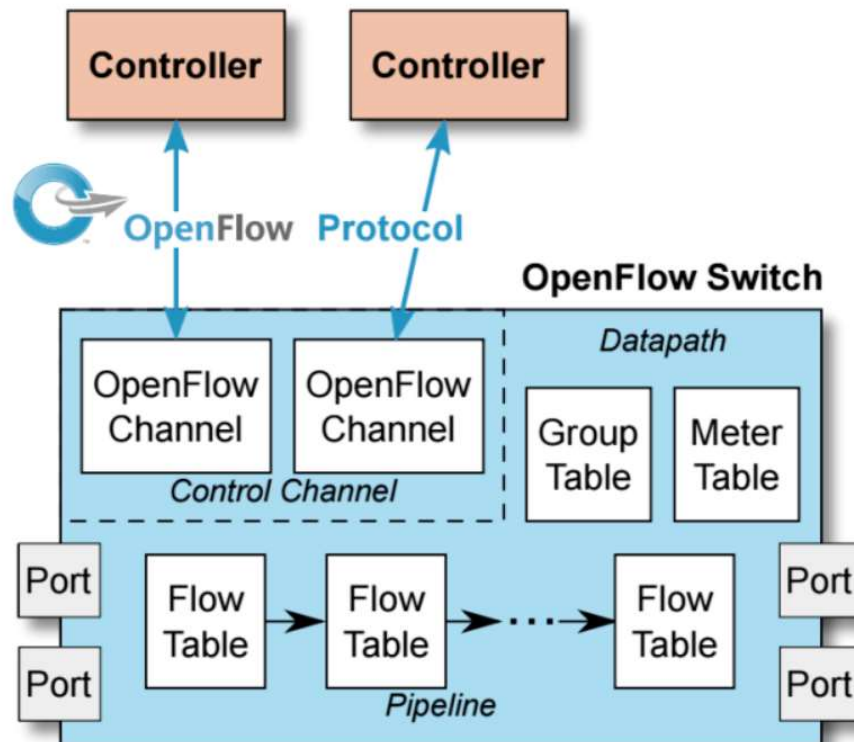
# PROTOCOLE OPENFLOW

- OpenFlow est un protocole de communication qui permet la programmation du comportement des commutateurs de réseau par un contrôleur externe



