RAPPORT DES TP DE RESEAUX

MICHON Guillaume

INFO 2019 -- Polytech Marseille

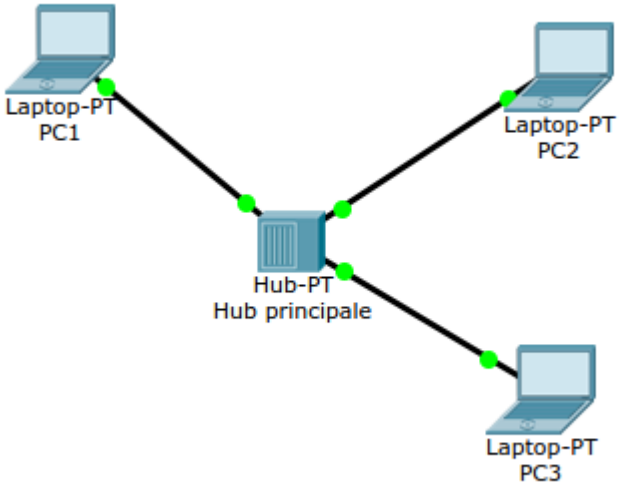
Table des matières

TP1

Un réseau simple

Mode « Realtime » (défaut)

Voici la configuration faite sur les différents équipements :

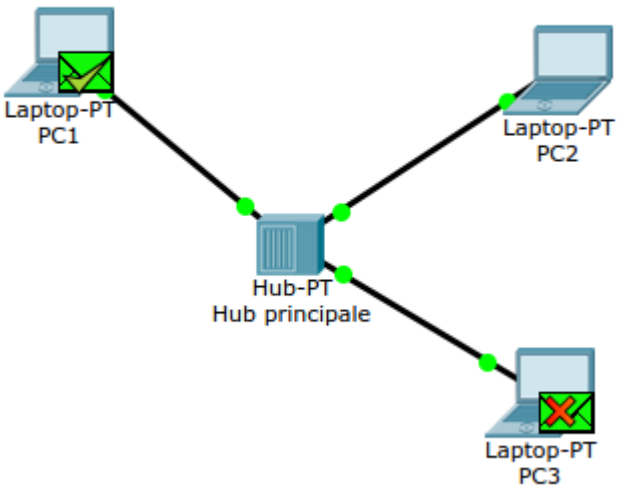


Nom	Adresse IP	Masque de sous-réseau
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.1	255.255.255.0
PC3	192.168.1.2	255.255.255.0

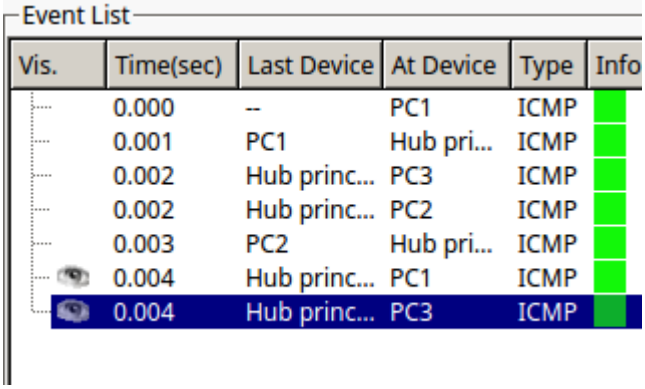
1. Dans cet exercice les 3 PC sont dans le même réseau par conséquence il fait configurer leur différente adresse IP ainsi que leur masque de sous réseau. Le Hub n'a pas de configuration par définition car il va retransmettre sur tous ses ports les différentes trames, il n'y a donc pas de routing à faire avec cette équipement réseau contrairement au switch.

Mode « Simulation »

2. Le mode simulation permet de simuler l'acheminement de PDU (dans notre cas du type ICMP) afin de voir les différents messages générés afin de transmettre le PDU.
   On peut faire visuellement sur le schéma les différents paquets envoyés et s'ils sont acceptés ou refusés par les différents appareils, comme le montre ci-dessous.

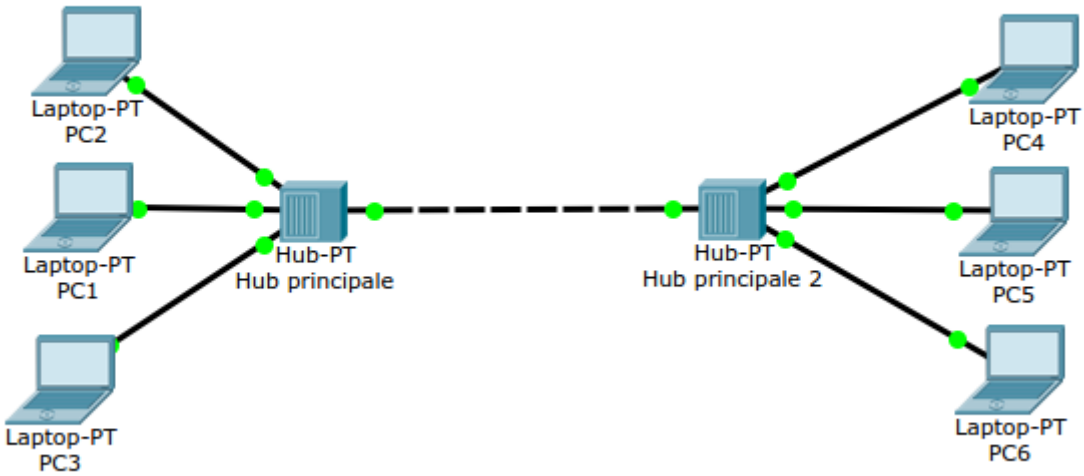


De plus le mode simulation permet d'avoir un résumé des différents messages envoyés avec une timeline ainsi que les différents appareils qui communique.



3. Comme précisé précédemment on utilise un Hub donc tous les PDU sont répétés sur les tous les ports du Hub.

Deux réseaux simples

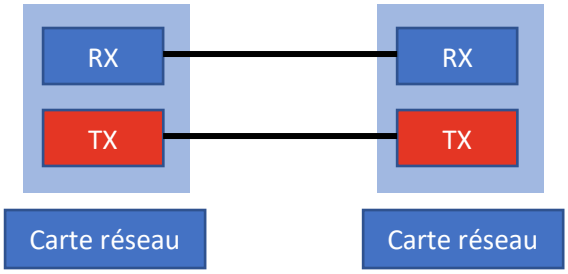


Voici la configuration faite sur les différents équipements :

