RT1 – Module M1101
Sujets de TP 5 à 10

PREAMBULE

1. Adresses réseau des salles

Vous savez que l'adresse réseau de la salle 405 est 10.4.105.0/24, celle de la salle 410 est 10.4.110.0/24, et celle de la salle 102 est 10.1.102.0/24. Le texte de l'ensemble des TP 5 à 10 est écrit pour la salle 405. A votre charge d'adapter les adresses mentionnées dans le texte à la salle dans laquelle se déroule votre séance de TP, ainsi que les autres noms (SW405 ou SW102 etc.).

2. Création des machines virtuelles (VM)

Dans chaque TP, vous devrez créer à l'aide de la commande `createvm` une ou plusieurs VM par machine physique, selon l'exemple affiché à l'appel de cette commande sans arguments d'entrée. Si rien n'est précisé dans le texte du TP, vous choisirez le disque virtuel nommé :

- `debian-9_2017.Debian_64.MEM1024.VTX.NP.SATA.vdi`

3. Câblage initial

En arrivant sur votre paillasse, aucun câble ne doit être connecté en dehors de eth1 des 2 PC sur SW405 sur le bandeau de pré-câblage. Si ce n'est pas le cas, rétablissez cette configuration initiale.

TP 5 - Module M1101

Les bases des couches OSI, le lien entre couches, matériel et Wireshark

Ce qu'on veut faire dans ce TP :Comprendre le fonctionnement de base des couches TCP/IP.

Pourquoi :Pour dans le prochain TP comprendre comment configurer un réseau et résoudre les problèmes.

Comment :En utilisant le logiciel Wireshark permettant de capturer les paquets sur la carte réseau.

Table des matières

1 Introduction

Wireshark est un logiciel d'analyse de trafic. Il permet de contrôler la carte réseau de la machine sur laquelle il tourne, récupère les paquets (trames) vues par la carte réseau et permet une analyse aisée des paquets.
Le but de ce TP est d'abord de comprendre précisément la structure avec laquelle Wireshark présente les informations de trafic, en comprenant le lien avec les couches du modèle OSI.

Wireshark est un logiciel gratuit et existe sous Linux et Windows. N'hésitez pas à l'installer sur vos machines personnelles et à regarder ce qui se passe sur votre réseau en dehors des cours.

Wireshark est installé sur les machines virtuelles Linux que vous allez créer.
Connectez-vous sur votre compte (chaque étudiant du binôme sur un PC différent, sur son compte perso). Dans un terminal, tapez `createvm` et copiez-collez la ligne avec le fichier VDI indiqué dans le préambule (page 1).
Logins et mdp habituels : rt/rt
Passer en root en tapant: `su`, password: *rt*. Tapez `wireshark &` pour lancer le logiciel.
Comme pour les autres TP, toutes les étapes sont à faire dans l'ordre.

2 Analyse des 3 sous-fenêtres de Wireshark

2.1 Préambule

- Dans l'onglet Capture, cliquez sur Options. Sélectionnez l'interface sur laquelle la capture doit être réalisée (eth1 sur la VM), décochez « *promiscious mode* » en bas et les différentes « *name resolutions* » dans l'onglet Options. Cliquez sur *Start*. La capture est lancée.
- Connectez vous sur http://kheops.unice.fr. Une fois cette page chargée, arrêtez la capture (Capture → Stop) .

2.2 Analyse de Wireshark et du fonctionnement général des réseaux d'un point de vue concret (physique/matériel)

Nous allons à présent procéder à une analyse structurée, « du plus général au plus détaillé », de la façon dont Wireshark représente le trafic. En faisant cela, on va découvrir ou se remémorer la structure de fonctionnement d'un réseau informatique.

Illustration 1: Structure graphique de Wireshark

Il est indispensable de lire le rappel sur les couches OSI, transparent 9 du TP 2.

Vous voyez que la fenêtre principale de Wireshark, où apparaît le résultat de la capture, est divisée en 3 sous-fenêtres.
On va successivement déterminer et comprendre ce que représente une ligne de chaque sous-fenêtre. Attention : la réponse donnée doit pouvoir s'appliquer à toutes les lignes de la sous-fenêtre, il ne s'agit pas seulement de lire ce que vous voyez écrit sur une ligne.

2.2.1 Analyse de la 1ère sous-fenêtre

1. Cliquez sur une ligne de la 1ère sous-fenêtre. Regardez le contenu de la 3ème sous-fenêtre. Refaîtes la même chose en cliquant sur une autre ligne de la 1ère sous-fenêtre. Ce contenu a t-il changé entre les 2 clics ?

2. a. Quelles sont les valeurs possibles (0, f, a, 5,...) que peut prendre un symbole de la partie gauche de la 3ème sous-fenêtre ? Quel est le nombre de ces valeurs possibles ?
   b. Combien de bits faut-il pour qu'un symbole (qui est un groupe de bits) puisse prendre ce nombre de valeurs, et quel est son nom courant ?

A retenir : Chaque ligne de la 1ère sous-fenêtre représente un paquet capturé sur la carte réseau (aussi appelé trame, voir Annexe 1). La 3ème sous-fenêtre représente la série de bits constituant ce paquet.

