Cours 59 : Automatisation Réseau

Dans ce cours nous verrons l'automatisation du réseau, tout d'abord nous verrons pourquoi utiliser l'automatisation d'un réseau et les bénéfices à l'utiliser. Puis nous ferons un plan logique des fonctions du réseau (Plan de donnée, plan de contrôle, plan de gestion).
Et nous verrons ce qu'est le Software-define networking (SDN), les APIs et la sérialisation des données.

Il est important d'avoir une connaissance basique sur l'automatisation du réseau. Dans un modèle traditionnel, les ingénieurs gèrent les appareils un à un en se connectant à leur CLI (Command Line Interface) Par SSH. Il y a certains inconvénients de configurer des appareils un à un :
- De simple petites erreurs peuvent être présentes.
- Cela prend du temps et est très inéfficace dans de grands réseaux.
- Il est difficile de s'assurer que tous les appareils adèrent bien aux standard de configurations de l'entreprise.

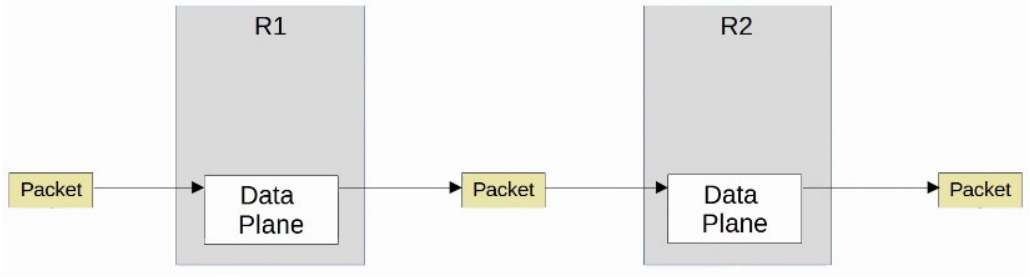
L'automatisation des réseaux offre plusieurs avantages :
- Les erreurs Humaines sont réduites (configurations, etc.)
- Les réseaux deviennent plus évoluable. Les nouveaux déploiements, changement de grand réseau, et réglage de problèmes peut être implémenté dans une fraction du temps.
- Les politique de réseau peuvent être assurés (Configuration de standard, version logiciel, etc.)
- L'efficacité amélioré des opération du réseau réduisent les coûts du réseau car chaque tâche peut demander plusieurs heures par personne.

Il existe une grande varité d'outils et de méthodes pouvant être utilisé pour automatiser des tâches dans le réseau :
- SDN
- Ansible
- Puppet
- Script Python
- etc...

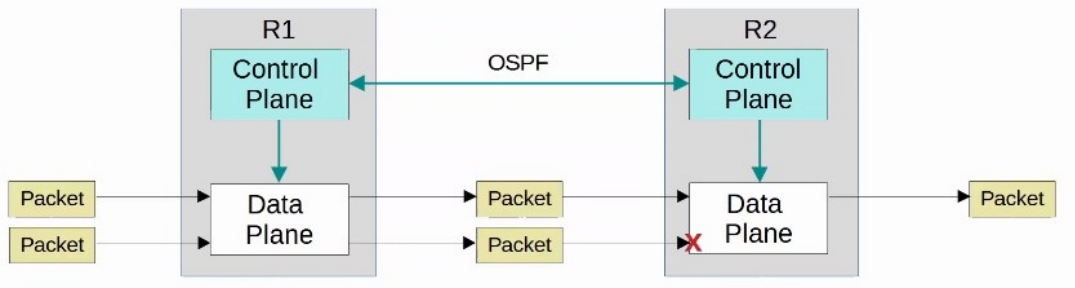
Pour automatiser un réseau il nous faut établir un plan logique des appareils.
Qu'est ce qu'un Routeur fait ?
Il transmet les messages entre les réseaux en examinant les information de l'entête de couche 3. Il utilise un protocole comme OSPF pour partager le routage de l'information avec d'autres routeurs et construire une table de routage.
Il utilise ARP pour construire une table ARP, en cartographiant les adresses IP et les adresses MAC.
Il utilise Syslog pour garder les logs des évènements qui se passent.
Il permet à un utilisateur de se connecter par SSH et de gérer.

Qu'est ce qu'un Switch fait ?
Il transmet les messages d'un LAN en examinant l'information dans l'entête de couche 2.
Il utilise STP pour s'assurer qu'il n'y a pas de boucle de couche 2 dans le réseau.
Il construit une table d'adresse MAC en examinant les trames des adresses MAC source.
Il utilise Syslog pour garder les logs des évènements qui se passent.
Il permet à un utilisateur de se connecter par SSH et de gérer.

