Administrer

```
Bastien Helec
Semestre 3 et 4
Ressources associées a la compétences Administrer :
- R301 : AC 21.01 AC 21.02
- R302 : AC 21.05
- R303 : AC 21.03 AC 21.04
- R304 : AC 21.03 AC 21.04
- R311 : AC 21.02 AC 21.06
- R312 : AC 21.06
- R313 : AC 21.01 AC 21.02 AC 21.03 AC 21.04 AC 21.05 AC 21.06
- R315 : AC 21.06
- SAE 3.02: AC 21.06
- SAE 3.Devcloud.03: AC 21.01 AC 21.02 AC 21.03 AC 21.04 AC 21.05 AC 21.06
- Portfolio : AC 21.01 AC 21.02 AC 21.03 AC 21.04 AC 21.05 AC 21.06
```

Sommaire

les liens en dessus sont clickable et renvoi vers les démonstrations correspondantes

Introduction : Rappel de la compétence Administrer

Retour au sommaire

La compétence Administrer à pour objectif d'administrer et de concevoir un réseau. Les apprentissages attendus sont :

- AC 21.01 : Configurer et dépanner le routage dynamique dans un réseau
- AC 21.02 : Configurer et expliquer une politique simple de QoS et les fonctions de base de la sécurité d'un réseau
- AC 21.03 : Déployer des postes clients et des solutions virtualisées adaptées à une situation donnée
- AC 21.04 : Déployer des services réseaux avancés
- AC 21.05 : Identifier les réseaux opérateurs et l'architecture d'Internet
- AC 21.06 : Travailler en équipe pour développer ses compétences professionnelles

Celle-ci demande de savoir en situation professionnelle :

- Concevoir et administrer l'infrastructure du réseau informatique d'une entreprise
- Installer et administrer les services réseaux informatiques d'une entreprise
- Déployer et administrer des solutions fixes pour les clients d'un opérateur de télécommunication
- Gestion des postes clients
- Utilisation des technologies de virtualisations

Demandant ainsi au futur professionnel de repondre au composantes essentielles suivantes :

- Choisir les solutions et téchnologies adaptées à la situation
- Réspecter les principes fondamenteaux de la sécurité informatiques
- Utiliser une approche rigoureuse pour la résolution des dysfonctionnements
- Respecter les règles métiers
- Assurer une veille technologique
- Communiquer avec les clients et le differents acteurs impliqués
- Utiliser une approche rigoureuse et methodique (démarche scientifique)

Le niveau attendu en fin d'année:

Retour au sommaire

Selon moi le niveau attendu en fin d'année pour la compétence Administrer est de savoir concevoir un réseau en le créant de A à Z de le dimensionner en fonction du cahier des charges , de le configurer et de le dépanner. Ainsi que pouvoir assurer le bon fonctionnement des équipements lié a l'utilisation d'internet et a l'entreprise :

- Les equipements réseaux (routeurs, switchs, firewall, etc...)
- Les equipements de virtualisations (serveurs, hyperviseurs, etc...)
- Les équipements clients (ordinateurs, tablettes, smartphones, etc...)

Tout ce travail doit être effectuer en réalisant de la documentation et pouvoir obtenir des trâces de ce qui a été fait pour pouvoir le reproduire ou le modifier si besoin s'en avoir a tout redimensionner et ainsi pouvoir communiquer et travailler en équipe.

Mon niveau actuel :

Retour au sommaire

Je pense mon niveau dans la compétence Administrer correspond au niveau attendu en fin d'année. Malgrès certain défauts lié à une documentation trop differentes d'un projet ou d'un rendu à l'autre et ainsi devoir tout reprendre depuis le début.

Je pense que mon niveau est bon car j'ai pu mettre en place des réseaux avec des protocoles de routage dynamique (BGP,OSPF,EIGRP,IBGP,RIP) pouvoir mettre en place des loopback et des VLAN, j'ai tendance a observer que le réseau suis bien la demande en appliquant du QoS de manière manuel (verification humaine), ainsi que le deploiement sans problème d'un serveur a l'autre en verifiant les adresses IP occupé ou les réseaux occupé avec nmap, puis verifier le bon fonctionnement en utilisant des outils comme ping, traceroute, mtr, etc...

Puis surtout j'ai pris l'habitude de réaliser l'administration système sur des conteneurs ou sur des machines virtuels dans un premier temps de part ma distribution de celle demander : Fedora. Mais aussi pour me permettre de garder un ordinateur sein et ainsi ne pas avoir des problèmes differents d'un projet à l'autre, ce qui m'arrivais trop souvent en première année.

