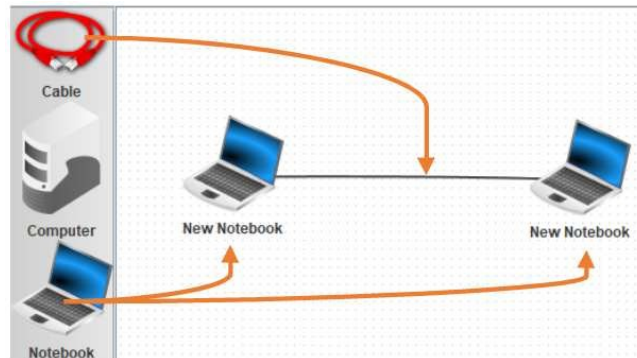
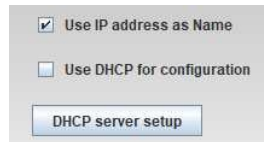


Partie 1 : Réseau LAN adressage statique

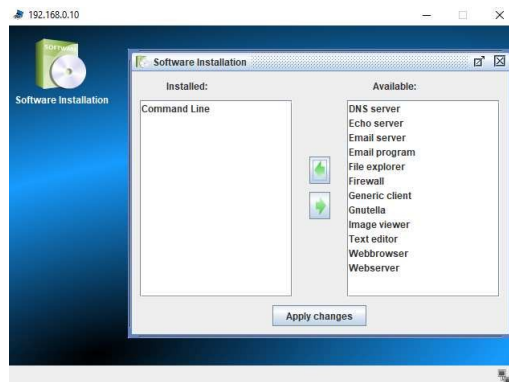
1. Ouvrir le logiciel Filius, saisir le schéma suivant :



2. Sauvegarder le fichier dans le répertoire de travail avec le nom suivant : « Reseau_V0.flx ».
3. Configurer les 2 postes de façon à afficher l'« IP comme nom » du poste et avec les adresses réseaux suivantes : **192.168.0.10** et **192.168.0.11**.
4. Lancer la simulation grâce à l'icône :




Pour valider la connexion d'une machine à une autre sur un réseau, on utilise la commande en ligne « ping ». Pour ce faire, il faut installer le logiciel « Command line » sur les Notebooks du schéma ci-contre.



5. Cliquer sur les Notebooks, puis installer le logiciel « Command line ». Sur l'un des deux Notebooks, cliquer sur l'icône « Command line » puis taper la ligne de commande **root /> ping 192.168.0.11** à partir du notebook 192.168.0.10, ou **root /> ping 192.168.0.10** à partir du Notebook 192.168.0.11. Observer la réponse à l'écran et justifier que les deux Notebooks ont bien communiqué ensemble.

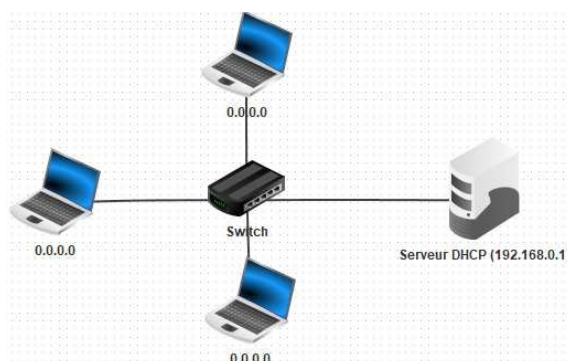


6. Stopper la simulation en cliquant sur l'icône , puis rajouter un 3ème Notebook et le connecter au réseau. Constaté et expliquer le problème.
7. Modifier le réseau en y insérant un « Switch ». Tester par l'intermédiaire de la commande « ping » que tous les Notebooks peuvent communiquer ensemble et ainsi que le nouveau réseau fonctionne.
8. Faire vérifier par le professeur puis sauvegarder le fichier avec le nom « Reseau_V1.flx ».