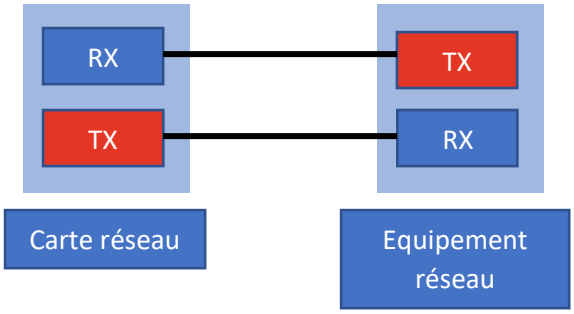
Nom	Adresse IP	Masque de sous-réseau
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.1	255.255.255.0
PC3	192.168.1.2	255.255.255.0
PC4	192.168.1.4	255.255.255.0
PC5	192.168.1.5	255.255.255.0
PC6	192.168.1.6	255.255.255.0

Deux réseaux simples

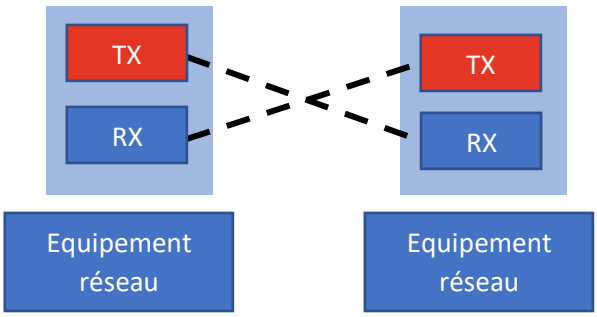
4. Afin de relier les hubs on utilise un câble coaxial.



Si on utilise un câble droit pour connecter deux carte réseau (deux PC par exemple) cela va pas fonctionner car on va envoyer sur l'interface de transmission de l'autre carte réseau et donc ne peux pas recevoir de donnée.



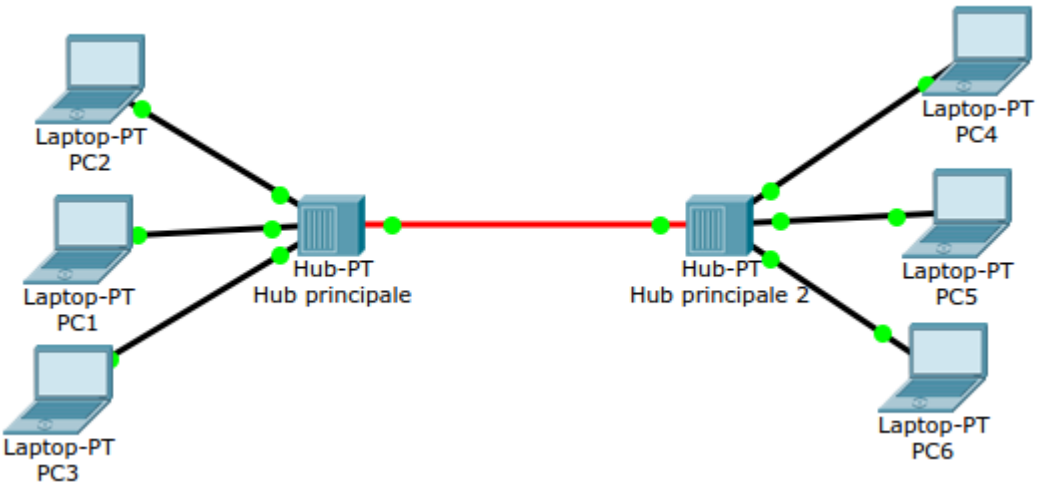
Lorsqu'on connecte un équipement réseau et une carte réseau le problème avec le câble droit ne ce pose pas, car sur les équipements réseau les interfaces RX (réception) et TX (transmission) son inversé par rapport au carte réseau classique.



Avec un câble croisé il n'y a donc pas de soucis lorsque on connecte deux équipement réseau entre elles ou deux carte réseau entre elles.

Que la fibre soit !

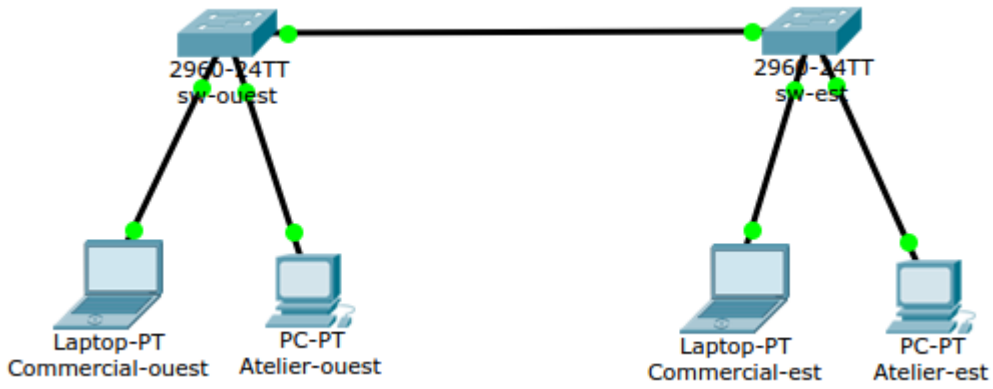
5. Pour pouvoir connecter les cartes fibres des deux hubs utilise un câble fibre.



6. Sachant que le réseau actuel est 192.168.1.0/24 si on change les adresses de 3 PC par 192.168.2.1, 192.168.2.2, 192.168.2.3 ils vont se retrouver hors du réseau et donc ils ne peuvent pas communiquer entre eux sans équipement réseau.
   Afin de pouvoir résoudre ce problème il suffit donc de changer le masque de sous-réseau des PC afin qu'ils se retrouve tous dans le réseau 192.168.0.0/22.

TP2

Réalisation d'un réseau



Sachant que le réseau des ordinateurs portables des commerciaux est dans le même réseau 192.168.1.0/24 et que les ordinateurs des ateliers sont dans le réseau 192.168.2.0/24, il est normal que les commerciaux puissent communiquer entre eux, que les ordinateurs des ateliers puissent communiquer entre eux, et que les ordinateurs des commerciaux ne puissent pas communiquer avec les ordinateurs des ateliers et inversement.

1. Sachant que la configuration de l'adresse IP est modifiable directement sur un des ordinateurs, par exemple une méchante personne de l'atelier peut changer son adresse IP par une adresse IP dans le réseau 192.168.1.0/24 par exemple 192.168.1.254 et il peut donc communiquer avec les commerciaux ou atelier. Donc l'étanchéité commercial/atelier n'est donc pas assuré.

2. Comme dis précédemment le PC commercial avec une adresse IP dans le plan d'adressage de l'atelier peut communiquer avec les autres ordinateurs de l'atelier car il se trouve dans le même réseau. Cependant il ne peut plus communiquer avec les autres commerciaux vus qu'il ne se trouve plus dans son réseau d'origine.
3. Le réseau n'est toujours pas sécurisé niveau étanchéité commercial/atelier.

Isolation 802.1Q

4. Lorsque la trame Ethernet rentre à l'intérieur d'un switch avec des VLAN la trame est modifié. On ajoute un champ tag 802.1q et le FCS est mis à jour. Ci-dessous la différence entre une trame Ethernet V2 et une trame Ethernet 802.1Q utilisé lorsqu'on utilise les VLAN 802.1Q.