De plus aujourd'hui je communique auprès des premières années des conseils pour pouvoir permettre de ne pas se retrouver dans la difficulté que j'ai pu avoir en première année.

Avec l'experience obtenu en deuxieme année avec les SAE clouds, j'ai pu mettre en place des infrastructures plus complexe tout comme en interne avoir mis en place une infrastructure chez moi.

Ce que je prevois de faire pour améliorer mon niveau :

Retour au sommaire

Je prevois de me renseigner plus sur les documentations des differents protocoles de routage dynamique comme par exemple les RFC du BGP , du RIP etc afin des les comprendres et pouvoir ainsi utiliser tout le potentiel associés au ceux-ci.

Je pense aussi réaliser des infrastructures toujours plus complexe en me permettant de mettre en pratique toutes les informations que j'aurais apprise auprès des documentations, Et donc ainsi réaliser moi meme une documentation sous forme de tutoriel.

Ce que j'ai réaliser :

Introduction :

Dans cette AC je doit ainsi prouver que je suis capable de configurer et donc de depanner le routage dynamique dans un réseau.

Grâce au cours exploiter durant le S3, mon stage et S4 et ma premiere année de formation R&T, j'ai pu apprendre a configurer et depanner des routeurs et des switchs Cisco et mikrotik.

Mais également de configurer les ordinateurs clients et serveurs pour qu'ils puissent correspondre au besoin demander.

Les protocoles de routage dynamique :

Dans ma formation nous avons pu voir les protocoles de routage dynamique suivant elle utilise ainsi la couches transport du modèle OSI :

- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)
- EIGRP (Enhanced Interior Gateway Routing Protocol)
- BGP (Border Gateway Protocol)
- STP (Spanning Tree Protocol)

Definitions :

- **RIP** : Le protocole RIP est un protocole de routage. Il utilise le nombre de sauts comme métrique. Il est limité à 15 sauts. Il est donc utilisé pour des réseaux de petite taille. Il est très simple à configurer et à déployer. Il est très peu utilisé de nos jours, sa sécurité est très faible et il est très lent à converger.

- **OSPF** : Le protocole OSPF est un protocole de routage créer par Cisco à état de lien. Il utilise la bande passante comme métrique. Il est utilisé pour des réseaux de taille moyenne à grande. Il est plus complexe à configurer et à déployer que RIP. Il est plus sécurisé et plus rapide à converger de part l'utilisation de l'algorithme de Dijkstra.

- **EIGRP** : Le protocole EIGRP est un protocole de routage. Il utilise la bande passante et la charge comme métrique. Il est utilisé pour des réseaux de taille moyenne à grande. Il est plus complexe à configurer et à déployer que RIP. Il est plus sécurisé et plus rapide à converger de part l'utilisation de l'algorithme de Dijkstra

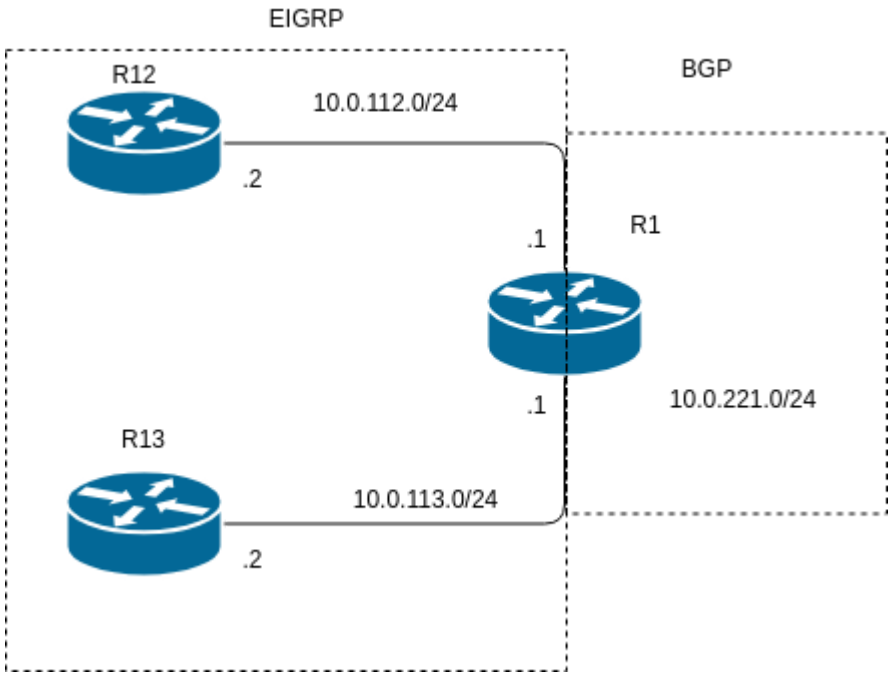
- **BGP** : Le protocole BGP est un protocole de routage. Il utilise la bande passante et la charge comme métrique. Il est utilisé pour des réseaux de taille moyenne à grande. Il est plus complexe à configurer et à déployer que RIP. Il est plus sécurisé et plus rapide à converger de part l'utilisation de l'algorithme de Dijkstra. De plus il utilise le système d'autonomie (AS) pour définir les routes, ainsi celle-ci permettent de definir plusieurs réseaux dans une meme zone et ainsi de pouvoir faire de l'agrégation de routes. J'ajouterais aussi que la configuration BGP permet de faire des redistribution de routes entre les protocoles de routage dynamique pour permettre de voir apparaitres que certains réseau soit sur d'autre AS ou bien utilise d'autre protocole de routage.