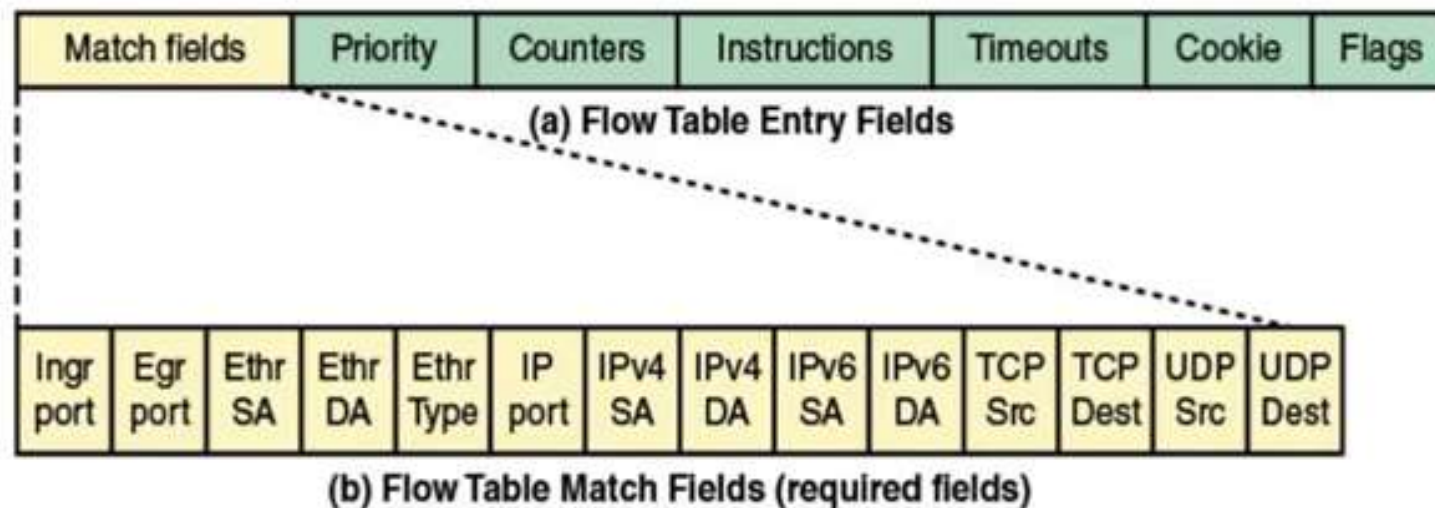
# FLOW TABLES

- OpenFlow Switch : c'est un switch qui détient un ou plusieurs tables de flux « **Flow tables** ».
  - gestion de la commutation des flux de données



## STRUCTURE DE « FLOW TABLE »

- Une entrée de table de flux est identifiée par ses champs « Match fields » et « priority » : ces champs pris ensemble identifient une entrée de flux unique dans une table de flux spécifique.



## STRUCTURE DE « FLOW TABLE »

- **Match Fields** : pour comparer les paquets. Il s'agit du port d'entrée et des en-têtes des paquets, et éventuellement d'autres champs du pipeline tels que les métadonnées spécifiées dans un tableau précédent.
- **priority** : priorité de correspondance de l'entrée de flux.
- **counters** : mis à jour lorsque les paquets sont comparés.
- **instructions** : pour modifier le jeu d'actions ou le traitement du pipeline.

## STRUCTURE DE « FLOW TABLE »

- **timeouts** : durée maximale ou temps d'inactivité avant que le flux ne soit expiré par le commutateur.
- **cookie** : valeur de données opaques choisie par le contrôleur. Peut être utilisé par le contrôleur pour filtrer les entrées de flux affectées par les statistiques de flux, les demandes de modification et de suppression de flux. Il n'est pas utilisé lors du traitement des paquets.
- **flags** : les flags modifient la manière dont les entrées de flux sont gérées ; par exemple, le flag OFPFF\_SEND\_FLOW\_REM déclenche des messages de suppression de flux pour cette entrée de flux.

## STRUCTURE DE « FLOW TABLE »

- L'entrée de flux qui utilise des caractères génériques pour tous les champs de correspondance (tous les champs sont omis) et dont la priorité est égale à 0 est appelée entrée de flux "table-miss".
- L'entrée de flux "**table-miss**" doit au moins prendre en charge l'envoi de paquets au contrôleur à l'aide du port réservé **CONTROLLER**

```
cookie=0x0, duration=12.927s, table=0, n_packets=2, n_bytes=196,  
priority=1, ip, nw_src=192.168.1.1, nw_dst=192.168.1.2 actions=output:"s1-eth2"  
cookie=0x0, duration=12.918s, table=0, n_packets=2, n_bytes=196,  
priority=1, ip, nw_src=192.168.1.2, nw_dst=192.168.1.1 actions=output:"s1-eth1"  
cookie=0x0, duration=12.959s, table=0, n_packets=37, n_bytes=3844, priority=0 actions=CONTROLLER:65535
```

# EXAMPLE

- Comportement du OpenFlow Switch

## Destination-based forwarding:

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	*	*	*	*	51.6.0.8	*	*	*	port6

*IP datagrams destined to IP address 51.6.0.8 should be forwarded to router output port 6*