Les fonctionnalités des appareils d'un réseau peuvent être divisés logiquement (et catégorisés) en des plans :
- Le plan de données : Toutes les tâches impliqués dans le partage/trafique des données de l'utilisateur depuis une interface vers une autre font partie du plan des données.
Un routeur qui reçoit un message, regarde la route qui correspond le plus à sa table de routage, et le transmet à l'interface la plus approprié pour le prochain bond. Il désencapsule l'entête original de couche 2, et la réencapsule avec une nouvelle entête destiné pour le prochain bond d'adresse MAC. Le Switch reçoit le message, et regarde l'adresse MAC de destination, et le partage en dehors de l'interface approprié (Ou bien inonde le réseau). Cela inclut des fonctions comme ajouter ou supprimer des balises 802.1q VLAN. Le NAT (Change l'adresse source/destination avant de transmettre le message) cela fait aussi partie du plan des données.
Décider de transmettre ou bloquer les messages à cause d'une ACLs, port Security, etc.. fait aussi partie du plan des données. Le plan de données est aussi appelé le « plan de transmission ».
Cela fonctionne comme sur le schéma ci dessous :

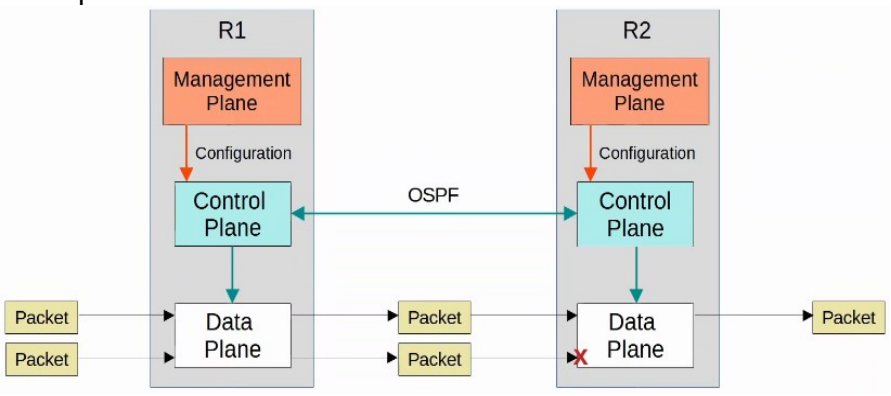


- Le plan de contrôle : Ce plan permet de répondre à comment un le plan de données d'un appareil faire pour transmettre ses décisions. Avec les tables de routage, les adresses MAC, les tables ARP, STP, etc... Les fonctions qui construisent ces tables (et d'autres fonctions qui influencent le plan de données) dont partie du plan de contrôle. Le plan de contrôle, contrôle ce que le plan de donnée fait par exemple en construisant la table de routage d'un routeur. Le plan de contrôle fait un travail « aerien » par exemple si OSPF ne transmet pas les paquets de données à un utilisateur, mais il informe le place de données comment les paquets devraient être transmis. Si STP n'est pas directement impliqué dans le processus de transmission des trames, mais il informe le plan de données à propos de quelles interface devrait ou ne devraient pas être utilisés pour partager les trames transmises. Les messages ARP ne sont pas des données utilisateurs, mais ils sont utilisé pour construire une table ARP qui est utilisé dans le processus de transmission de données.
Cela fonctionne comme sur le schéma suivant :



Dans un réseau traditionnel, le plan de donnée et le plan de contrôle sont tout les deux distribués. Chaque appareils à ses propres plans de données et ses propre plan de contrôle. Les plans sont distribués sur le réseau.

- Le plan de gestion : Tout comme le plan de contrôle, le plan de gestion fait un travail « aerien ».
Le plan de gestion n'affecte pas directement le transfert des messages dans le plan de données.
Le plan de gestion consiste dans l'utilisation de protocoles qui sont utilisés pour gérer les appareils. Comme par exemple SSH/Telnet, utilisés pour se connecter au CLI d'un appareil pour le configurer ou le gérer. Ou bien Syslog utilisé pour garder les logs des évènements qui se passent sur l'appareil. SNMP utilisé pour monitorer les opérations de l'appareil. NTP est utilisé pour maintenir un temps précis sur l'appareil.
Cela peut se résumer par le schéma suivant :