- **STP** : Le protocole STP est un protocole qui a pour but d'éviter les bouclages réseaux et ainsi limité le calcul du switch, ce n'est pas a proprement parlait un protocole de routage mais est très utile pour depanner et configurer un routage dynamique.

Démonstration de mes compétences :

- Configuration est mise en place d'un réseau avec EIGRP : Dans le contexte de la formation dans la ressource R302 j'ai pu mettre en place via l'application GNS3 un réseau interne avec le protocole EIGRP et utiliser l'attributs **weight** pour le BGP qui nous permet de choisir la route que l'on souhaite utiliser :

Tout d'abord j'ai mis en place le réseau suivant :



Puis on a configurer les routeurs de cette manière :

```
R12(config)# interface FastEthernet0/0
R12(config-if)# ip address 10.0.112.2 255.255.255.0
R12(config-if)# no shutdown
R12(config-if)# exit
R12(config)# do write memory
R12(config)# router eigrp 100
R12(config-router)# network 0.0.0.0 255.255.255.255
R12(config-router)# exit
R12(config)# do write memory
```

Ici on a configurer le routeur R12 avec une adresse IP et le protocole eigrp avec le numéro de l'AS 100. J'ai terminer par sauvegarder la configuration.

Les mêmes commandes ont été effectuées sur les autres routeurs en changeant l'adresse IP de l'interface FastEthernet0/0. Sauf R1 qui a été configurer en BGP

Pour etres sur que cela fonctionne nous avons effectuer un `show ip route` sur le routeur R12 :

```
show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
```

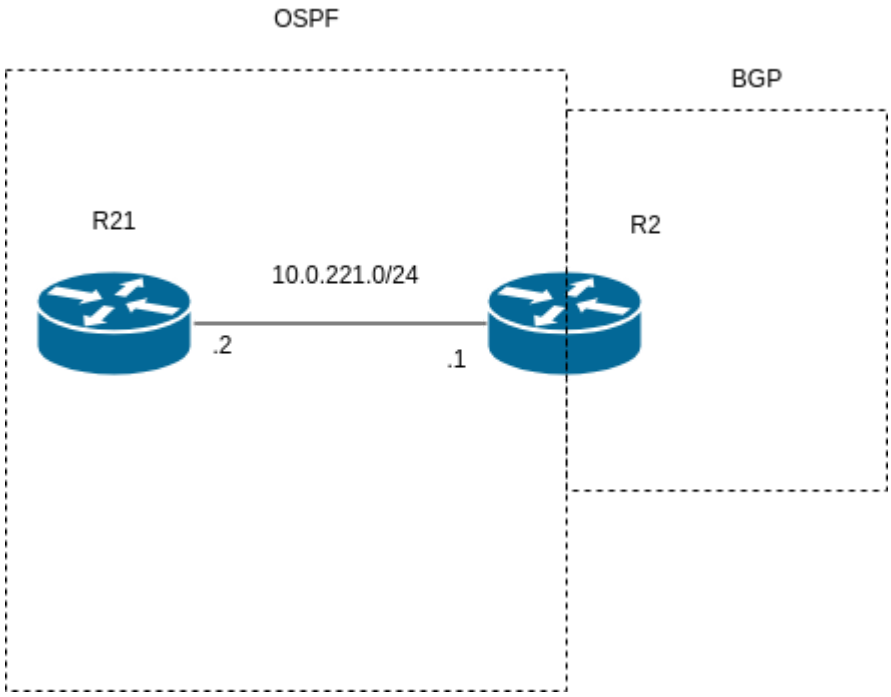
```
     100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       100.0.0.0/8 is a summary, 00:30:36, Null0
C       100.1.0.0/24 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
D       10.0.14.0/24 [90/30720] via 10.0.112.1, 00:30:36, FastEthernet0/0
D       10.0.12.0/24 [90/30720] via 10.0.112.1, 00:30:36, FastEthernet0/0
D       10.0.0.0/8 is a summary, 00:30:37, Null0
D EX    10.0.23.0/24 [170/25602816] via 10.0.112.1, 00:30:36,
FastEthernet0/0
C       10.0.112.0/24 is directly connected, FastEthernet0/0
D       10.0.113.0/24 [90/30720] via 10.0.112.1, 00:30:39, FastEthernet0/0
D EX    10.0.221.0/24 [170/25602816] via 10.0.112.1, 00:30:39,
FastEthernet0/0
```