## Firewall:

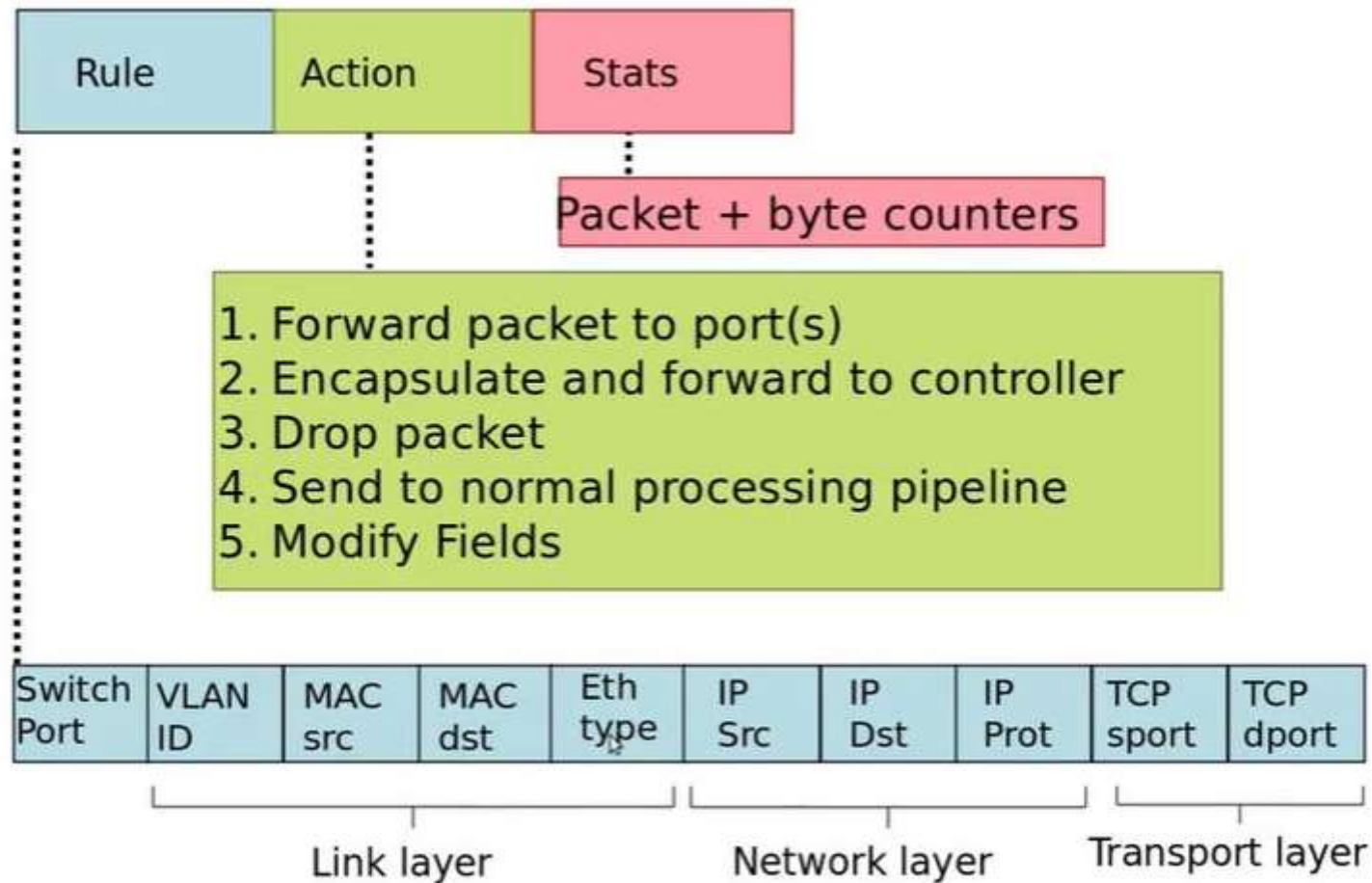
Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Forward
*	*	*	*	*	*	*	*	*	22	drop

*do not forward (block) all datagrams destined to TCP port 22*

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Forward
*	*	*	*	*	128.119.1.1	*	*	*	*	drop

