TD/TP Réseaux n°1: Rappels Réseaux

Notions abordées:

Le but de ce TP est de rafraichir vos connaissances sur les notions acquises dans le module M212 telles que

- les commandes permettant des tests de connectivité au niveau local et sur internet
- utiliser un outil d'analyse de trames tel que Wireshark pour analyser les protocoles tels que:
  - IP (TTL, @IP,..)
  - ARP
  - Ethernet : adressage mac
  - ICMP type Echo, Reply, Time exceeed
  - Encapsulation de protocoles avec traceroute, Ping,

Vous utiliserez essentiellement le logiciel Wireshark disponibles sur les PCs des salles de TP.
Vous utiliserez également PacketTracer V7 en vous connectant avec votre compte net académie créé en S2 sur https://www.netacad.com/courses/packet-tracer

A. Manipulations sous Wireshark

1) Commandes système

- Relever la configuration réseau de votre poste de travail. Commande *ipconfig*

2) Captures de flux issus de différentes commandes :

1. Ouvrez Wireshark et lancez la capture de trames sur votre interface réseau.
   - Dans la fenêtre de commande, visualisez la table arp de votre machine *arp -a*
   - Faite un ping *@ip-de-votre-voisin* ou toute autre adresse.
   - Refaites un ping sur la même adresse. deuxième ping par rapport au tout premier paquet envoyé ?
   - Arrêter la capture à la réception du résultat
   - Sauvegarder le fichier sous *captureArp*

   a. Sur votre fenêtre de commande, que constatez-vous sur le temps d'exécution entre les deux pings successifs ? Expliquez pourquoi cette différence.

2. Ouvrez Wireshark et lancez la capture de trames sur votre interface réseau.
   - Dans la fenêtre de commande : ping www.unice.fr ou toute autre adresse.
   - Arrêter la capture à la réception du résultat
   - Sauvegarder le fichier sous *capturePing*

3. Relancez la capture de trames sur votre interface réseau
   - Dans la fenêtre de commande : tracert www.google.fr ou toute autre adresse.
   - Arrêter la capture à la réception du résultat
   - Sauvegarder le fichier sous *captureTraceroute*

3) Analyse flux ARP

Pour répondre aux questions suivantes, utiliser le résultat de la *captureARP.pcapng*

- Quels sont les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames capturées ?

- Quelles sont les longueurs des messages échangés par les différents protocoles ?

Étude du paquet IP correspondant au premier message ARP Request.

Caractéristiques Ethernet:

- Quelle est l'adresse MAC source de la trame Ethernet ?
- Quelle est l'adresse MAC destination trame Ethernet ?

Caractéristiques ARP :

- Quelle est la taille du paquet ARP ?
- Quelle est la valeur du champ Protocol Type contenu dans le message ARP ?
- Quelle est l'adresse IP Source du paquet ARP ?
- Quelle est l'adresse IP destination du paquet ?
- Quelle est l'adresse MAC Source incluse dans le message ARP ?
- Quelle est l'adresse MAC Destination incluse dans le message ARP ?

Étude du paquet IP correspondant au second message ARP Reply

Caractéristiques Ethernet:

- Quelle est l'adresse MAC source de la trame Ethernet ?
- Quelle est l'adresse MAC destination trame Ethernet ?

Caractéristiques ARP :

- Quelle est la taille du paquet ARP ?
- Quelle est la valeur du champ Protocol Type contenu dans le message ARP ?
- Quelle est l'adresse IP Source du paquet ARP ?
- Quelle est l'adresse IP destination du paquet ?
- Quelle est l'adresse MAC Source incluse dans le message ARP ?
- Quelle est l'adresse MAC Destination incluse dans le message ARP ?

4) Analyse flux ICMP

Pour répondre aux questions suivantes, utiliser le résultat de la *capturePing.ws*
Sélectionner à la souris les octets de données du message de requête. Comparer ces données avec celles affichées dans la fenêtre d'affichage brut.

Message ICMP «Echo Request»

- Quelle est la taille l'en-tête ? Quelle la taille des données transportées,
- Quel est le type de message ICMP ?

- Quel est son identificateur[1] ?
- Quel est le numéro de séquence[2] ?
- Quelle est l'adresse IP destination du paquet ?
- Quelle est la valeur du champ Protocol Type ?
- Quelle est la valeur du champ Time to Live ?

Message ICMP «Echo Reply»

- Quel est le type de message ICMP ?
- Quel est son identificateur ? (A comparer à la requête question)
- Quel est le numéro de séquence ?
- Quelle est l'adresse IP destination du paquet ?
- Quelle est la valeur du champ Protocol Type ?
- Quelle est la valeur du champ Time to Live ?

- Comparer ces données avec celles affichées dans le message de requête.
- Comment le champ de séquence évolue dans le temps ?
- Calculer l'écart de temps entre l'émission de chaque message Echo Request et la réception de chaque message Echo Reply.
- Comparer les résultats avec les valeurs maximum, moyenne et minimums fournis par la commande ping.

5) Analyse traceroute

Pour répondre aux questions suivantes, utiliser le résultat de la *captureTraceroute.ws*

Protocoles capturés

- Quels sont les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames capturées ? Il est probable que les paquets ICMP soient précédés d'un jeu de questions/réponses DNS.
- Relever l'adresse IP renvoyée avec la réponse DNS associée à l'adresse IP de google

Message UDP

- Quelle est l'adresse IP destination du premier paquet contenant le message UDP
- Quelles sont les valeurs des champs Protocol Type et Time to Live ?
- Comparer l'adresse IP destination relevée avec celle de la réponse DNS.
- Noter les valeurs caractéristiques de l'en-tête IP en vue d'une utilisation ultérieure.
- Combien d'octets de données sont présents dans ce message de requête ?

