Université Nice SOPHIA ANTIPOLIS

L3 Miage, 24 janvier 2019

TP-3 Réseaux : Couche liaison

1 Objectifs pédagogiques

L'objectif de ce TP est de se familiariser avec les principales fonctions la couche liaison. Pour cela, on va utiliser le logiciel de formation `Cisco Packet Tracer`.

2 Consignes

Ressources : Vous pouvez utiliser les matériels du cours (slides de CM, TPs passés, ...) ainsi que toute ressource disponible sur Internet.

3 Installer Cisco Packet Tracer

`Cisco Packet Tracer` est un simulateur de matériel réseau `Cisco` (routeurs, commutateurs). Le but de `Packet Tracer` est d'offrir aux élèves et aux professeurs un outil permettant d'apprendre les principes du réseau, en acquérant principalement des compétences aux technologies spécifiques de Cisco. Donc, il est utilisé principalement pour s'entraîner, se former, et préparer les examens des certifications de Administrateur Réseaux Cisco. Cependant, il constitue aussi un outil assez complet pour faire de la simulation réseau dans un cadre pédagogique en dehors des formations certifiantes Cisco.

Vous pouvez le télécharger gratuitement depuis `https://www.netacad.com/fr/courses/packet-tracer/introduction-packet-tracer` à condition de s'inscrire à la *Cisco Networking Academy* et lancer le cours *Introduction to Packet Tracer*, cours de 10h en anglais que je vous conseille de suivre. Le logiciel est disponible pour *Linux* et pour *Windows*, mais pas pour *Mac*. Si vous utilisez *Mac*, le plus simple c'est d'avoir une machine virtuelle *Linux*. Notez que une fois `Packet Tracer` installé, vous aurez besoin de votre compte *Cisco Networking Academy* pour vous loguer dans le logiciel et le démarrer. *Donc, ne manquez pas l'inscription ! ! !*

4 Démarrer Cisco Packet Tracer

`Cisco Packet Tracer` est déjà installé sur les machines de la salle. Notez que le chemin par défaut de l'installation est `/opt/pt`, ce qui implique que pour le lancer il faut taper dans la ligne de commande `/opt/pt/packettracer` car on n'a pas fait de liens symboliques dans `/usr/local/bin`. Si vous avez installé `Cisco Packet Tracer` dans votre ordinateur, taper directement `/packettracer` dans la ligne de commande, cela suffira normalement.

La première fois que vous démarrez le logiciel, il faut se loguer avec l'identifiant (ou adresse email) que vous utilisé pour vous inscrire. Si vous ne sortez pas du *login*, il ne faudra pas le retaper dans les prochaines séances.

En plus du materiel officiel que vous pouvez trouver sur la *Cisco Networking Academy*, un manuel en francais très simple de prise en main est disponible sur `http://www.siloged.fr/cours/docs/manuels/doc_packettracer.pdf`. De toute façon, vous pouvez le trouver aussi dans le site du TP.

5 Configuration initiale du réseau

D'abord, on va configurer un réseau simple comme celui montré dans la Fig. 1. Notez que les ordinateurs sont connectés par un *hub*, donc le support physique est partagé par tous les ordinateurs. On verra les consequences de ce choix dans les prochaines sections. Ce simple réseau nous permettra de se familiariser

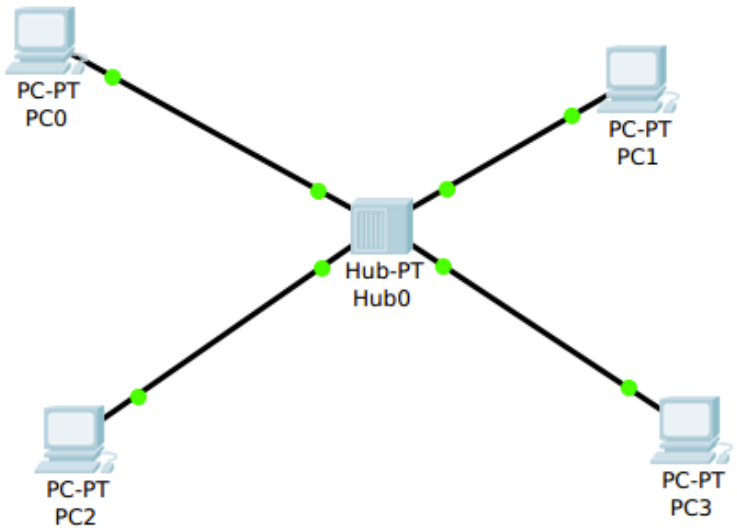

FIGURE 1 – Réseau avec un hub

avec `Cisco Packet Tracer`.