*do not forward (block) all datagrams sent by host 128.119.1.1*

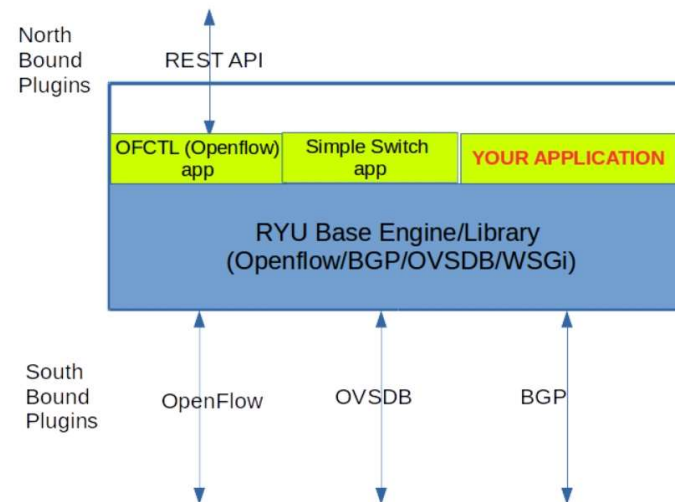
# COMPORTEMENT DE OPENFLOW SWITCH





# RYU CONTROLLER

- Lorsque le nouveau paquet entre dans le switch, s'il ne correspond pas aux flux existants, le switch l'envoie au contrôleur.
- Le contrôleur inspecte le paquet et construit la logique.
- Installe le flux pour cette session (correspondance) dans le commutateur.
- Packet IN/Package OUT

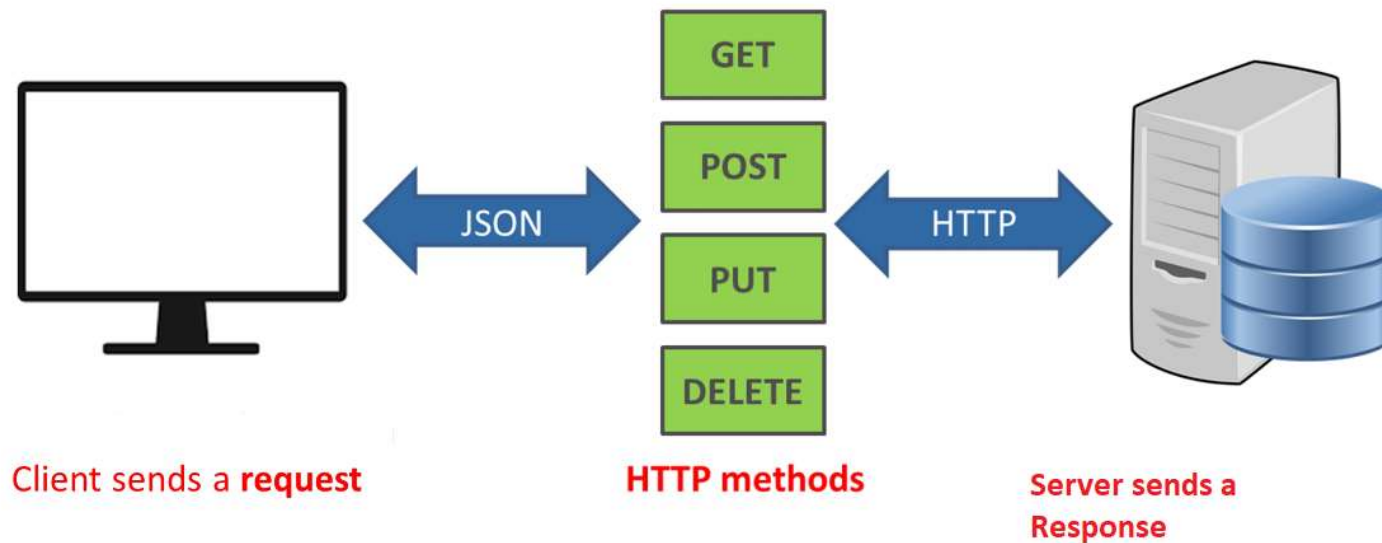


## INTERACTION ENTRE LE SWITCH ET RYU

- Installer « **the Table Miss Entry** » dans le switch
- Lorsque le paquet arrive au switch, il correspond à **the Table Miss Entry**, alors le switch l'envoie au contrôleur (message PACKET IN).
- Le contrôleur recherche le **mac src** du paquet et le met à jour dans sa base de données (**port to mac mapping**).
- Le contrôleur recherche le **mac de destination** du paquet et décide du port de sortie.
- Le contrôleur envoie le paquet au switch (message PACKET OUT)
- Le contrôleur ajoute le flux en utilisant (**FLOW Modification message**), ici le « **match fields** » est basé sur l'adresse MAC.