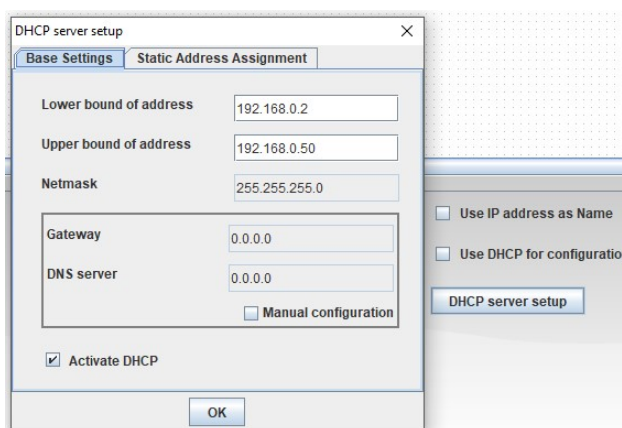
Partie 2 : Réseau LAN adressage dynamique

Si l'on souhaite superviser un réseau de grande taille avec plus de 50 postes, il faudra toujours vérifier que les adresses IP soient correctes et si on veut remplacer ou rajouter un poste, se rappeler les adresses disponibles : c'est une vraie gageure. Heureusement, il existe un protocole qui s'occupe de tout cela pour nous : le **DHCP** qui sera hébergé sur une machine spéciale « un serveur ».

1. Ouvrir le schéma « adressage_dynamique_V0.flw ».



2. Sur le serveur, paramétrer le DHCP de la façon suivante :



3. Lancer la simulation et relever les nouvelles adresses des machines, puis ajouter 2 nouvelles machines **en activant la configuration par DHCP** et constater le bon fonctionnement de tout le réseau grâce à la commande ping.

Ce que nous venons de simuler est un réseau de petite taille de type PAN (*Private Area Network*) ou de type LAN (*Local Area Network*) dans une configuration « étoile ».

Ce qu'il faut retenir dans cette partie :

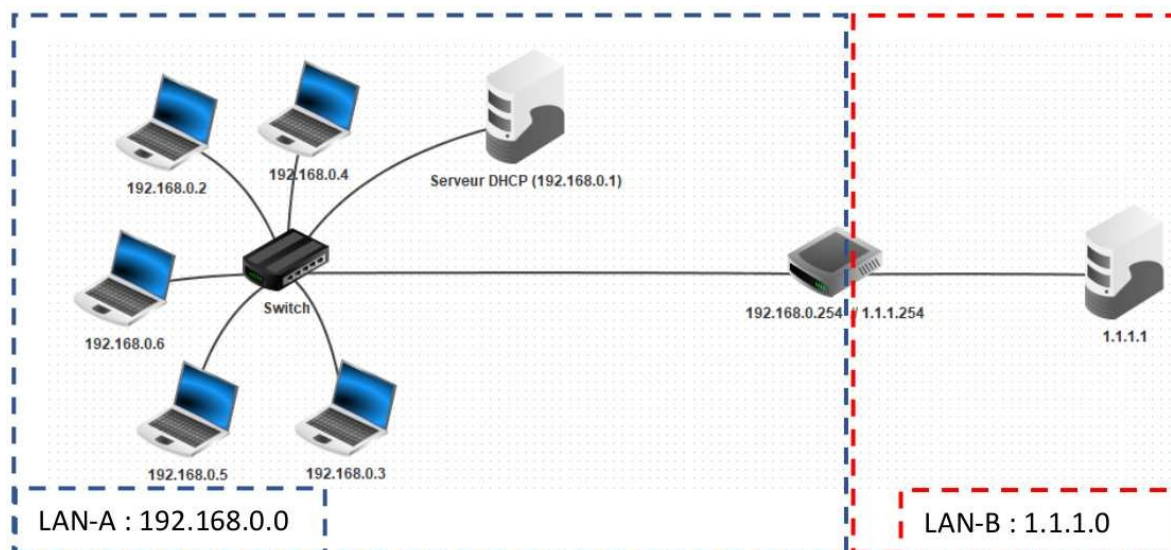
- **Une carte réseau** sur chaque machine.
- Un Switch si on veut étendre le réseau. (Configuration **étoile**)
- Un **protocole** identique. (Ici, c'est le **protocole IP**)
- Des adresses IP qui appartiennent au **même réseau**. Pour savoir si les machines appartiennent au même réseau, on fait des calculs sur les adresses et les masques de sous-réseau (*Netmask*) : cette partie pourra être abordée dans « TD_reseau_V0.pdf* » ou dans l'activité précédente « *Comment monter un réseau local (LAN) pour faire une partie en réseau ?* ».
- On peut simplifier la gestion des adresses IP avec un **serveur DHCP**.

On va maintenant simuler la connexion vers l'extérieur, c'est-à-dire **Internet**.