On peut voir que le réseau et bien détecter en EIGRP et que les routeurs sont bien connecter entre eux.

- Configuration est mise en place d'un réseau avec OSPF :

Dans le contexte de la formation dans la ressource R302 j'ai pu mettre en place via l'application GNS3 un réseau interne avec le protocole OSPF :

Tout d'abord j'ai mis en place le réseau suivant :



Puis on a configurer le routeurs de cette manière :

```
R21(config)# interface FastEthernet0/0
R21(config-if)# ip address 10.0.221.2 255.255.255.0
R21(config-if)# no shutdown
R21(config-if)# exit
R21(config)# do write memory

# Configuration de l'OSPF

R21(config)# router ospf 1
R21(config-router)# network 10.0.221.0 255.255.255.0 area 0
R21(config-router)# exit
R21(config)# do write memory
```

Ici on a une configuration OSPF classique en definissant le numéro de l'AS 1 et le réseau

On a ainsi configurer également sur le router R2 uniquement la partie ospf presente ci-dessus.

Puis on a réaliser un `show ip route` sur le routeur R21 :

```
show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
```

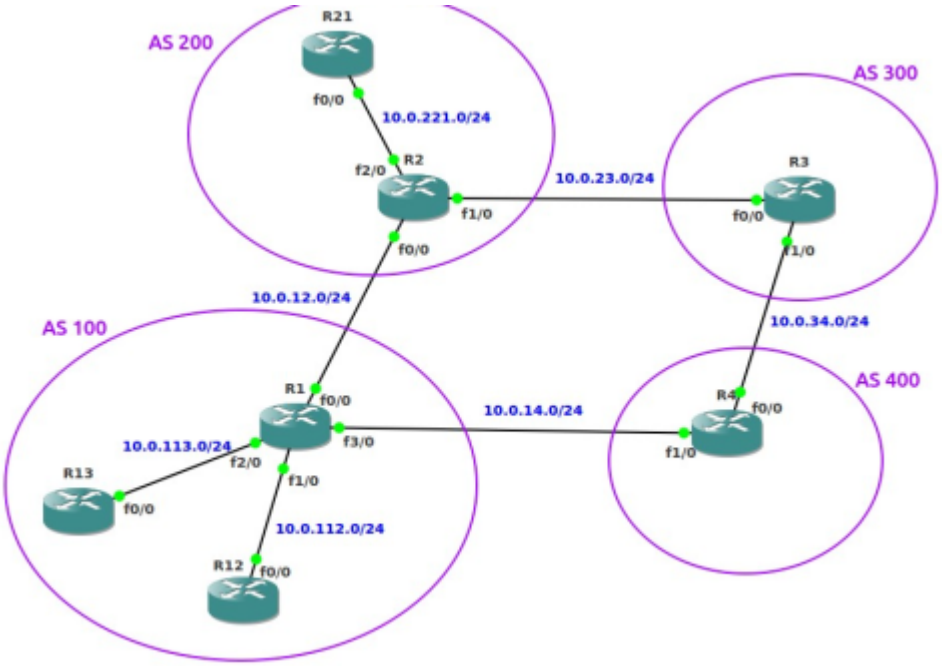
```
     100.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
O       100.2.0.2/32 [110/2] via 10.0.221.2, 00:02:43, FastEthernet0/0
O E2    100.0.0.0/8 [110/1] via 10.0.221.2, 00:02:43, FastEthernet0/0
O E2    100.1.0.0/24 [110/1] via 10.0.221.2, 00:02:43, FastEthernet0/0
C       100.2.0.0/24 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O E2    10.0.14.0/24 [110/1] via 10.0.221.2, 00:02:43, FastEthernet0/0
O       10.0.12.0/24 [110/2] via 10.0.221.2, 00:02:44, FastEthernet0/0
O E2    10.0.0.0/8 [110/1] via 10.0.221.2, 00:02:44, FastEthernet0/0
O       10.0.23.0/24 [110/2] via 10.0.221.2, 00:02:44, FastEthernet0/0
O E2    10.0.112.0/24 [110/1] via 10.0.221.2, 00:02:44, FastEthernet0/0
O E2    10.0.113.0/24 [110/1] via 10.0.221.2, 00:02:44, FastEthernet0/0
C       10.0.221.0/24 is directly connected, FastEthernet0/0
```