# REST API

- Une API RESTful est une interface de programme d'application (API) qui utilise des requêtes HTTP pour GET, PUT, POST et DELETE des données.



# REST API

- Les 4 méthodes sont :
  - **GET** : Récupère des données d'un serveur distant. Il peut s'agir d'une seule ressource ou d'une liste de ressources.
  - **POST** : Crée une nouvelle ressource sur le serveur distant.
  - **PUT** : Met à jour les données sur le serveur distant.
  - **DELETE** : Supprime les données du serveur distant.

# OFCTL : RYU.APP.OFCTL APPLICATION

- C'est une application fourni par l'API REST pour **configurer/mettre à jour/supprimer** les **flux/statistiques** des switches

- Exemple :

- récupérer les noms des switches dans le réseau

- `curl -X GET http://localhost:8080/stats/switches`

- `curl -X GET http://localhost:8080/stats/switches`

- `[1, 2, 3, 4]`

- Récupérer les informations existantes dans le flow table su switch 1

- `curl -X GET http://localhost:8080/stats/flow/1`

- Les ports du switch 1

- `curl -X GET http://localhost:8080/stats/port/1`



30

# PROCOTOLE VxLAN

Virtual Extensible LAN

## POURQUOI VXLAN

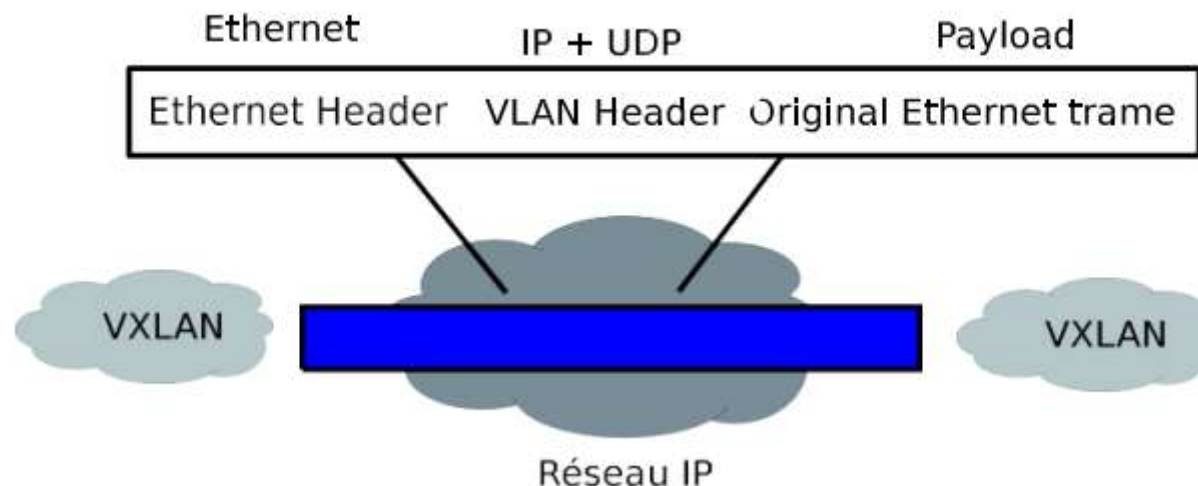
- Le VXLAN est une extension du VLAN de la couche 2. Il a été conçu pour fournir la même fonctionnalité VLAN avec une plus grande extensibilité et flexibilité. Le VXLAN offre les avantages suivants :
- **Flexibilité des VLAN dans les segments** : Il fournit une solution pour étendre les segments de couche 2 sur l'infrastructure réseau sous-jacente afin que la charge de travail puisse être placée sur des serveurs physiques dans le Data Center.