Pour accéder à un autre réseau, il faut « accéder » à un autre réseau à partir de notre réseau local, ceci se fait par une machine spéciale qui possède au minimum 2 cartes réseau et qui permet de passer d'un réseau à un autre : le **routeur**.

Partie 3 : La passerelle (sortir du réseau)

1. Ouvrir le schéma « Gateway_V0.flx* ».



Sur ce schéma, on retrouve le LAN A précédent en bleu et un nouveau réseau LAN B en rouge. Ces 2 réseaux communiquent au travers du routeur qui possède 2 cartes réseau. **Le routeur possède donc 2 adresses IP : une pour chaque réseau.**

2. Lancer la simulation et « pinguer », à partir de n'importe quel Notebook, le serveur distant à l'adresse IP 1.1.1.1.
3. Observer la réponse et justifier si l'échange s'est correctement déroulé ou non.

Si rien ne se passe, c'est que l'envoi de la commande ping ne sort pas du réseau. Les machines du réseau A ne savent pas comment sortir vers l'extérieur (l'adresse 1.1.1.1 n'étant pas dans le réseau A, c'est donc forcément une adresse distante). Il faut donc renseigner l'adresse de la passerelle (*Gateway*) sur tous les postes. . . ou laisser le serveur DHCP s'en charger pour nous.

4. Configurer de nouveau le serveur DHCP du réseau LAN A en insérant l'adresse de la passerelle, c'est-à-dire l'adresse du routeur qui appartient au réseau LAN A.
5. Sur le LAN B, il n'y a pas de serveur DHCP, Il faut donc paramétrer manuellement l'adresse de la passerelle (*Gateway*) sur le serveur 1.1.1.1. Comme précédemment, la passerelle pour le LAN B correspond à l'adresse du routeur qui appartient au réseau LAN B.
6. Lancer la simulation et tester la communication avec la commande ping. Faire valider par le professeur.
7. Sauvegarder votre fichier avec le nom : « Gateway_V1_OK.flx »

Ce qu'il faut retenir dans cette partie :

- **Un routeur** permet de relier un réseau à un autre.
- Le routeur a au minimum **2 cartes réseau** donc 2 adresses IP. Chacune de ces adresses IP correspond à la passerelle d'un réseau.
- Si on ne configure pas bien l'adresse de la **passerelle** sur les postes du LAN, rien ne sort.

Nous verrons dans la [partie 6](#), un modèle un peu plus crédible de l'Internet, et les protocoles de routage.

Partie 4 : Serveur Web distant

On peut rapidement mettre en place un serveur web sur le serveur 1.1.1.1 en ajoutant le logiciel « *Webserver* » et en l'activant. Ensuite, il faudra ajouter un navigateur (le logiciel « *Webbrowser* ») sur l'un des postes pour pouvoir s'y connecter en tapant son adresse.

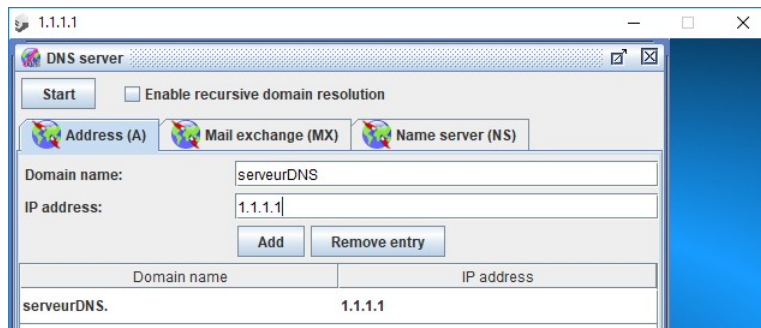
- « Installer » le logiciel **Webserver** sur le serveur 1.1.1.1 et le démarrer.
- « Installer » le logiciel **Webbrowser** sur un des postes du réseau LAN A, le démarrer, puis taper **http://1.1.1.1** dans la **barre d'adresse** pour accéder au serveur Web.
- Vérifier que le site web s'affiche dans le navigateur.
- En installant le logiciel « *Text editor* » sur le serveur, on peut modifier la page *index.html* contenue dans le répertoire *Webserver*. Modifier un peu le texte de la **balise** `<h2>` et relancer le serveur.
- Constater les modifications.
- Sauvegarder votre fichier avec le nom « *ReseauClientServeurV1.flx* ».