On peut voir que le réseau et bien détecter en OSPF et que les routeurs sont bien connecter entre eux.

- Configuration est mise en place d'un réseau avec BGP :

Dans le contexte de la formation dans la ressource R302 j'ai pu mettre en place via l'application GNS3 un réseau interne avec le protocole BGP :

Tout d'abord j'ai mis en place le réseau suivant :



On a configurer les routeurs R1 R2 R3 et R4 de sorte a avoir les configurations principales pour les réseaux BGP.

Puis en fonction des AS on a configurer le BGP de cette manière :

```
R1(config)# router bgp 100
R1(config-router)# neighbor 10.0.12.2 remote-as 200
R1(config-router)# neighbor 10.0.14.4 remote-as 400
R1(config-router)# exit
R1(config)# do write memory
```

Sur le routeur R1 on a configurer le BGP avec le numéro de l'AS 100 et les voisins avec leur AS respectif.

Les mêmes commandes ont été effectuées sur les autres routeurs en correspondance avec les AS et les réseaux.

Quand tout les routeurs BGP sont créer on reçoit des messages entre les routeurs :

```
*Mar 1 00:00:17.923: %BGP-5-ADJCHANGE: neighbor 192.168.23.3 Up
```

puis on vois les routes BGP apparaitre sur les routeurs comme ici sur R3:

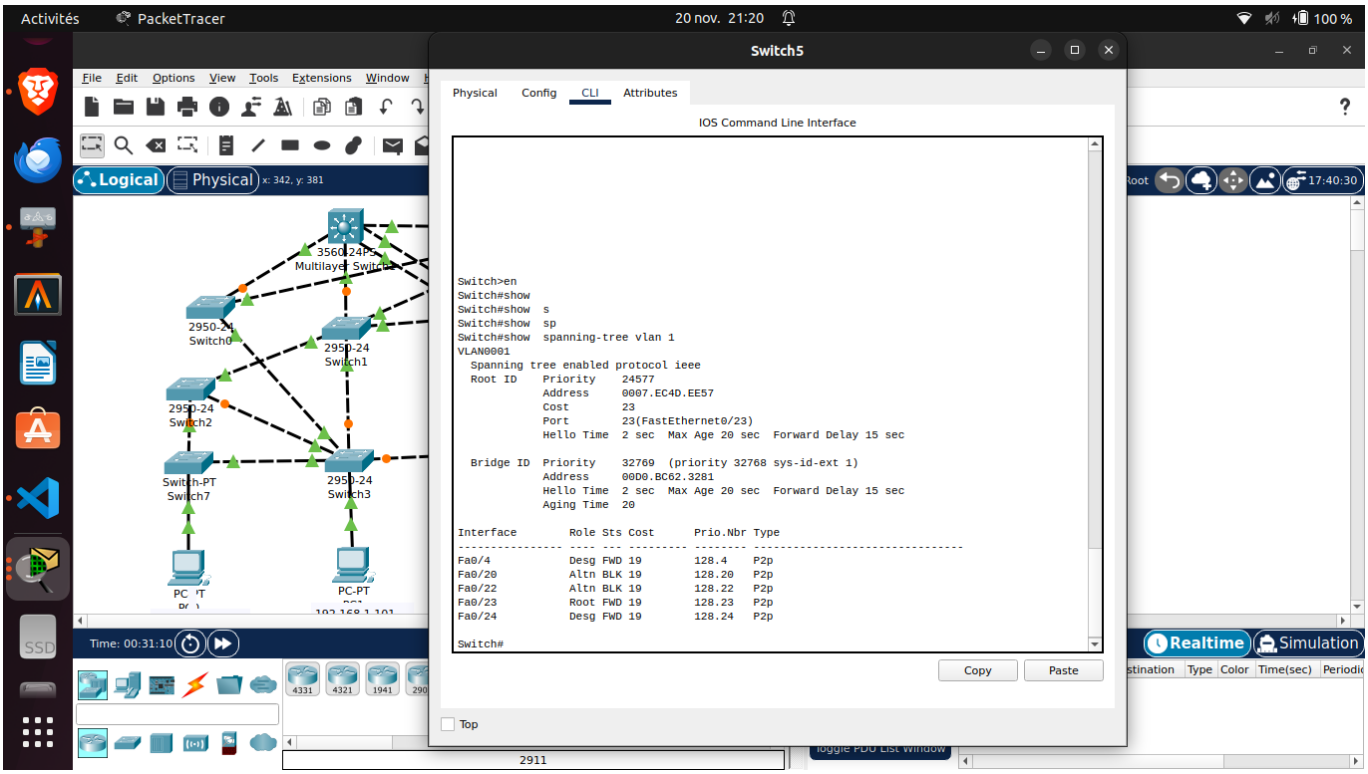
```
show ip bgp

BGP table version is 27, local router ID is 100.3.0.3
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete


r> 10.0.23.0/24     100.2.0.2                0             0 200 ?
```

```
> 10.0.221.0/24    100.2.0.2                0             0 200 ?
```