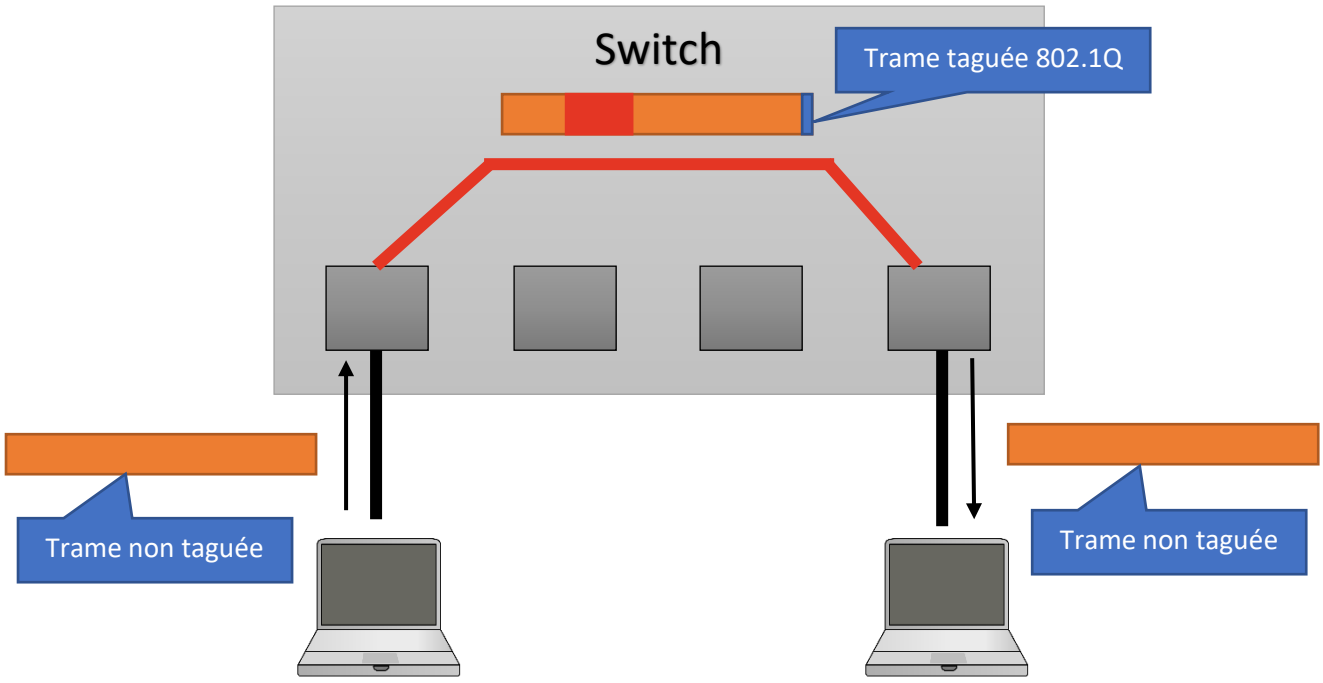
Trame Ethernet V2

@MAC destination	@MAC source	Type	Donnée	FCS

Trame Ethernet 802.1Q

@MAC destination	@MAC source	Type = 802.1Q	Type	Donnée	FCS

Lorsque la trame ressort du switch la trame est détagué et le FCS est recalculé, donc la trame redevient exactement la même que à son entrée dans le switch.



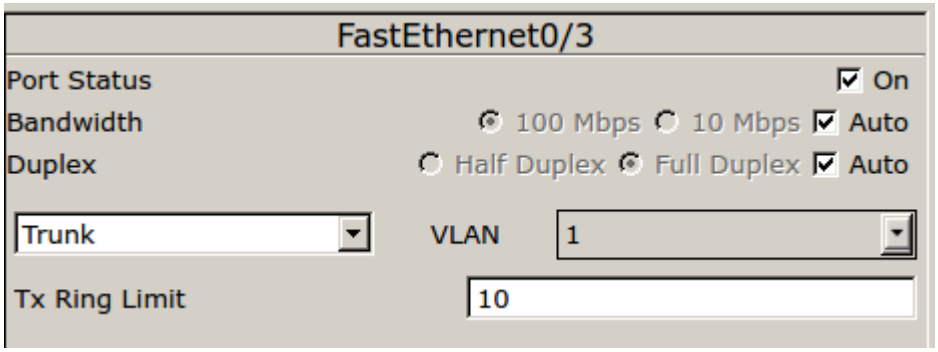
5. L'état de la connectivité est-ouest et commerciaux-atelier est le suivant :

Source	Destination	Status
Commercial-ouest	Atelier-ouest	✖
Commercial-ouest	Commercial-est	✖
Commercial-ouest	Atelier-est	✖
Atelier-ouest	Commercial-est	✖
Atelier-ouest	Atelier-est	✖
Commercial-est	Atelier-est	✖

Dans ce cas là aucune des machines peuvent communiquer entre elles. Cela est dû à deux choses.

- La première c'est à cause de la mise en place de VLAN sur les ports des switch donc les ateliers et les commerciaux ne peuvent pas communiquer (ce qu'on veut avoir).
- La deuxième est non voulue car elle concerne les communications entre les deux même département (par exemple entre atelier-est et atelier-ouest), elle est dû à la perte du tag 802.1Q après la sortie du premier switch. En effet lorsqu'une trame sort d'un switch elle est détagué et donc le prochain switch ne peux pas connaitre le tag 802.1Q et donc la trame n'arrivera pas à destination car elle sera jetée car dans le mauvais VLAN. Une solution à ce problème c'est de mettre les ports reliant les deux switch en mode « Trunk ».