Partie 5 : Serveur DNS local

Taper l'adresse du serveur distant n'est pas une chose aisée pour le cerveau humain, il faut se souvenir de toutes les adresses de tous les serveurs que l'on souhaite utiliser... Pour pallier à ce défaut, il a été implémenté un service permettant de nommer les **domaines** (serveur ou ensemble de serveurs) avec des noms plus « humains ». Ainsi, il n'est plus nécessaire de se rappeler les adresses IP mais juste le nom de domaine des serveurs. Ce **service** s'appelle **DNS**.

Les entreprises ou particuliers voulant « inscrire » et divulguer leur nom de domaine le font auprès d'entreprises spécialisées : les « **registrars** ». Ce service n'est pas gratuit. Nous allons simuler de façon extrêmement simplifiée le concept de DNS.

1. Sur le serveur distant 1.1.1.1, installer un nouveau logiciel « *DNS server* » puis le paramétrer comme suit et le démarrer.



On a maintenant un serveur de nom de domaine ou serveur DNS. Il faut maintenant renseigner son adresse sur tous les postes (ou laisser le DHCP le faire pour nous).

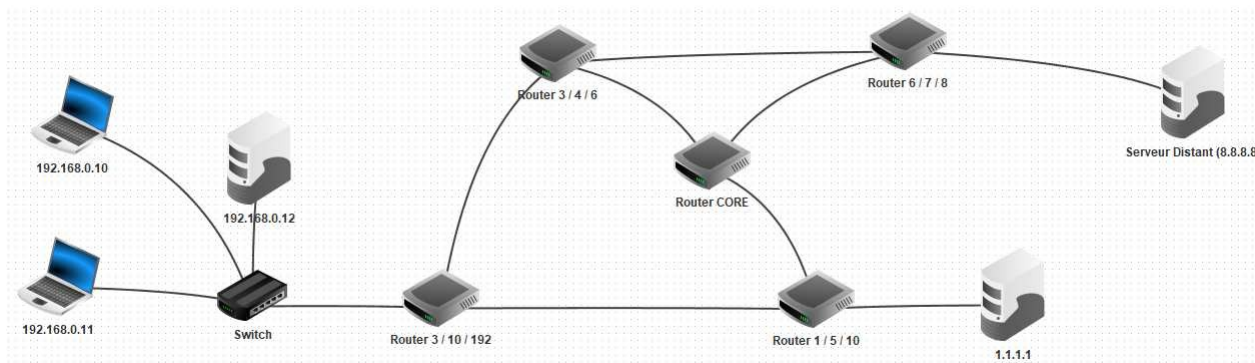
2. Configurer de nouveau le serveur DHCP en insérant l'adresse du serveur DNS.
3. Lancer la simulation et mettre dans la barre d'adresse d'un navigateur **http://serveurDNS**.
4. Constater le bon fonctionnement.
5. Sauvegarder votre fichier avec le nom : « *ReseauClientServeurV2.flx* »

Ce qu'il faut retenir dans cette partie :

- **Le serveur** fournit, par exemple, des pages html... mais il peut faire beaucoup d'autres choses.
- **Le client** se connecte au serveur à travers le réseau.
- Plusieurs clients peuvent se connecter **simultanément** sur le même serveur.
- Le **service DNS** permet de convertir une adresse **symbolique** en une adresse **logique**.