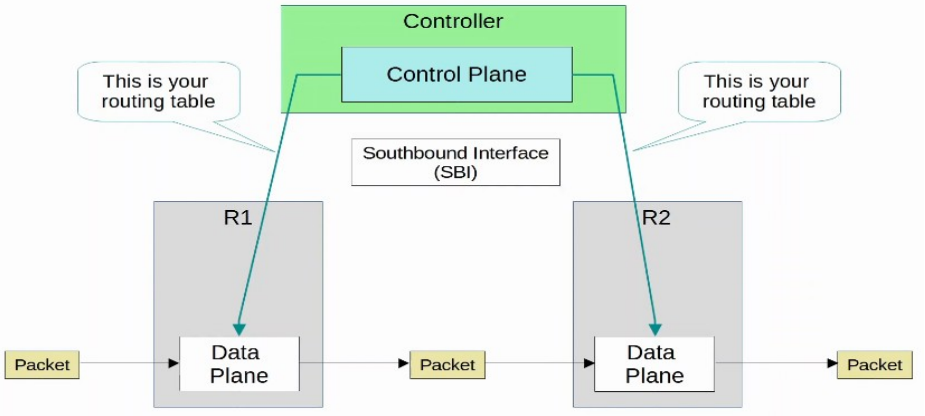
Le plan de donnée est la raison pour laquelle l'on achète des routeurs et des Switchs (et des infrastructure réseau en général), pour transmettre les messages. Seulement le plan de contrôle et de gestion sont tout deux nécessaire pour que le plan de donnée fasse correctement son travail.

Les opérations de gestion et de contrôle sont géré par le CPU. Cela n'est pas utile pour les opérations du plan de donnée car le fonctionnement du CPU est lent. Au lieu de cela du matériel spécialisé ASIC (Application-Specific Integrated Circuit) est utilisé. ASICs sont des puces construits dans cette interêt spécifique.
En voici une image :

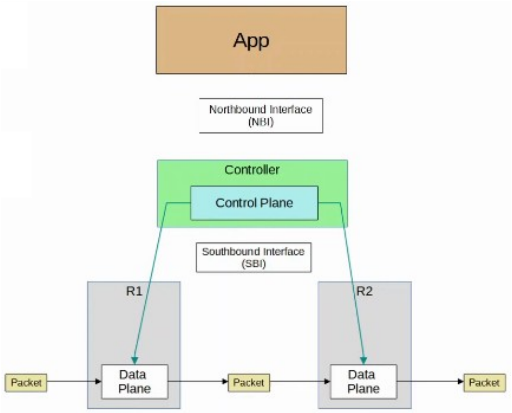
En utilisant un Switch comme exemple :
Lorsque la trame est reçu, le ASIC (Non pas le CPU) est responsable de la logique de Switching.
La table Adresse MAC est stocké dans une sorte de mémoire appelé TCAM (Ternary Content-Addressable Memory).
Un autre nom commun pour les adresses MAC est table CAM.
Le ASIC alimente l'adresse MAC de destination de la trame dans la TCAM, qui retourne une adresse MAC correspondant à l'entrée de l'adresse MAC.
La trame est ensuite transmise en dehors vers l'interface approprié.
Les routeurs modernes utilisent aussi du matériel similaire dans le plan de donnée : Un ASIC est désigné pour la transmission logique, et des tables stockés dans le TCAM.

Pour résumer, lorsqu'un appareil reçoit un trafique de contrôle/gestion (destiné à lui même) il va utiliser le CPU. Lorsqu'un appareil reçoit le trafique de données qui devrait passer par l'appareil, il utilisé ASIC pour une meilleure rapidité.