6. Après avoir configuré un port Trunk sur les deux switch comme ci-dessous on obtient l'état de connectivité suivante :



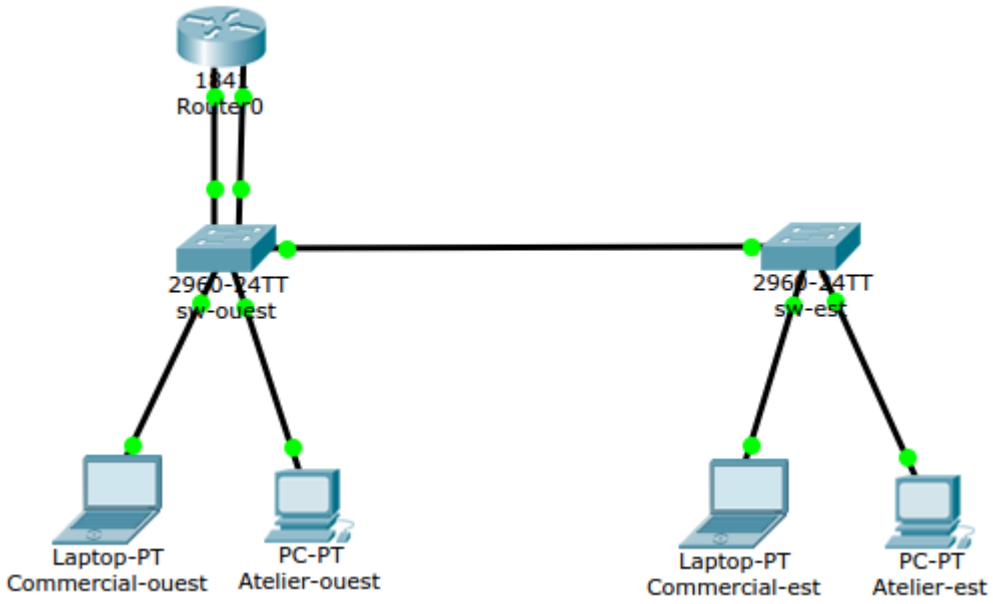
Source	Destination	Status
Commercial-ouest	Atelier-ouest	✖
Commercial-ouest	Commercial-est	✔
Commercial-ouest	Atelier-est	✖
Atelier-ouest	Commercial-est	✖
Atelier-ouest	Atelier-est	✔
Commercial-est	Atelier-est	✖

Ce qui correspond bien à l'isolation que l'on souhaite obtenir.

7. Vu que l'isolation des ordinateurs des divers département se fait au niveau des ports du switch grâce au VLAN 802.1Q, si l'utilisateur change son adresse IP pour être dans le sous réseau d'un autre département cela ne sera pas suffisant pour pouvoir communiquer. En effet il pourra communiquer qu'avec les personnes possédant le même VLAN mais aussi qui est dans le même sous réseau.

Dé-isolation 802.1Q

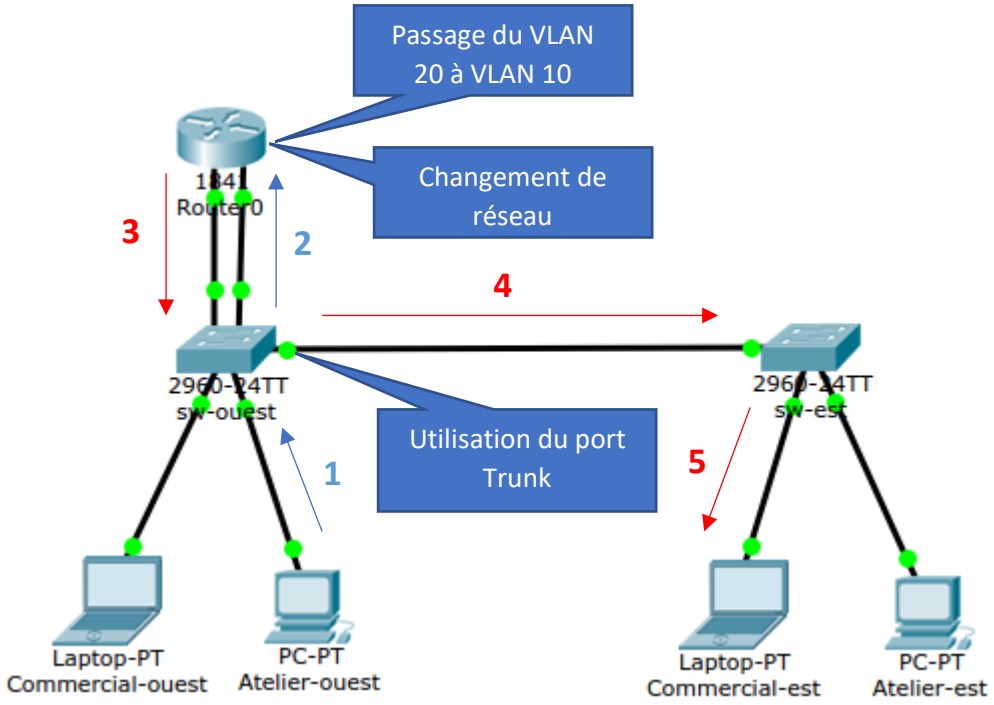
Après avoir rajouté un routeur 1841 et avoir configuré une carte avec une IP sur le plan d'adressage des commerciaux et une autre avec une IP sur le plan d'adressage des ateliers, et avoir mis les bons VLAN sur les bons ports on obtiens le réseau ci-dessous :



8. A l'heure actuelle voici l'état de connectivité :

Source	Destination	Status
Commercial-ouest	Atelier-ouest	✔
Commercial-ouest	Commercial-est	✔
Commercial-ouest	Atelier-est	✔
Atelier-ouest	Commercial-est	✔
Atelier-ouest	Atelier-est	✔
Commercial-est	Atelier-est	✔

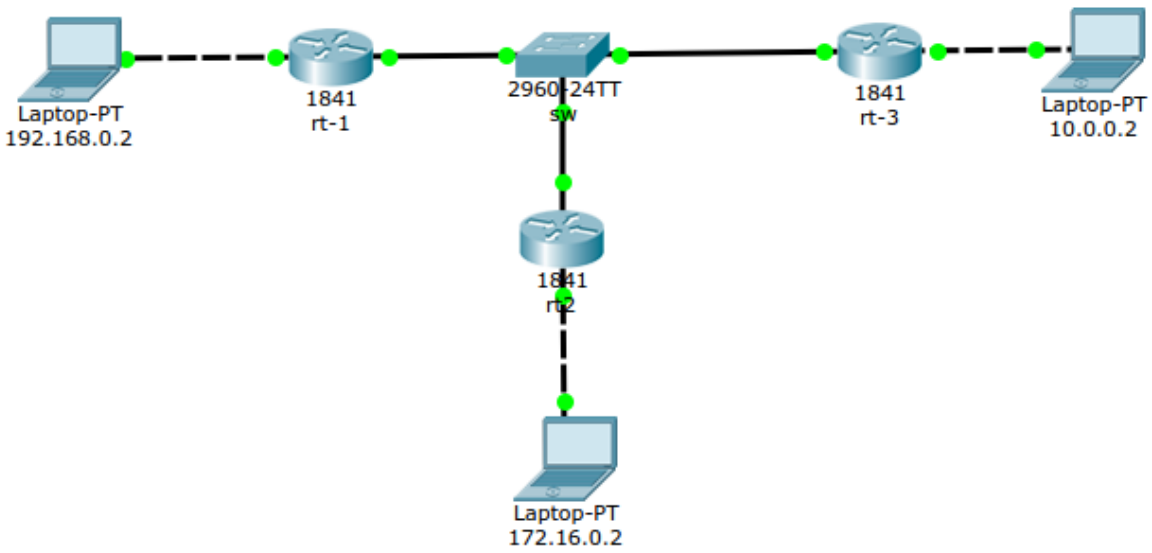
9. Ici le routeur joue le rôle de passerelle et il va permettre de changer de VLAN et de sous réseau dans notre cas voici un exemple de la communication entre un atelier et un commercial. En rouge c'est les communications avec un VLAN de 10 et dans le réseau correspondant aux commerciaux, et en bleu les communications avec un VLAN de 20 et dans le réseau correspondant aux ateliers.