Message ICMP «Time Exceeded»

---

[1] Le champ identifiant est codé sur 16 bits et définit l'identifiant de l'émetteur. (Numéro du processus assigné à l'application lors de l'exécution). Cela permet de le rendre unique inter application.

[2] Le champ Séquence est codé sur 16 bits et permet au récepteur, d'identifier s'il manque un paquet. Ainsi, si le récepteur reçoit la séquence 1 puis 3, il peut en déterminer une perte d'un paquet.

- Quelles sont les @IP source et destination du paquet de la première réponse ICMP Time Exceeded ?
- Quel est le type de message ICMP ? (Les champs Type, message ICMP Echo Request.)
- Comparer les valeurs caractéristiques de cet en-tête avec celles notées ci-avant.
- Est-ce que le message ICMP contient de nouveaux octets de données ?

Evolution du champ TTL

- Combien de messages UDP sont émis avec la même valeur de champ TTL dans l'entête de paquet IP ?
- Quelles sont les adresses IP source des paquets ICMP Time Exceeded ?
- Comparer ces adresses avec celles données lors de l'exécution de la commande traceroute.
- Quel est le type du message ICMP reçu lorsque l'hôte destinataire est atteint ?
- Comment calculer les temps affichés par la commande traceroute à partir des valeurs données dans la colonne Time de la fenêtre des trames capturées ?

B. Notation CIDR - plages d'adresses, adresse de broadcast

Indiquez en regard de chaque réseau la plage d'adresses assignables qu'il définit.

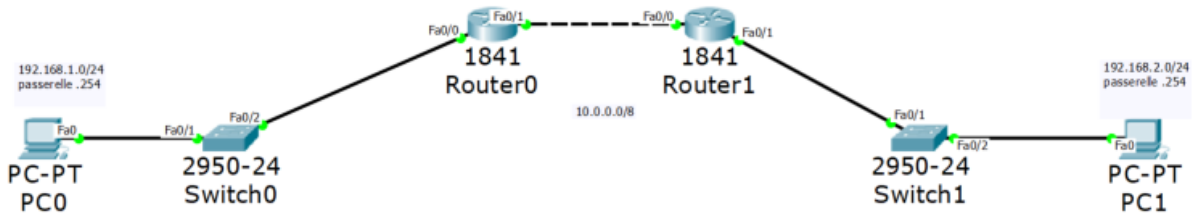
Adresse IP	Adresse réseau	définit la plage d'adresses :		@ broadcast
Ex: 10.0.1.55/8	*10.0.0.0*	**de:** *10.0.0.1*	***à:*** *10.255.255.254*	*10.255.255.255*
a) 192.168.1.100 /26				
b) 173.67.0.12 /16				
c) 34.70.122.64 /19				

C. Routage

Cette partie du TP nécessite PacketTracer. Vous allez utiliser la version disponible sur votre poste de travail il faudra vous identifier avec vos identifiants cisco net academy que vous avez créé en S2.

1) Routage statique

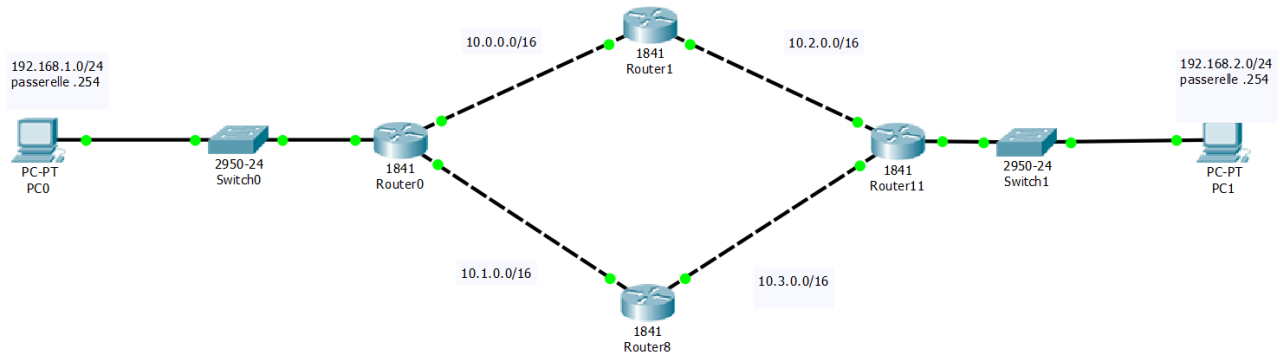
Réalisez le schéma suivant sous packet Tracer *ExoC_1_RoutageStatique.pkt*



- Combien y a-t-il de réseaux locaux dans ce schéma ?
- Il vous faudra configurer les postes et les routeurs en routage statique pour permettre la communication entre les deux PCs.
- Vérifiez en mode simulation que la communication est correcte entre les deux réseaux.

2) Routage dynamique

Renommez le fichier précédent en *ExoC_2_RIP.pkt* et modifiez le selon le modèle ci-dessous :



Vous allez configurer un routage dynamique sur ce réseau. Pour cela il faut remplir la table RIP des routeurs avec chacun des réseaux présents à ses interfaces. Le protocole RIP se charge de diffuser les réseaux de proche en proche.

- Testez la communication entre les deux PC. Utilisez le mode simulation pour savoir par quel chemin circulent les messages.

- Mettez hors tension le routeur1 et testez à nouveau la communication. Que se passe-t-il ?