Créez le réseau de la Fig. 1 en sélectionnent dans le panel inférieur quatre ordinateurs dits "génériques" (`End Devices` → `End Devices` → `Generic`) et un hub (`Network Devices` → `Hubs` → `Generic`). Connectez les dispositifs en sélectionnent du paire torsadé droit (`Connections` → `Copper Straigh-Through`). Celui-ci correspond au cable Ethernet typique qu'on utilise normalement pour connecter un appareil hôte à un dispositif réseau (hub, switch ou router).

Afin de pouvoir démarrer une simulation, il faut encore configurer les cartes réseaux des PCs. Vous allez le faire pour `PC0`, `PC1` et `PC2`. Cliquez sur chaque PC, allez vers `Config`→ `FastEthernet`→ `IP Configuration` et dans la champ `IP address` saisissez `192.168.1.1`. Le champ `Subnet mask` se remplira automatiquement avec la bonne valeur de `255.255.255.0`. Pour l'instant, peut-être, cela ne vous dites rien, mais vous verrez dans le prochaines séances. Répétez la manipulation avec `PC1` et `PC2`, en leur attribuant les adresses IP `192.168.1.2` et `192.168.1.3`, respectivement.

Avant de continuer, on va s'arrêter sur le niveau de réalisme du simulateur. `Cisco Packet Tracer` implemente les fonctionnalités basiques des dispositifs émulés. De cette façon, pour les ordinateurs, il y a un remède de `Desktop` avec des applications système et réseaux les plus courantes. Il y a aussi un petit environment de programmation (onglet `Programming`) qui nous permet de coder des applications réseaux simples en utilisant des APIs en `JavaScript` et en `Python`. Maintenant, je vous demande d'accéder au `Desktop` → `Command Prompt` de l'un des PCs et taper la commande `help` ou `?`. Cela vous affichera les commandes disponibles. Vous retrouverez les commandes minimales d'un système et quelques commandes basiques réseaux. Notez que la console affichée rappelle à celle de Windows (processus `cmd.exe`, *Windows Command Prompt*). Donc, vous retrouverez plûtot la syntaxe qu'on retrouve sur Windows, même si ces commandes sont aussi assez similaires aux commandes UNIX. Vérifiez que la configuration des adresses IP a été bien prise en compte par le biais de la commande `ipconfig` (sous UNIX, la commande est `ifconfig`). Vous pouvez profiter aussi pour taper la commande `arp -a`. Normalement, vous verrez que les tableaux ARP des PCs sont encore vides, puisque vous venez de démarrer et configurer les dispositifs.

6 Un test simple de communication

Dans cette section, on va procéder à faire un test simple de communication entre deux dispositifs, c.-à.-d. un *pinger* une machine distante (destination) depuis une machine local (source). Cette expression vient de la commande classique utilisé sur le terminal pour l'executer : la commande `ping`. Cette commande génère un datagramme ICMP (*Internet Control Message Protocol*) de type requête (le ping) avec le but d'attendre la machine distante et déclencher une réponse ICMP (le pong) de sa part qui sera retournée vers la machine appelante. De cette manière, la machine à l'origin du ping peut tester qu'il y a bien de la connectivité jusqu'à la couche 3 (Réseau).

A ce comment-là, on peut démarrer notre première simulation `Packet Tracer`. Pour cela, passez en mode `Simulation` en cliquant le symbole du chronomètre en bas à droite. Notez qu'en haut à droite, vous avez la liste d'événements `Event List`. C'est le même concept qu'on avait étudié dans le premier TP de réseau. En effet, `Packet Tracer` est un vraie simulateur à événements discrets, où les évènements sont encore une fois les arrivés et les departs de paquets des dispositifs. Cliquez dans le bouton `Edit Filters` et sélectionnez le protocoles `ARP` et `ICMP`. Cela veut dire qu'uniquement les échanges concernants ces deux protocoles seront affichés dans le panel `Simulation / Event list`.