10. Vu que les VLAN sont configuré au niveau des différents switch/routeur je pense que niveau sécurité c'est correct. En effet si une personne mal attentionnée change son adresse IP afin d'être dans le sous réseau d'un autre département, son VLAN ne changera pas et donc il sera tout le temps dans le même groupe de communication et donc il n'y aura pas d'usurpation d'IP car s'il le fait il ne sera pas dans le même réseau et donc il ne pourra pas communiquer. La dé-isolation via la mise en place du router0 permet au deux départements de communiquer quand même.

TP3

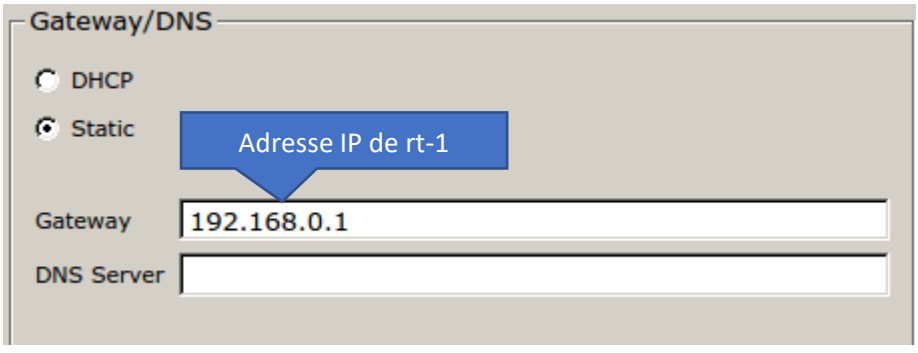
Routage statique simple



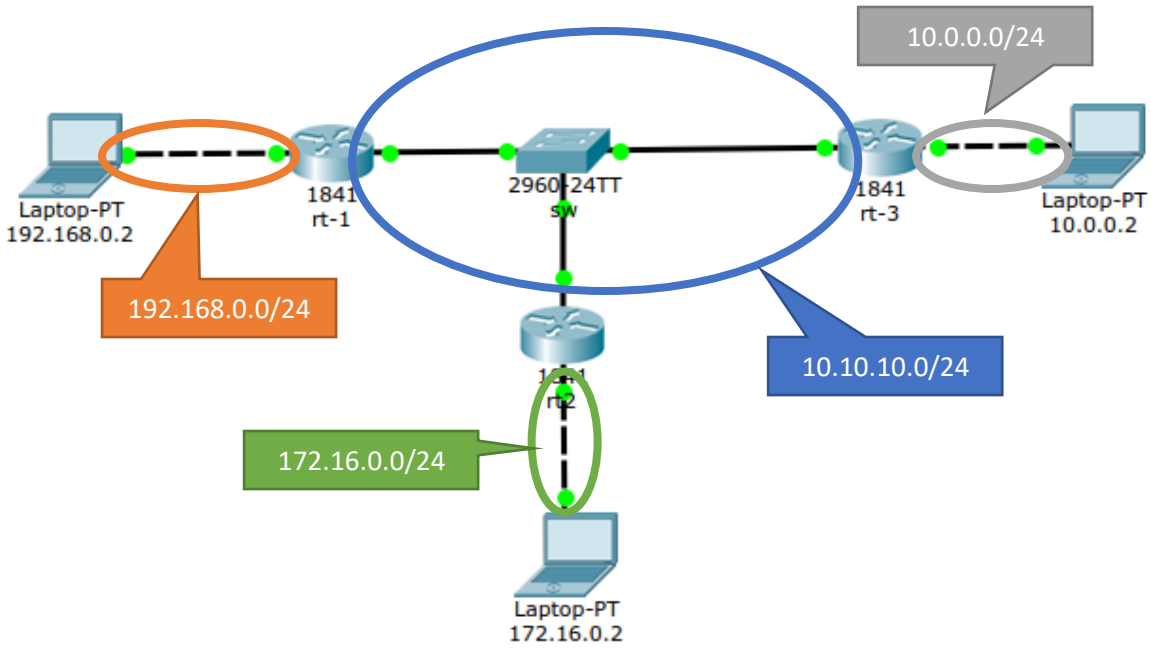
Voici les différents adresse IP/Masque pour chaque interface de ce schéma :

Nom	Interface	Adresse IP	Masque
192.168.0.2	FastEthernet0	192.168.0.2	255.255.255.0
Rt-1	FastEthernet0/0	10.10.10.1	255.255.255.0
	FastEthernet0/1	192.168.0.1	255.255.255.0
172.16.0.2	FastEthernet0	172.16.0.2	255.255.255.0
Rt2	FastEthernet0/0	10.10.10.2	255.255.255.0
	FastEthernet0/1	172.16.0.1	255.255.255.0
10.0.0.2	FastEthernet0	10.0.0.2	255.255.255.0
Rt-3	FastEthernet0/0	10.10.10.3	255.255.255.0
	FastEthernet0/1	10.0.0.1	255.255.255.0

1. Le routeur situé derrière le PC représente le routeur par défaut nommé la passerelle (Gateway) c'est par ce routeur que passera les communications qui ne sont pas dans le sous-réseau du PC ou si aucune entrée dans la table de routage a été configuré par l'administrateur du réseau. Il ne faut pas oublier de configurer la passerelle sur chaque PC comme ci-dessous pour le PC 192.168.0.2 (avec Packet Tracer) :



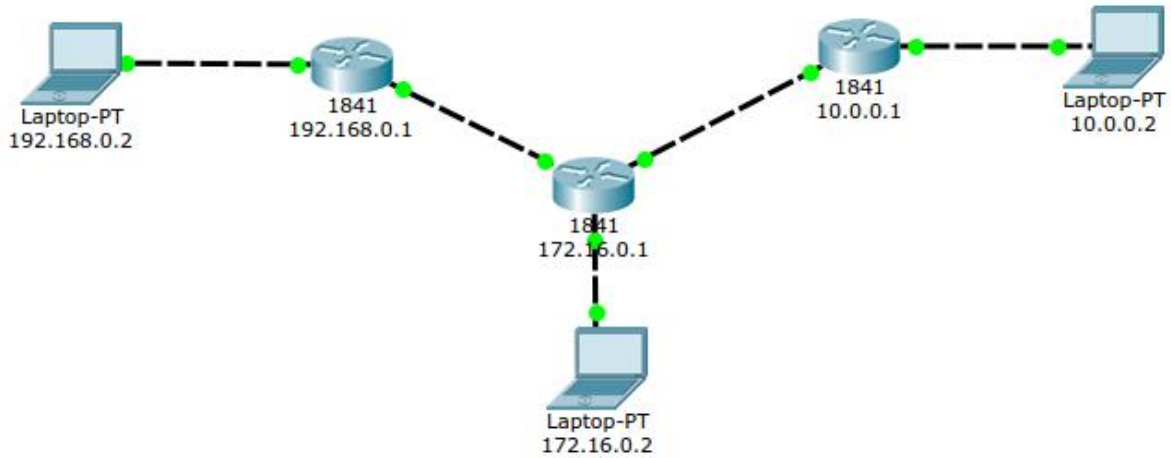
2. Afin de réaliser ce réseau il a fallu rajouter 1 réseau de plus qui correspond au réseau situé entre tous les routeurs qui sont relié par un switch



3. Afin de réaliser ce réseau il a fallu entrer 2 entrées dans les tables de routages de chaque routeur. Ces entrées correspondent aux façons d'atteindre les sous-réseaux proches.