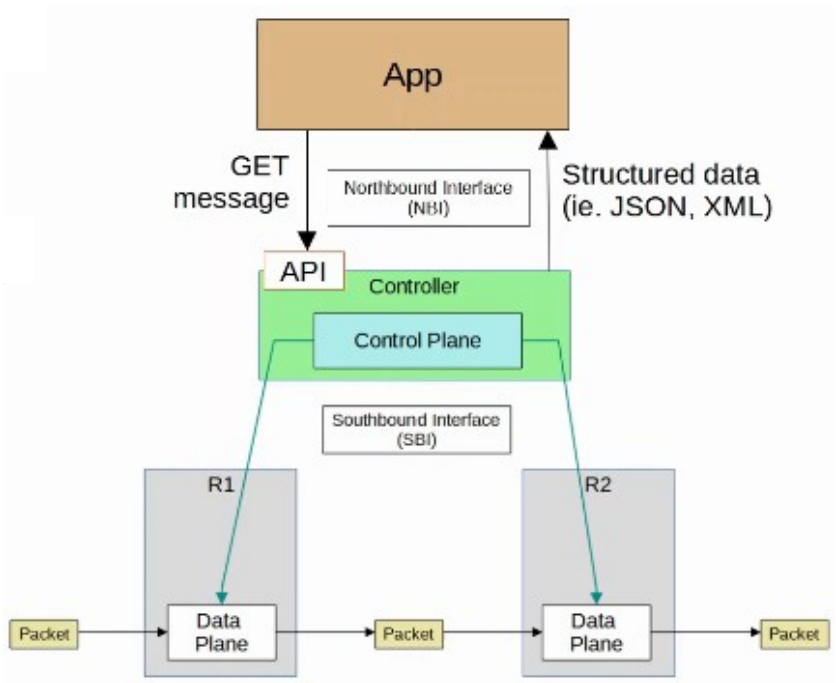
Voyons le concept des SDN pour Software-Defined Networking. Il s'agit d'une approche des réseaux qui centralise le plan de contrôle dans une application appelé controlleur.
Ce concept est similaire à celui déjà appris qui concerne les WLAN.
Le SDN est aussi appelé Software-Defined Architecture (SDA) our Controller-Based Networking.
Le plan de contrôle traditionnel utilisé une architecture distribué.
Par exemple chaque routeur dans un réseau lance OSPF et les routeurs partagent leur information de routage et calcule ensuite leurs route préféré pour chaque destination.
Un controlleur SDN centralise les fontions du plan de contrôle comme le calcule du routage.
Cela est juste un exemple de combien le plan de contrôle varie.
Le controlleur peut intéragir de manière programmé avec les appareils du réseau en utilisant des API (Application Programming Interface).
Voici un schéma qui permet de résumer :



Le Southbound Interface (SBI) est utilisé pour la communication entre le controlleur et les appareils du réseau qu'il controle. Cela consiste en général de l'utilisation d'un protocole de communication et d'un API (Application Programming Interface). Les API facilitent l'échange de données entre des programmes. Les données sont échangés entre le controlleur et les appareils du réseau.
Un API sur les appareils du réseau permettent au controlleur d'accéder aux informations sur un appareil, il contrôle leur table de plan de données, etc.
En utilisant le SBI, le controlleur communique avec les appareils géré et recueille des informations à propos d'eux, par exemple les appareils présent sur le réseau, la topologie (Comment les appareils sont connectés entre eux), les interfaces disponibles sur chaque appareil, leurs configurations.
Le Northbound Interface (NBI) est ce qui permet d'intéragir avec le controleur, d'accéder aux données qu'il recueille à propos du réseau, il le programmen et fait des changements dans le réseau via SBI.
Cela peut se résumer par le schéma suivant :



Le REST API est utilisé sur le controlleur comme interface pour que les applis interagisse avec lui.
REST est l'acronyme de Representational State Transfer
Les données sont envoyés dans un format structurés (Sérialisé) comme JASON ou XML.
Le schéma suivant résume cela :



Cela rend plus facile l'utilisation des données pour les programmes.

Voyons un comparatif de l'automatisation des réseaux traditionnels et des SDN.
Les tâches de réseaux peuvent être automatisés dans une architecture réseau traditionnel aussi :
Avec des script pouvant être écris (en utilisant Python par exemple) pour envoyer des commandes à plusieurs appareils en même temps.
La bonne utilisation de Python pour des Expression Régulière peut analyser par la commande « show » pour recueillir des informations à propos des appareils du réseau.
Le résultat de la commande « show » permet de comprendre facilement :

```
Switch#show interfaces
GigabitEthernet0/0 is up, line protocol is up (connected)
  Hardware is iGbE, address is 0cb0.28f6.5500 (bia 0cb0.28f6.5500)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Unknown, Unknown, link type is auto, media type is unknown media type
  output flow-control is unsupported, input flow-control is unsupported
  Auto-duplex, Auto-speed, link type is auto, media type is unknown
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     83 packets input, 8576 bytes, 0 no buffer
     Received 82 broadcasts (82 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 82 multicast, 0 pause input
     54 packets output, 7221 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

La centralisation robuste des données collectés par les controlleurs SDN facilite grandement ces fonctions. Le controlleur collecte l'information à propos de tous les appareil du réseau.
Les API Northbound permettent aux applications d'accéder aux informations dans un format facile à comprendre pour les programmes (Comme par exemple JSON, XML).
La centralisation des données facilite l'analyse large du réseau.
Les outils SDN peuvent fournir des bénéfices d'automatisation sans que cela requière des scripts ou applications.
Il n'est plus nécessaire d'être expert dans l'automatisation pour utiliser des outils SDN.
Les API permettent tout de même aux application tiers d'intéragir avec le contrôlleur, qui peut être très puissant. SDN et l'automatisation ne sont pas les même choses, les architectures SDN facilitent grandement l'automatisation de tâches variés dans le réseau par des controlleurs SDN et des API.