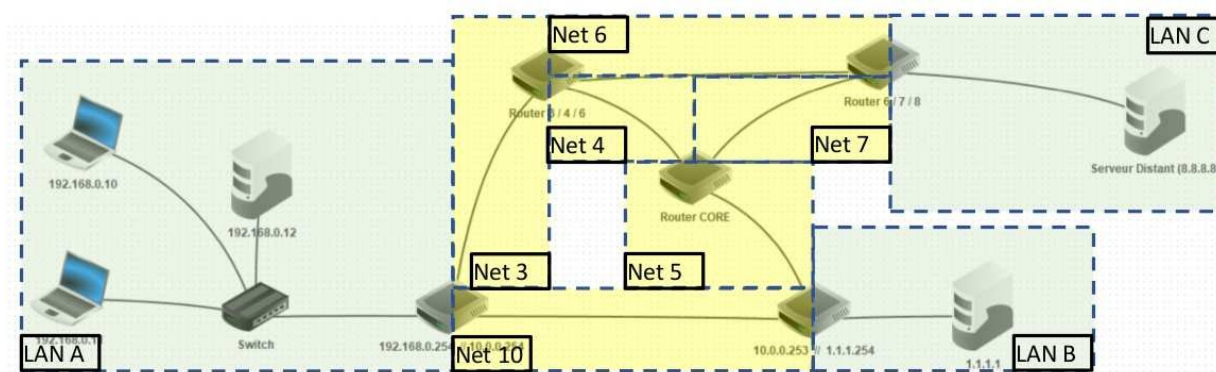
Partie 6 : Routage statique

Le schéma suivant permet de reproduire un peu plus le fonctionnement d'internet. Les paquets (informations) sont transmis à travers le réseau de routeur en routeur. Le protocole utilisé, appelé « **TCP** », permet de garantir que les paquets seront transmis (si aucun routeur critique n'est en panne).



Sur le schéma ci-dessous, on retrouve au total 9 « réseaux ». Les trois réseaux de couleur verte « LAN A, B, C » sont des réseaux locaux que nous connaissons déjà.

Les réseaux jaunes « NET 3, 4, 5, 6, 7, 10 » font partie du réseau des réseaux, c'est-à-dire Internet (qui est un WAN). Ils ne contiennent que des routeurs mais peuvent éventuellement relier d'autres LAN et ne représentent, bien sûr, qu'une infime partie du réseau réel (plusieurs millions de routeurs).



Destination	Netmask	Next gateway	NIC
3.3.3.254	255.255.255.255	127.0.0.1	127.0.0.1
10.0.0.254	255.255.255.255	127.0.0.1	127.0.0.1
192.168.0.254	255.255.255.255	127.0.0.1	127.0.0.1
3.3.3.0	255.255.255.0	3.3.3.254	3.3.3.254
10.0.0.0	255.255.255.0	10.0.0.254	10.0.0.254
192.168.0.0	255.255.255.0	192.168.0.254	192.168.0.254
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
0.0.0.0	0.0.0.0	3.3.3.253	3.3.3.254
1.1.1.0	255.255.255.0	10.0.0.253	10.0.0.254

La table de routage ci-contre est celle du routeur entre le LAN A et le Net 10. On y retrouve les 4 colonnes :

- Destination (réseau à atteindre)
- Masque de sous-réseau de ce réseau
- Passerelle (adresse du prochain routeur)
- NIC (interface de sortie à utiliser pour envoyer le paquet vers le prochain routeur)

En grisé, apparaissent, dans le tableau ci-dessus, les lignes définies « automatiquement ». Elles concernent les adresses réseaux correspondant aux adresses des interfaces (paramétrage initial).

- L'adresse 127.0.0.1 est une adresse spéciale qui renvoie sur la machine elle-même.

En noir, apparaissent, dans le tableau ci-dessus, les « entrées » manuelles. Elles précisent le comportement du routeur pour des réseaux connus ou non.

- L'adresse 0.0.0.0 et son masque 0.0.0.0 définissent une adresse réseau inconnue. On peut voir ici que pour les adresses inconnues, le routeur passe les paquets au routeur 3/4/6 en relayant vers 3.3.3.253 à partir de l'interface 3.3.3.254, le réseau Net 3 étant commun à ces 2 routeurs.

4. Relever les tables de routage des 2 routeurs impliqués dans cette communication et vérifier la cohérence entre les tables de routage et le résultat de la commande « **tracert** ».
5. Exécuter une commande en ligne « **tracert** » depuis le LAN A vers le serveur 8.8.8.8 du LAN C.
6. A partir des adresses IP rencontrées lors du routage des paquets entre le LAN A et le LAN C, surligner sur le [document-réponse](#), le trajet de ces paquets et noter les réseaux par lesquels ils passent. Le chemin suivi est-il optimal ?
7. Sauvegarder ce fichier sous « reseau_routage_test.flv » et ajouter des nouvelles entrées dans la table de routage du routeur 3/4/6 et celle du routeur 6/7/8 pour optimiser le trajet entre le LAN A et le LAN C.
8. Exécuter une commande en ligne « **tracert** » depuis le LAN A vers le serveur 8.8.8.8 du LAN C et vérifier que le trajet des paquets a bien été optimisé.
9. Exécuter une commande en ligne « **tracert** » depuis le serveur 8.8.8.8 du LAN C vers le LAN A et vérifier que le trajet des paquets est aussi optimisé.