Pour rt-1	Pour rt2	Pour rt-3
Network Address	Network Address	Network Address
172.16.0.0/24 via 10.10.10.2	192.168.0.0/24 via 10.10.10.1	192.168.0.0/24 via 10.10.10.1
10.0.0.0/24 via 10.10.10.3	10.0.0.0/24 via 10.10.10.3	172.16.0.0/24 via 10.10.10.2

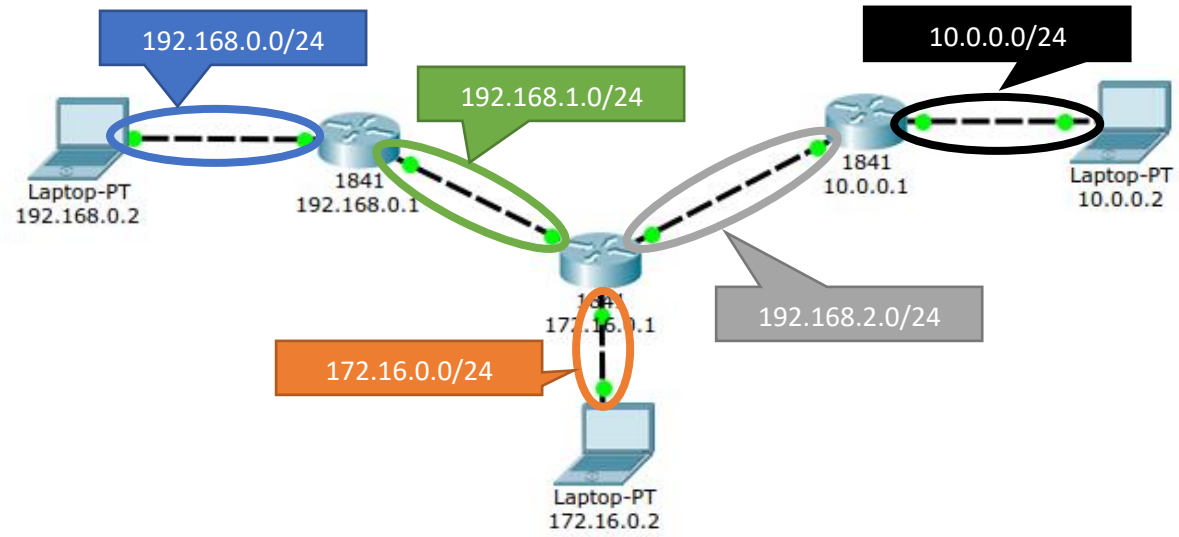
Autre routage statique



Voici les différents adresse IP/Masque pour chaque interface qui ont été utilisé pour ce schéma :

Nom	Interface	Adresse IP	Masque
192.168.0.2	FastEthernet0	192.168.0.2	255.255.255.0
192.168.0.1	FastEthernet0/0	192.168.0.1	255.255.255.0
	Ethernet0/1/0	192.168.1.1	255.255.255.0
172.16.0.2	FastEthernet0	172.16.0.2	255.255.255.0
172.16.0.1	FastEthernet0/0	172.16.0.1	255.255.255.0
	FastEthernet0/1	192.168.2.1	255.255.255.0
	Ethernet0/1/0	192.168.1.2	255.255.255.0
10.0.0.2	FastEthernet0	10.0.0.2	255.255.255.0
10.0.0.1	FastEthernet0/0	10.0.0.1	255.255.255.0
	Ethernet0/1/0	192.168.2.2	255.255.255.0

4. Il a fallu ajouter 2 réseaux supplémentaires car un routeur fait la liaison entre deux réseaux.

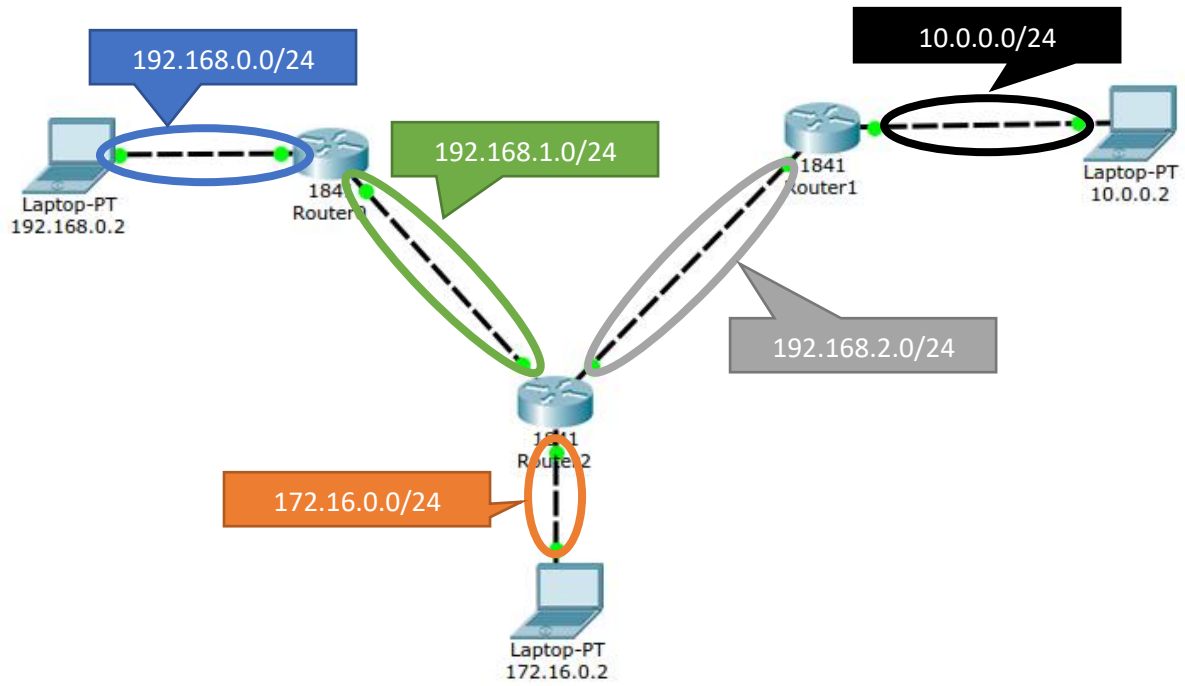


5.