- Amélioration de l'utilisation du réseau : VXLAN a résolu les limitations du STP de la couche 2, table de commutation, nombre limité des VLANs.
  - Les paquets VXLAN sont transférés dans le réseau sous-jacent sur la base de leur en-tête de couche 3 et peuvent tirer pleinement parti du routage de couche 3 et des protocoles d'agrégation de liens pour utiliser tous les chemins disponibles.
- Une meilleure évolutivité : VXLAN utilise un identifiant de segment de 24 bits appelé identifiant de réseau VXLAN (VNID), ce qui permet de faire coexister jusqu'à 16 millions de segments VXLAN dans le même domaine administratif.



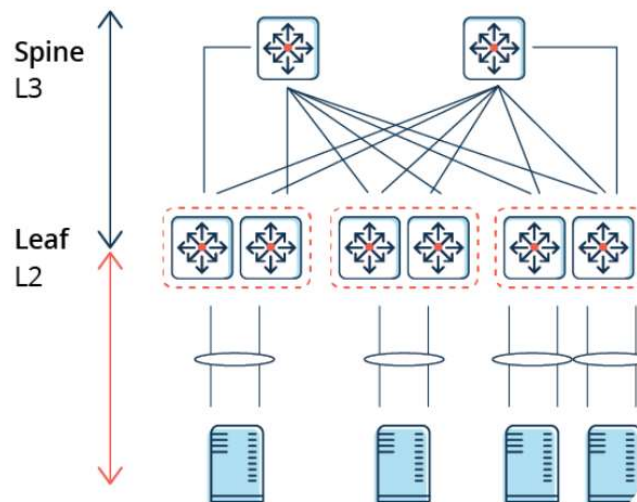
# FONCTIONNEMENT

- On veut pouvoir déployer un réseau Ethernet sur un ensemble de sous-réseaux IP
- Cette communication doit pouvoir se faire au travers d'un réseau overlay
- Par conséquent, la trame Ethernet est :
  - Encapsulée dans un segment UDP, lui-même encapsulé dans un paquet IP, lui-même encapsulé dans une trame Niveau 2 (Ethernet par ex)



# VxLAN : TOPOLOGIE

- Architecture : Spine Layer, Leaf layer
- La couche Spine : est utilisée pour le transport. Les équipements « leaf » sont les seuls à se connecter aux équipements « Spine » via des liens routés.
- La couche Leaf est celle où les hôtes et les autres périphériques se connectent. Elle gère toutes les fonctions VxLAN, comme la création des réseaux virtuels et le mappage des VLAN aux VNI.

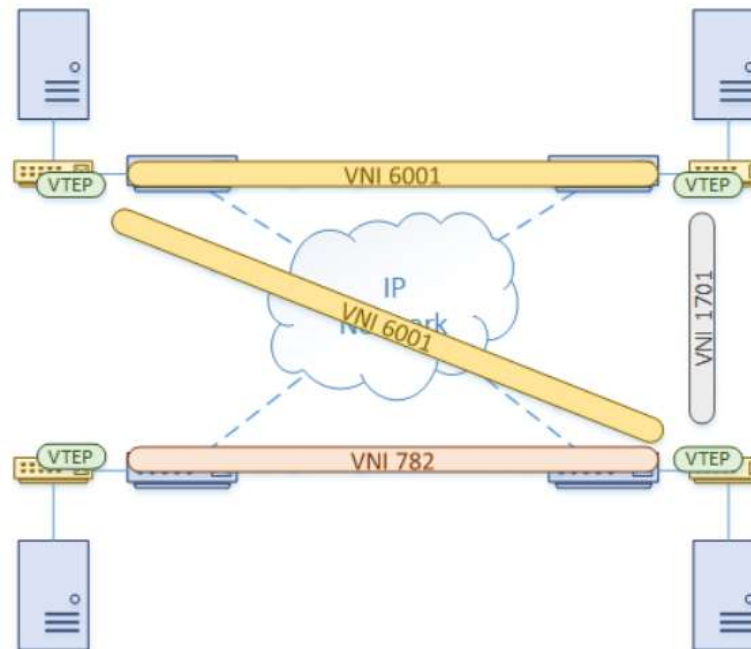


## TERMINOLOGIE

- **VTEP** : un point d'entrée dans un VxLAN
- La tâche de VTEP est d'encapsuler/désencapsuler les entêtes VxLAN
- Le VTEP peut être une application virtuelle ou un équipement réseau (Routeur cisco csr1000k, cisco Switch Nexus9)