Ce qu'il faut retenir dans cette partie :

- Le **protocole IP** permet de router les données dans un réseau.
- Les routeurs connaissent le chemin vers quelques réseaux dans des **tables de routage**.
- Il existe un chemin « **par défaut** » ou du « **dernier recours** » quand le réseau n'est pas connu.
- Certains routeurs forment comme une épine dorsale (**backbone**) de l'Internet (ils connaissent beaucoup de chemins).


Partie 7 : Routage dynamique

Le routage statique est réalisable « à la main » mais est assez pénible pour l'administrateur réseau. Mais que se passe-t-il sur un très grand nombre de routeurs et/ou lorsque les machines n'appartiennent pas à une seule entité ?

Le fonctionnement du routage à grande échelle n'est pas du ressort des humains et il existe des protocoles permettant d'auto-configurer les routeurs de façon dynamique. Les routeurs s'adaptent en fonction de l'état des autres et parviennent à trouver des routes malgré les pannes, les coupures électriques. . .

1. Ouvrir le schéma « reseau_routage_V4.flis » et régler la vitesse de simulation à 40%.
2. Configurer l'ensemble des 5 routeurs sur « *Automatic Routing* » et lancer la simulation.
3. Refaire l'ensemble des **tracert** et remarquer quelques différences sur les routes utilisées.
4. Retirer quelques connections (non cruciales) entre des routeurs et relancer les tests.

Exemple de routeur « Backbone » de chez *Huawei*

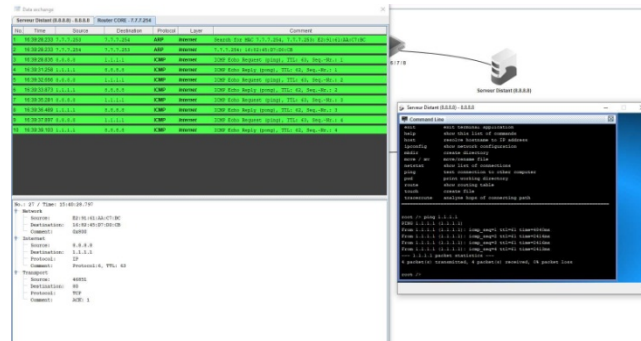
	Paramètres	NE9000-20
	Capacité de commutation	209 Tbit/s
	Performances de transmission	36 160 Mpps
	MPU	2
	SFU	8
	Emplacements	20
	Types de ports	400GE, 100GE, 40GE et 10GE
	Consommation d'énergie typique	0,4 W/G
	Dimensions (H x L x P)	2200 mm x 600 mm x 1000 mm (49,5U) Le NE9000 présente une armoire unique et s'adapte aux installations sans armoire

Source : <https://e.huawei.com/fr/material/onLineView?MaterialID=6a63b272f4a44e6d85a6a00672d22b58>

Partie 8 : Trames et paquets

Pour mieux comprendre les échanges entre machines, on va regarder ce qui se passe au niveau des routeurs et comment les différents protocoles entrent en jeu.

1. Ouvrir le schéma « reseau_routing_V4.flw ».
2. Lancer la simulation et afficher les échanges de l'interface 7.7.7.254 sur le routeur CORE. Dans le même temps, on va envoyer un ping depuis le serveur 8.8.8.8 vers le serveur 1.1.1.1. Disposer les fenêtres



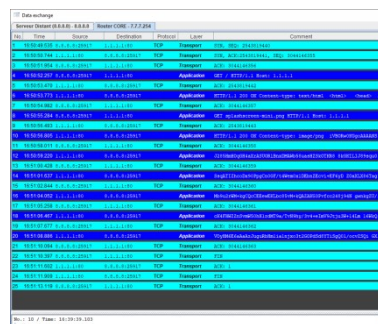
de façon à obtenir observer les deux en même temps.

Si tout se passe bien, vous devez observer un affichage qui ressemble à celui-ci-dessus (la visibilité est intentionnellement tronquée car c'est juste un aperçu). Ceci est l'ensemble des trames qui circulent sur l'interface de façon chronologique.

3. Indiquer le nom des protocoles utilisés durant le ping et la couche (*layer*) correspondante.
4. Faire une copie d'écran et annoter, au maximum, les trames qui apparaissent.

Les trames utilisées pour un ping sont de « bas niveau ». On va aller plus loin, en chargeant une page HTML depuis un serveur distant.