6. Afin de réaliser ce réseau il a fallu rajouter 2 entées dans chaque routeur. Ci-dessous les différentes tables de routage de chaque routeur :

Pour 192.168.0.1	Pour 172.16.0.1	Pour 10.0.0.1
Network Address	Network Address	Network Address
172.16.0.0/24 via 192.168.1.2	192.168.0.0/24 via 192.168.1.1	192.168.0.0/24 via 192.168.2.1
10.0.0.0/24 via 192.168.1.2	10.0.0.0/24 via 192.168.2.2	172.16.0.0/24 via 192.168.2.1

Routage dynamique RIP



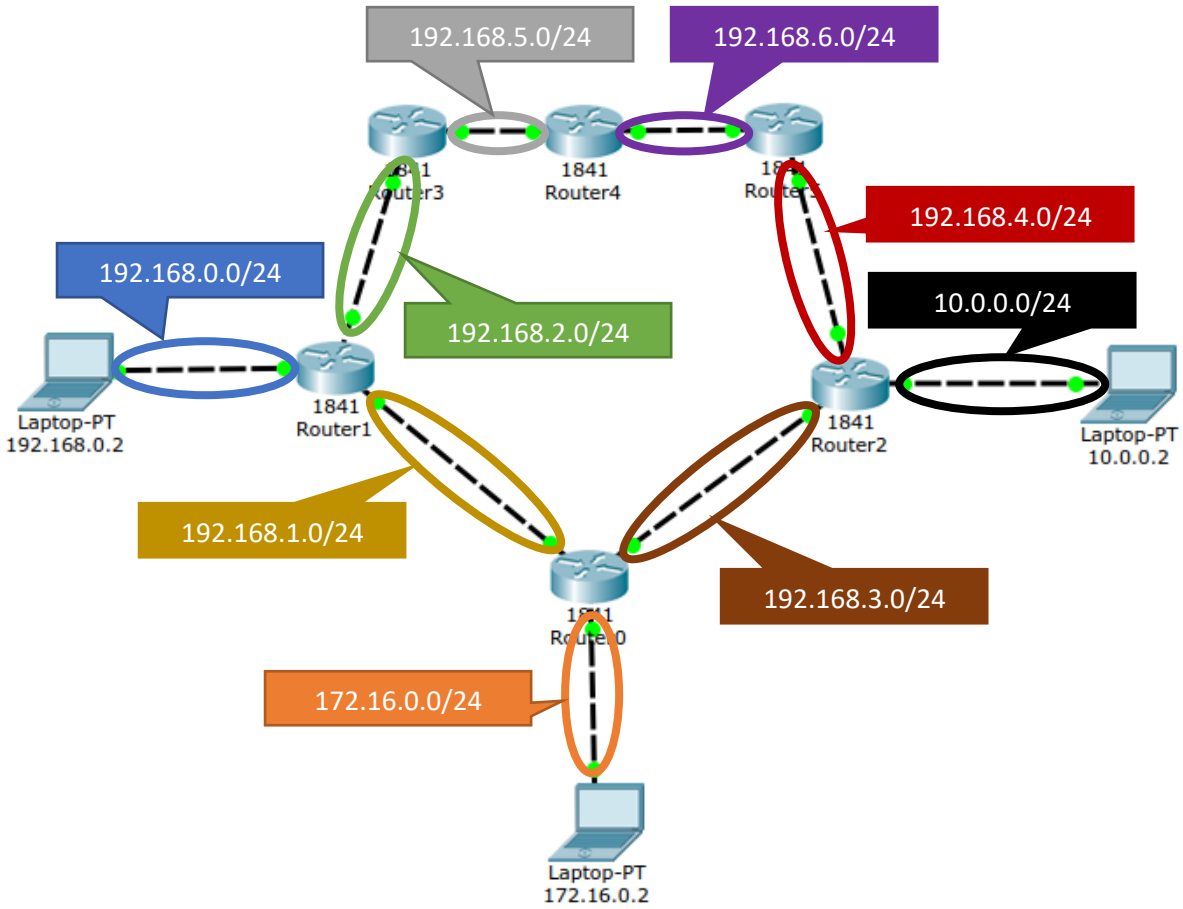
Voici les différents adresse IP/Masque pour chaque interface qui ont été utilisé pour ce schéma :

Nom	Interface	Adresse IP	Masque
192.168.0.2	FastEthernet0	192.168.0.2	255.255.255.0
Router0	FastEthernet0/0	192.168.0.1	255.255.255.0
	FastEthernet0/1	192.168.1.2	255.255.255.0
172.16.0.2	FastEthernet0	172.16.0.2	255.255.255.0
Router2	FastEthernet0/0	172.16.0.1	255.255.255.0
	FastEthernet0/1	192.168.1.1	255.255.255.0
	Ethernet0/1/0	192.168.2.1	255.255.255.0
10.0.0.2	FastEthernet0	10.0.0.2	255.255.255.0
Router1	FastEthernet0/0	10.0.0.1	255.255.255.0
	FastEthernet0/1	192.168.2.2	255.255.255.0

7. Afin de réaliser ce réseau il a fallu rajouter autant d'entrée qu'il y a de réseau aux bornes du routeur, pour la même raison que précédemment il faut donc rajouter deux réseaux supplémentaires. Voici les différentes tables de routage :

Pour Router0	Pour Router1	Pour Router 2
Network Address 192.168.0.0 192.168.1.0	Network Address 10.0.0.0 192.168.2.0	Network Address 172.16.0.0 192.168.1.0 192.168.2.0

Autre routage dynamique RIP



Voici les différents adresse IP/Masque pour chaque interface qui ont été utilisé pour ce schéma :

Nom	Interface	Adresse IP	Masque
192.168.0.2	FastEthernet0	192.168.0.2	255.255.255.0
Router1	FastEthernet0/0	192.168.0.1	255.255.255.0
	FastEthernet0/1	192.168.1.2	255.255.255.0
	Ethernet0/1/0	192.168.2.1	255.255.255.0
172.16.0.2	FastEthernet0	172.16.0.2	255.255.255.0
Router0	FastEthernet0/0	172.16.0.1	255.255.255.0
	FastEthernet0/1	192.168.1.1	255.255.255.0
	Ethernet0/1/0	192.168.3.1	255.255.255.0
10.0.0.2	FastEthernet0	10.0.0.2	255.255.255.0
Router2	FastEthernet0/0	10.0.0.1	255.255.255.0
	FastEthernet0/1	192.168.3.2	255.255.255.0
	Ethernet0/1/0	192.168.4.1	255.255.255.0
Router3	FastEthernet0/0	192.168.2.2	255.255.255.0
	FastEthernet0/1	192.168.5.1	255.255.255.0
Router4	FastEthernet0/0	192.168.5.2	255.255.255.0
	FastEthernet0/1	192.168.6.1	255.255.255.0
Router5	FastEthernet0/0	192.168.6.2	255.255.255.0
	FastEthernet0/1	192.168.4.2	255.255.255.0