Cliquez dans le symbole d'enveloppe fermé (tout à droite) pour programmer le *ping* : l'envoie d'un datagramme ICMP encapsulé dans une trame Ethernet. Comme il s'agit de tester si deux dispositifs peuvent se communiquer, il faut sélectionner la source et la destination de la communication. Donc, il faut cliquer une première fois sur l'ordinateur qui fera de source (`PC0`), et une deuxième fois sur celui qui fera de destination `PC1` [1]. Vous verrez qu'un événement *depart* d'un datagramme ICMP depuis `PC1` est maintenant programmé pour l'instant temporel `0.000` seconds dans la `Event list`. Au long de la simulation, vous verrez la `Event List` se remplir avec les departs des paquets (date programmé de depart depuis chaque dispositif). Si vous cliquez sur un événement vous aurez accès : (1) à un petit descriptif sur ce qui se passe et où dans le modèle OSI (onglet `OSI model`), (2) au format de la PDU à l'arrivé (`Inbound PDU Details`) et (3) au format de la PDU à la sortie (`Outbound PDU Details`) : oui, car une machine peut modifier une PDU [2] avant de la relayer ! ! ! Notez que le format de la PDU de chaque couche est affichée séparément en ordre descendant, c.-à.-d., tout en haut, vous aurez les champs de la PDU de la couche 2, et ensuite les champs de la PDU de la couche 3 jusqu'à arriver à la couche la plus haute du paquet, tout en bas. Maintenant, vous cliquez sur `Capture / Forward` pour faire avancer d'un pas la simulation. Normalement vous verrez que une requête ARP (*Address Resolution Protocol*) va se programmer automatiquement pour le même instant que la requête ICMP.

Question 1 : Pourquoi cette requête ARP a apparu automatiquement ? Consultez le format du datagramme ICMP. En sachant, que le protocole ICMP est placé à la couche 3, est-ce qu'il vous manque quelque chose dans son format ?

Vous cliquez sur `Capture / Forward` pour commencer la simulation. Notez que la requête ARP se déplace jusqu'au hub et qu'un nouvel événement *depart* est maintenant programmé pour l'instant temporel `0.001` seconds, cette fois-là depuis depuis le hub. Consultez le format de la requête ARP.

Question 2 : Dans quel champ de quel protocole pouvez vous retrouver l'adresse MAC de la machine destinataire de la requête ARP ? Quelle est sa valeur ? Pourquoi ?

Question 3 : Dans quel champ de quel protocole pouvez vous retrouver les adresses MAC et IP de la machine source de la requête ARP ? Quelle est leur valeur ?

Question 4 : Dans quel champ de quel protocole pouvez vous retrouver l'adresse IP de la machine dont on veut obtenir son adresse MAC (la machine objectif de la requête ARP) ? Quelle est leur valeur ?

1. Il est également possible de générer une requête ICMP en ouvrant le `Command Prompt` du `PC0` et en tapant là-bas la commande `ping 192.168.1.2`
2. Je vous rappelle que les paquets de données sont appelés `PDU: Protocol Data Unit` dans un jargon plus technique.

Vous re-cliquez sur `Capture / Forward` et la requête ARP arrive heureusement à destination. Tapez au nouveau la commande `arp -a` dans tous les PCs.

Question 5 : Quels sont les PCs qui ont reçu la requête ARP ? Pourquoi ?

Question 6 : Quels sont les PCs qui ont mis à jour leurs tableaux ARP ? Pourquoi ?

Une réponse ARP viens d'être créer dans le `PC1`. Continuez avec la simulation en cliquant sur `Capture / Forward` jusqu'au moment où la réponse ARP arrive à sa destination. Tapez au nouveau la commande `arp -a` dans le `PC0`.

Question 7 : Dans quel champ de quel protocole pouvez vous retrouver l'adresse MAC de la machine destinataire de la réponse ARP ? Quelle est sa valeur ? Pourquoi ?

Question 8 : Dans quel champ de quel protocole pouvez vous retrouver les adresses MAC et IP de la machine source de la réponse ARP ? Quelle est leur valeur ?

Question 9 : Comment-est que vous savez que c'est une reponse ?

Question 10 : Quels sont les PCs qui ont reçu la réponse ARP ? Pourquoi ?

Question 11 : Quels sont les PCs qui ont mis à jour leurs tableaux ARP ? Pourquoi ?

A ce moment, la requête ICMP qui était à l'origine de tous ces échanges peut partir de `PC0`. Cliquez sur les détails de la PDU.

Question 12 : Détaillez la suite d'encapsulations de la requête ICMP ?

Question 13 : Retrouve le type et le code de la requête ICMP ? Qu'est ce qu'ils veulent dire ? (NOTE : reviser les slides du CM4 Réseau.)

Continuez avec la simulation en cliquant sur `Capture / Forward` jusqu'au moment où la requête ICMP arrivera à sa destination.

Question 14 : Quels sont les PCs qui ont reçu la requête ICMP ? Pourquoi ?