# TERMINOLOGIE

- VTI et VNI
- VTI : Interface IP utilisée comme adresse IP source pour encapsuler le trafic VXLAN
- VNI : Un champs de 24 bits ajouté dans le header VXLAN. C'est l'Equivalent du VLAN ID dans le monde Ethernet



# FONCTIONNEMENT



1. Une trame arrive sur un port de commutateur à partir d'un hôte. Ce port est un port (d'accès) non balisé régulier, qui attribue un VLAN au trafic
2. Le commutateur détermine que la trame doit être transférée vers un autre emplacement. Le commutateur distant est connecté par un réseau IP. Il peut être proche ou à plusieurs sauts
3. Le VLAN est associé à un VNI, donc un en-tête VxLAN est appliqué. Le VTEP encapsule le trafic dans les en-têtes UDP et IP. Le port UDP 4789 est utilisé comme port de destination. Le trafic est envoyé sur le réseau IP
4. Le commutateur distant reçoit le paquet et le décapsule. Une trame de couche 2 régulière avec un ID VLAN est laissée
5. Le commutateur sélectionne un port de sortie pour envoyer la trame. Ceci est basé sur les recherches MAC normales. Le reste du processus est normal.

# CONFIGURATION

- Spine :
- Création d'une interface loopback, et activation de protocole de routage multicast et Ospf
  - ip pim sparse-mode
  - ip ospf X area 0
- Configuration des interfaces physiques et activation de routage multicast et ospf
- Choix de point de rendez-vous
  - ip pim bidir-enable
  - ip pim rp-address x.x.x.x
  - ip pim bsr-candidate loopback0

# CONFIGURATION

- Leaf:
- la première partie de configuration est similaire à celle des routeurs « Spine »
- Configuration de VTEP:
  - Création d'une interface « nve » (network virtualization endpoint) et la mapper avec Virtual Network Identifier (VNI) et le groupe multicast

```
interface nve1
no ip address
source-interface Loopback0
member vni 6010 mcast-group 239.0.60.10
```

- Configuration de l'interface physique rattachée au réseau LAN, afin de créer une interface overlay

```
no ip address
service instance 1 ethernet
encapsulation untagged
```

# CONFIGURATION

- Création du « domain-bridge » et l'associe au « service instance »

```
bridge-domain 1  
  member vni 6010  
  member GigabitEthernet3 service-instance 1
```



# SD-WAN

Software-Defined Wide-Area Network

# POURQUOI SD-WAN

- Rôle des réseaux WANs : connecté les utilisateurs à leurs entreprises, campus ou serveurs dans les Data Center.
- La commutation de circuit qui assure fiabilité et sécurité n'est plus adéquate en présence :
  - De mobilité des utilisateurs
  - Hébergement des applications dans les Clouds : explosion de la bande passante, temps de latence plus élevé
- L'utilisation du haut débit sur le réseau WAN rend les exigences de sécurité encore plus strictes.
  - Pose des problèmes : sécurité et défaillance (pannes ou saturation).



# SD-WAN

- SD-WAN : technologie qui offre un accès multi-réseaux
  - MPLS, FTTH, Boucle local, xDSL, 4G/5G
- Approche Centralisée pour gérer la gestion de réseaux :
  - Plan de gestion
  - Plan de contrôle
  - Plan de données (Forwarding plane)
- Réseau centralisé intelligent :
  - Plus d'automatisation
  - Simplification des opérations de configuration réseaux
  - Monitoring et détection de défaillances