5. Effacer la page contenant les trames.
6. Lancer le « Webserver » présent sur le serveur 1.1.1.1, puis sur le serveur 8.8.8.8, lancer le « Webbrowser » en indiquant `http://1.1.1.1` dans la barre d'adresse.



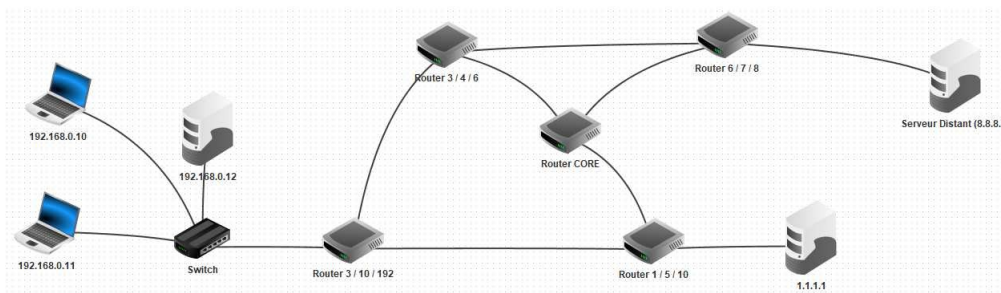
7. Indiquer le nom des protocoles utilisés durant le chargement de la page et les couches (*layer*) correspondantes.
8. Pourquoi l'image est coupée en plusieurs paquets ?
9. Faire une copie d'écran et annoter, au maximum, les trames qui apparaissent.

- Le logiciel d'analyse des trames s'appelle « *sniffer* » en anglais.
- Les différentes couches « **RESEAU**, **INTERNET**, **TRANSPORT** et **APPLICATION** » constitue le modèle TCP/IP.
- TCP assure que les paquets arrivent à bon port grâce à un mécanisme de numérotation et d'acquittements : SYN, ACK.

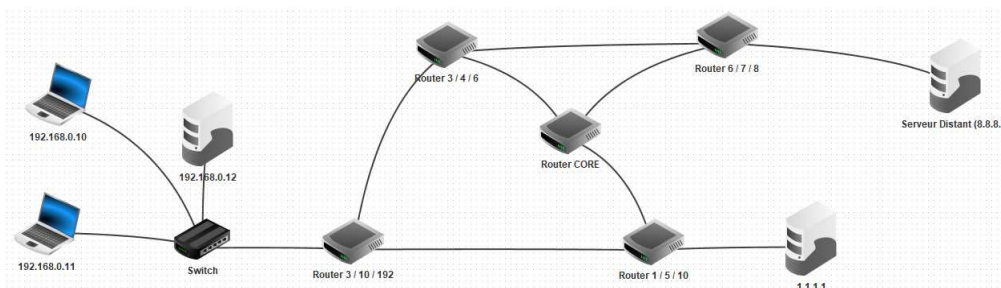
Nom :
Prénom :

Document-Réponse

1. Schémas à compléter



Commentaires :



Commentaires :

Routeur 3/4/6

Forwarding table			
Destination	Netmask	Next gateway	NIC
6.6.6.254	255.255.255.255	127.0.0.1	127.0.0.1
4.4.4.254	255.255.255.255	127.0.0.1	127.0.0.1
3.3.3.253	255.255.255.255	127.0.0.1	127.0.0.1
6.6.6.0	255.255.255.0	6.6.6.254	6.6.6.254
4.4.4.0	255.255.255.0	4.4.4.254	4.4.4.254
3.3.3.0	255.255.255.0	3.3.3.253	3.3.3.253
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
0.0.0.0	0.0.0.0	4.4.4.253	4.4.4.254
192.168.0.0	255.255.255.0	3.3.3.254	3.3.3.253

Routeur 6/7/8

Forwarding table			
Destination	Netmask	Next gateway	NIC
8.8.8.254	255.255.255.255	127.0.0.1	127.0.0.1
6.6.6.253	255.255.255.255	127.0.0.1	127.0.0.1
7.7.7.253	255.255.255.255	127.0.0.1	127.0.0.1
8.8.8.0	255.255.255.0	8.8.8.254	8.8.8.254
6.6.6.0	255.255.255.0	6.6.6.253	6.6.6.253
7.7.7.0	255.255.255.0	7.7.7.253	7.7.7.253
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
0.0.0.0	0.0.0.0	7.7.7.254	7.7.7.253

2. Tables de routage à modifier (partie noir)