Question 15 : Quel est le PC qui répond ? Pourquoi ?

Une réponse ICMP viens d'être créer dans l'un des PCs. Continuez avec la simulation en cliquant sur `Capture / Forward` jusqu'au moment où la réponse ICMP arrive à sa destination.

Question 16 : Quels sont les PCs qui ont reçu la réponse ICMP ? Pourquoi ?

Question 17 : Quels sont les PCs qui ont décapsulé la réponse ICMP ? Pourquoi ?

Allez dans le `PC3` et configurez l'interface réseau en attribuant l'adresse IP `192.168.1.2`. Notez que cette adresse est déjà attribuée au `PC1`. Donc, il faudra changer l'adresse du `PC1` à p. ex. `192.168.1.4`. Maintenant cliquez sur `Capture / Forward`. Normalement, un requête ARP gratuite (*gratuitous ARP*) vient d'être générée par le simple fait de configurer par première fois l'interface réseau de `PC3`.

Question 18 : Dans quel champ de quel protocole pouvez vous retrouver l'adresse MAC de la machine destinataire de la requête ARP ? Quelle est sa valeur ? Pourquoi ?

Question 19 : Dans quel champ de quel protocole pouvez vous retrouver les adresses MAC et IP de la machine source de la requête ARP ? Quelle est leur valeur ?

Question 20 : Dans quel champ de quel protocole pouvez vous retrouver l'adresse IP de la machine dont on veut obtenir son adresse MAC (la machine objectif de la requête ARP) ? Quelle est leur valeur ? Pourquoi ?

Vous re-cliquez sur `Capture / Forward` le nombre des fois nécessaires pour faire arriver la requête ARP gratuite à sa destination. Tapez au nouveau la commande `arp -a` dans tous les PCs.

Question 21 : Quels sont les PCs qui ont reçu la requête ARP gratuite ? Pourquoi ?

Question 22 : Quels sont les PCs qui ont mis à jour leurs tableaux ARP ? Pourquoi ? Notez la valuer de l'adresse IP de la machine objectif de la requête ARP.

Allez chez `PC0`, ouvrez son `Command Prompt` et tapez `ping 192.168.1.2`. Cela refera le test de communication antérieur. Cliquez sur `Capture / Forward` jusqu'au moment où la requête ICMP arrivera à sa destination.

Question 23 : Quels sont les PCs qui ont reçu la nouvelle requête ICMP ? Pourquoi ?

Question 24 : Quel est le PC qui répond ? Est-il est le même qu'avant ? Pourquoi ?

Si vous continues la simulation, vous verrez que la commande `ping 192.168.1.2` génère jusqu'à quatre échanges ICMP.

7 Des collisions

Dans cette section, on va étudier le concept de collision. Pour cela, simplement, générez deux requêtes ICMP simultanées en utilisant le symbole d'enveloppe fermé (tout à droite). Programmez la première requête ICMP depuis le `PC0` vers le `PC3`, et la deuxième requête ICMP depuis le `PC1` vers le `PC2`. En dependant des états de tableaux ARP à ce point du TP, vous verrez partir les deux requêtes ICMP au même moment, ou plus probablement, une requête ICMP et une requête ARP depuis `PC0` et `PC1`. Cliquez sur `Capture / Forward` jusqu'à la fin de la simulation.

Question 25 : Qu'est ce qui se passe au hub ? Pourquoi ?

Question 26 : Est-ce que les PCs sont informés sur ce qui vient de se passer au hub ? Comment ? NOTE : Reviser les slides du cours.

8 Du hub au switch

Pour continuer vous allez remplacer le hub avec un switch ((`Network Devices` → `Switches` → `2960`) pour metre en place un réseau comme celui montré dans la Fig. 2. assurez vous que les tableaux ARP des tous les PCs sont vides. Pour cela, rendez vous sur les *Command Prompts* de tous les PCs et tapez `ARP -d` pour effacer les tableaux.
Vérifiez l'état du tableau de `forwarding` du switch. Pour cela tapez `show mac address-table` sur le `IOS Command Line Interface` (onglet CLI). Normalement le tableau est aussi vide. Désormais, on va répéter les experiences précédentes mais avec un switch à la place d'un hub. Programmez à nouveau une requête ICMP depuis le `PC0` vers le `PC1`. A nouveau une requête ARP pour obtenir l'adresse MAC du `PC1` va être envoyé depuis `PC0`. (Il se peut que des requêtes ERP gratuites soient aussi générées depuis