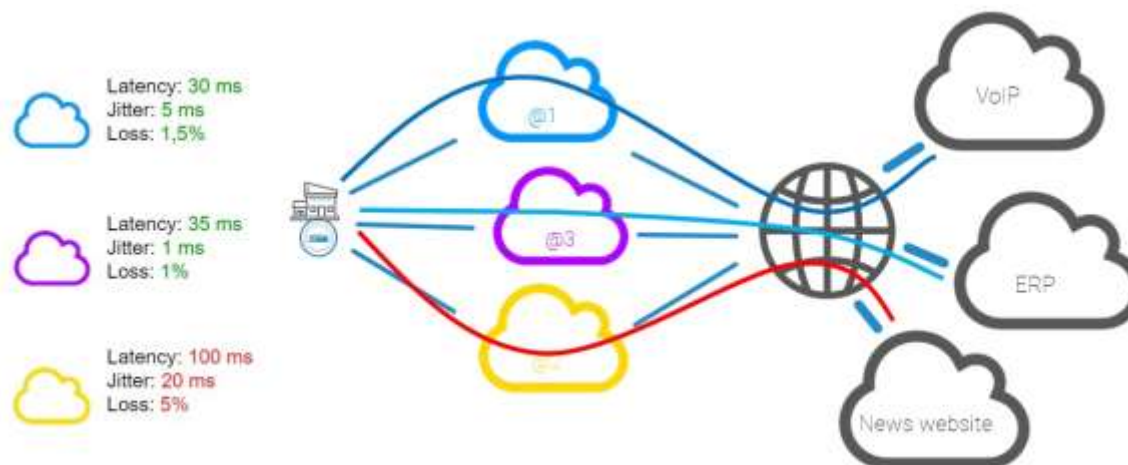
## SD-WAN : AVANTAGE

- Augmentation de la bande passante par l'activation de liens de secours inactifs et l'équilibrage dynamique des charges
- Fournir un accès plus rapide permettant un accès direct aux succursales
- Réduire les coûts opérationnels et de gestion grâce à une gestion centralisée
- Réduction des coûts du WAN grâce à l'utilisation d'une connectivité internet ou LTE moins chère comme alternative au réseau MPLS
- Une sécurité multicouche qui offre la souplesse nécessaire pour déployer la bonne sécurité au bon endroit: soit sur site, soit dans le cloud



# SD-WAN : FONCTIONNEMENT

- Le SD-WAN (Software Defined Wide Area Network) est un ensemble de fonctionnalités logicielles permettant de faciliter la gestion de réseaux interconnectés et sécurisés ainsi que la gestion de liens WAN multiples.
- Une des approches fonctionnelles du SD-WAN consiste à choisir de manière automatique et transparente les liens réseau à emprunter selon les flux et leurs contraintes de performances associées (latence acceptée, taux de disponibilité...).



# PARAMÈTRES D'ÉVALUATION

## ○ Paramètres de supervision

- Méthode de détection
  - TCP Probe: cette méthode est basée sur des requêtes vers le port TCP utilisé par le serveur applicatif à joindre
  - ICMP : : cette méthode est basée sur l'envoi régulier de paquets de type ICMP Request sur chaque lien
- Délai d'expiration
  - Il s'agit du délai maximal attendu pour une réponse à une tentative de connexion avec la méthode de détection choisie
- Intervalle de tests
  - Il s'agit du laps de temps qui s'écoule entre deux tentatives de connexion.
- Echecs avant dégradation
  - Il s'agit du nombre maximal de tentatives de connexion échouées avant de déclarer que l'objet cible est injoignable ou que le lien est dégradé

# PARAMÈTRES D'ÉVALUATION

- les métriques du SLA SD-WAN
  - La latence :
    - La notion de latence SD-WAN représente le temps écoulé entre l'envoi d'un paquet et la réception d'une réponse à celui-ci. Il s'agit donc réellement d'une notion de RTT (round-trip time)
  - La gigue :
    - représente la variation de la latence au cours du temps. Elle est calculée par rapport à toutes les valeurs de latence mesurée au cours des 10 dernières minutes
  - Taux de perte de paquets :
    - Il s'agit du ratio entre le nombre de requêtes de connexion émises et le nombre de réponses reçues.
  - Taux d'indisponibilité:
    - Il s'agit du ratio entre le temps où une passerelle est disponible et le temps pendant lequel elle a été inaccessible.