8. Afin de réaliser ce réseau il a fallu rajouter autant d'entrée qu'il y a de réseau aux bornes du routeur, pour la même raison que précédemment il faut donc rajouter deux réseaux supplémentaires. Voici les différentes tables de routage :

Pour Router0

Network Address
172.16.0.0
192.168.1.0
192.168.3.0

Pour Router1

Network Address
192.168.0.0
192.168.1.0
192.168.2.0

Pour Router2

Network Address
10.0.0.0
192.168.3.0
192.168.4.0

Pour Router3

Network Address
192.168.2.0
192.168.5.0

Pour Router 4

Network Address
192.168.5.0
192.168.6.0

Pour Router5

Network Address
192.168.4.0
192.168.6.0

9. Si on débranche la connexion entre Router1 et Router0 ont ce rend compte que si on fait un ping de 10.0.0.2 sur 192.168.0.2 le paquet ICMP passera par le chemin du haut au lieu de passer par le bas, car la table de routage a été mis à jour après le débranchement. Par contre si on débranche le lien avant qu'il une mise à jour de la table sur les routeurs l'envoie du paquet échouera.
10. Si on rebranche cette connexion et qu'on recommence le PING celui-ci repassera par le bas grâce au protocole RIP qui est basé sur un vecteur de distance. Pareil que précédemment si la table de routage n'est pas à jour il y a de grande chance que le paquet passe par le haut.
11. Si on le souhaite passer le trafic de 10.0.0.2 vers le chemin du haut il suffit d'ajouter une nouvelle route static dans la table de routage qui sera traité avec plus de priorité que une entrée RIP.

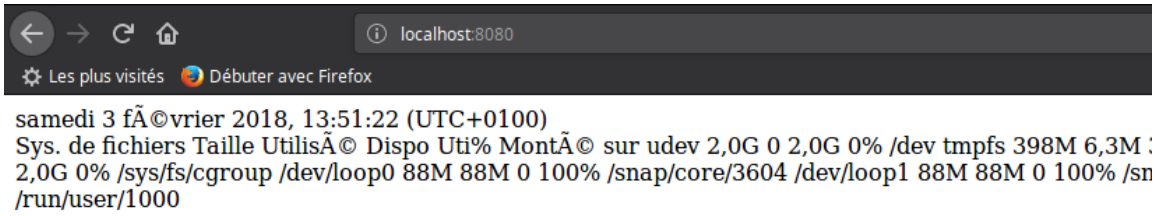
TP4

Client – serveur avec Netcat, le couteau suisse réseau

1. Afin de pouvoir crée un mini serveur web qui affiche la date locale ainsi que l'état d'occupation des partitions il faut savoir quelle commande on aura besoin :
    - La commande « date » : Pour afficher la date locale
    - La commande « df » : Pour afficher l'état d'occupation des partitions (on l'utilisera avec l'option -H pour un meilleur affichage)
    - La commande « echo » : Pour afficher le résultat des commandes précédente et formatter le tout en HTML
    - La commande « nc » : Pour crée le serveur netcat (on utilisera les options -l pour mettre le serveur en écoute et l'option -p pour définir le port 8080 car sur mon ordinateur il y a déjà un serveur apache qui tourne sur le port 80)

```
guillaume@shathon ~ echo -e "HTTP/1.1 200 \n\n<p>$(date)<br/>$(df -H)<p>" | nc -l -p 8080
```

Si je regarde mon navigateur sur le port 8080 j'obtiens donc :



Et si on regarde le terminal on se rend compte qu'une demande de page HTTP à étais faite sur notre serveur Netcat :

```
guillaume@shathon ~ echo -e "HTTP/1.1 200 \n\n<p>$(date)<br/>$(df -H)<p>" | nc -l -p 8080
GET / HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: Phpstorm-9b0baf73=ff93c8b1-3243-4430-bdc6-88bd7d15df71
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

2. Par défaut Netcat utilise TCP si on souhaite changer en UDP il faudra utiliser l'option -u
    1. Echanger un fichier du client vers le serveur avec TCP :
        - Coté client (après avoir lancé le serveur) :

```
guillaume@shathon ~ echo "Hello World TCP" > fichier.txt
guillaume@shathon ~ nc localhost 1234 < fichier.txt
guillaume@shathon ~
```

        - Coté serveur :

```
guillaume@shathon ~ nc -l -p 1234 > fichier_sortie
guillaume@shathon ~ cat fichier_sortie
Hello World TCP
```

    2. Echanger un fichier du serveur vers le client avec TCP :
        - Coté serveur :

```
guillaume@shathon ~ echo "Hello World I'm server TCP" > fichier.txt
guillaume@shathon ~ nc -l -p 1234 < fichier.txt
```

        - Coté client (après avoir lancé le serveur) :

```
guillaume@shathon ~ nc localhost 1234 > fichier_sortie
guillaume@shathon ~ cat fichier_sortie
Hello World I'm server TCP
```

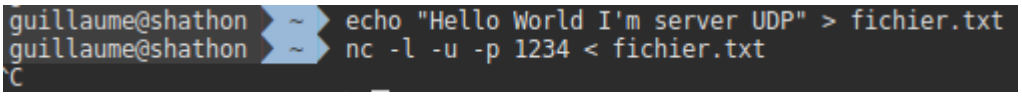
    3. Echanger un fichier du client vers le serveur avec UDP
        - Coté serveur :

```
guillaume@shathon ~ nc -l -u -p 1234 > fichier_sortie
^C
x guillaume@shathon ~ cat fichier_sortie
Hello World UDP
```

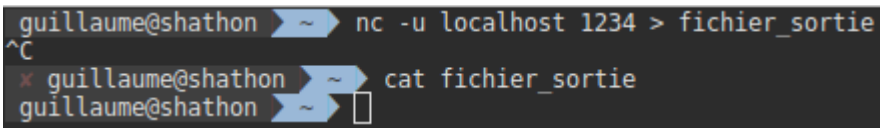
        - Coté client (après avoir lancé le serveur) :

```
guillaume@shathon ~ echo "Hello World UDP" > fichier.txt
guillaume@shathon ~ nc -u localhost 1234 < fichier.txt
^C
```

4. Echanger un fichier du serveur au client avec UDP :
    - Coté serveur :



    - Coté client (après avoir lancé le serveur) :



Ici l'envoie de fichier ne fonctionne pas car vu qu'on utilise UDP il n'y pas de vérification que le client est connecté (car dans UDP il n'y a pas de système de handshake). Une solution à ce problème c'est d'envoyer continuellement le fichier avec une boucle par exemple.