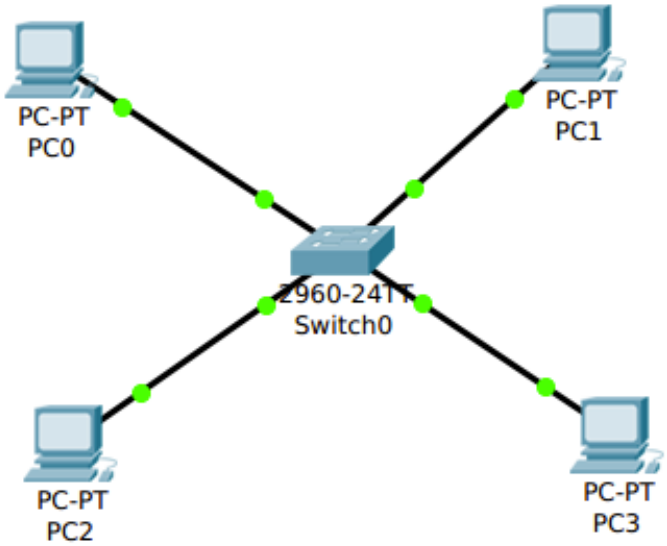

FIGURE 2 – Réseau avec un switch

`PC1`.) En tout cas, si vous cliquez sur `Capture / Forward` une ou plusieurs requêtes ARP vont arriver au switch. Tapez à nouveau `show mac address-table`.

Question 27 : Est-ce que le tableau de `forwarding` du switch a changé ? Pourquoi ?

Continuez avec la simulation en cliquant sur `Capture / Forward` jusqu'au moment où les requêtes ARP arrivent à sa destination.

Question 28 : Quels sont les PCs qui ont reçu les requêtes ARP (gratuites ou pas) ? Pourquoi ?

Question 29 : Quels sont les PCs qui ont mis à jour leurs tableaux ARP ? Pourquoi ?

Normalement, s'il y avait requêtes gratuites, elles ont échouées. Cela est dû au fait que `Packet Tracer` assume que toute requête ARP *gratuite* (qui ne cible pas une machine avec une adresse IP particulière) en provenance d'une machine inconnue est jetée par mesure de precaution. Cela est une sécurité souvent implémentée dans les ordinateurs. Notez que une requête ARP *normale* vient aussi d'une machine inconnue, mais elle cible une machine particulière, qui éventuellement traitera la requête.

Cliquez sur `Capture / Forward` pour observer maintenant l'envoi de la requête ICMP originalement programmée.

Continuez avec la simulation en cliquant sur `Capture / Forward` jusqu'au moment où la requête ICMP arrivera à sa destination.

Question 30 : Est-ce que les mêmes PCs qu'auparavant ont reçu la requête ICMP ? Pourquoi ?

Une réponse ICMP viens d'être créer dans l'un des PCs. Continuez avec la simulation en cliquant sur `Capture / Forward` jusqu'au moment où la réponse ICMP arrive à sa destination.

Question 31 : Est-ce que les mêmes PCs qu'auparavant ont reçu la réponse ICMP ? Pourquoi ?

Question 32 : Est-ce que le switch a eu besoin de connaitre les adresses IP dans les échanges précédents ? Pourquoi ?

9 Le tableau de `forwarding` du switch

Dans le section précédente, on a vu que le role qui joue le tableau de *forwarding* du switch, mias vous este sure d'avoir bien compris comment le switch apprend ce tableau ? Allez dans le `IOS Command Line Interface` du switch et passez au mode privilégié en tapant `enable`. Vous noterez que `>` est remplacé avec `#` au debut de la ligne de commandes. Maintenant, effacez le tableau en saisissant `clear mac address-table`. Allez dans le `PC0` et tapez sur `Command Prompt` `ping 192.168.1.3`. Cela générera quatre requêtes ICMP à destination de `192.168.1.3`. J'attire votre attention sur le fait que cette requête ICMP de type echo (un ping) n'est pas *broadcast* sinon *unicast*, pas comme les requêtes ARP qui sont par definition *broadcast*.

Question 33 : Quels sont les PCs qui reçoivent la premiere requête ICMP ? Pourquoi ?

Regardez tableau de forwarding du switch après le passage de la réponse ICMP.

Question 34 : Quels sont les PCs qui reçoivent les suivantes requête ICMP ? Pourquoi ?

10 Des collisions dans un switch ?

Répétez maintenant l'experience décrite dans la Section 7.

Question 35 : Qu'est ce qui se passe au switch maintenant ? Pourquoi ?