On peut voir que le réseau et bien détecter en BGP et que les routeurs sont bien connecter entre eux.

- Configuration est mise en place d'un réseau avec STP :

Dans la ressource R301 j'ai pu mettre en place via l'application Cisco Packet Tracer un réseau interne avec le protocole STP :



On peut voir pour un réseau complexe les routes prises par le protocole STP pour éviter les bouclages réseaux.

- Virtualisation du réseau :

Durant la SAE.3.Devcloud.03 On a pu virtualiser des appareils de routages comme le routeur c8000 avec le router edge csr1000v.

- Configuration des VPN sur serveur et client :

De part les blocages de port de l'IUT j'ai du mettre en place un VPN entre mon clusters proxmox chez moi, pour me permettre d'acceder a tout les ports exterieur.

Pour ce faire j'ai créer un VPN avec wireguard sur un serveur proxmox dans un contener LXC, puis une configuration entre mon serveur proxmox chez moi et les differents clients.

De part la sécurité du VPN je ne vais pas montrer par des captures d'écrans les configurations mais je vais expliquer comment j'ai fait :

1. Installation de wireguard sur le serveur proxmox :

```
apt install wireguard
```

2. Génération des clés sur le serveur proxmox :

```
wg genkey | tee privatekey | wg pubkey > publickey
```

3. Configuration du serveur wireguard et du client wireguard:

```
[Interface]
PrivateKey= [ Clefs priver du serveur  Clefs priver du client]
Address = [ Adresse IP du serveur wireguard Adresse IP du client wireguard]
ListenPort = 51820

[Peer]
PublicKey = [ Clefs public du client wireguard Clefs public du serveur
wireguard]
AllowedIPs = [ Adresse IP du client wireguard Adresse IP du serveur
wireguard (ou 0.0.0.0/0 pour le full tunnel)]
Endpoint =  [ Adresse IP du client wireguard ou ip publique ]
PersistentKeepalive = 25
```

Bien evidement on a du configurer a l'interieur du serveur VPN les regles de forwarding et de NAT pour permettre au client de pouvoir acceder a internet.

```
iptables iptables -t nat -A POSTROUTING -s [ Réseau wireguard ] -o eth0 -j
MASQUERADE
```

Et sur le routeur on autorise l'accès au serveur wireguard en ouvrant le port 51820.

Sous linux on utilise seulement les CLI pour pouvoir configurer le VPN.

Sous windows et android l'entreprise Wireguard a créer une application pour pouvoir configurer le VPN de manière graphique. Sans pour autant changer les configurations de bases.

Pour ma part j'ai configurer mon VPN en full tunnel pour pouvoir acceder a tout les ports et mon cluster proxmox.

Ce que j'en conclu :

Retour au sommaire

J'estime que je suis capable de configurer et de depanner le routage dynamique dans un réseau. Egalement de configurer les ordinateurs clients et serveurs pour qu'ils puissent correspondre au besoin demander et faire la planification du réseau complet d'une infrastructure.

J'en conclu que j'ai obtenu le niveau attendu en fin d'année pour la compétence Administrer.