3. Pourquoi doit-on lancer Wireshark en mode administrateur (c'est-à-dire depuis le compte root) ?

2.2.2 Analyse de la 2ème sous-fenêtre

Lisez les annexes 2 et 3.

4. Structure générale de la 2ème sous-fenêtre: au vu des protocoles mentionnés, que représente chaque ligne de cette sous fenêtre ?
   NB : Ne déroulez pas les lignes de la 2ème sous-fenêtre, qui exposent des détails que nous analyserons dans les parties suivantes.

5. Cliquez sur les différentes lignes de la 2ème sous-fenêtre. Comment s'appelent les parties surlignées pour chaque ligne de la 2ème sous-fenêtre dans la 3ème sous-fenêtre.

6. Rappelez ce qu'est l'encapsulation et comment ce phénomène se manifeste dans les 2ème et 3èmes sous-fenêtres.

7. A quoi correspond le protocole indiqué dans la 5ème colonne (colonne « Protocole ») de la 1ère sous-fenêtre ?

3 Analyse des fondamentaux de chaque couche OSI et de sa fonction

On part de la capture des paquets que vous avez faite lorsque vous vous êtes connectés au serveur web kheops.unice.fr .

3.1 La couche application

Observez le contenu de la requête *HTTP get* en sélectionnant le bon paquet dans la 1ère sous-fenêtre et en déroulant la bonne ligne dans la 2ème sous-fenêtre :

1. Quel but a ce paquet ?

2. Que vous indiquent les informations que vous voyez à l'intérieur quant au programme qui a généré ce paquet ?

Observez les 2 paquets DNS :

3. A quoi servent ces paquets ?

4. DNS est un protocole appartenant à quelle couche OSI ?

5. Quel protocole de couche transport est utilisé avec HTTP? Pourquoi ?

6. Quel protocole de couche transport est utilisé avec DNS ? Pourquoi ?

3.2 La couche transport

Cliquer sur le paquet de requête *HTTP get* de la 1ère sous-fenêtre, et dérouler la ligne correspondant à l'entête TCP dans la 2ème sous-fenêtre. Faites de même avec le *HTTP ok*.

1. Observez la paire de ports utilisés pour les 2 paquets. Que remarquez-vous ?

2. Quel est le but général de la couche transport (voir Figure 5) ?

3. Décrire comment ce but est atteint en décrivant l'écriture du paquet dans la RAM en complétant la phrase suivante :
   « ….....est identifiée grâce.....inscrit dans l'entête de couche transport du paquet .»

4. Résumez ces étapes sous la forme du schéma de la figure 2, en remplaçant avec précision *test*, *action* et *paquet*.

5. Les ports de transport (ports TCP ou UDP) sont-ils censés changer au cours du trajet du paquet dans le réseau, entre la source initiale et la destination finale ?

3.3 La couche réseau

Analysez les adresses IP des 2 paquets *HTTP get* et *HTTP ok* :

1. Que remarquez-vous ?

2. Que fait d'abord le système d'exploitation quand il reçoit un paquet de la carte réseau ? Répondez sous la forme du schéma de la figure 2, en remplaçant toujours avec précision *test*, *action* et *paquet*.

3. Les adresses IP sont-elles censées changer au cours du trajet du paquet dans le réseau, entre la source initiale et la destination finale ?

4. Quelle différence observez-vous dans les valeurs du champ TTL des 2 paquets *HTTP get* et *HTTP ok* ? Comment l'expliquez-vous (que veut dire « TTL », et à quoi sert-il) ?

3.4 La couche liaison de données

Analysez les adresses MAC des 2 paquets *HTTP get* et *HTTP ok* :

5. Que remarquez-vous ?

6. Que fait la carte réseau d'une machine quand elle reçoit une trame ? Répondez sous la forme du schéma de la figure 2, en remplaçant toujours avec précision *test*, *action* et *paquet*.

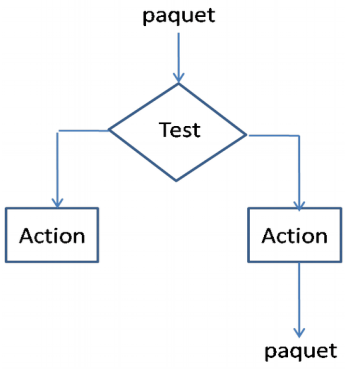


Illustration 2: Diagramme de flux

7. Les adresses MAC sont-elles censées changer au cours du trajet du paquet dans le réseau, entre la source initiale et la destination finale ?

4 Approfondissement de la couche transport

1. A partir des réponses apportées dans la section 3.3, déduisez pourquoi ce qu'on appelle un « serveur » doit avoir des ports fixes (fixé par la norme).

2. Le port côté « client » est-il fixe ?

3. A quoi sert alors la triple poignée de main TCP ?

4. Ouvrez la page web à l'url http://kheops.unice.fr. Tapez dans un terminal : `netstat -tpn`
   A quoi correspond une ligne qui vous est affichée ? La décrire en détail, en faisant le lien entre le problème de la couche transport et l'ouverture de page web que vous venez de faire.

5 Approfondissement de la couche réseau : le protocole IP

5.1 Adresses IP et MAC : différences

Vous pourrez regrouper vos réponses aux manipulations suivantes sous la forme d'un tableau (voir figure 3).

- Lancer une capture dans Wireshark. Depuis un terminal, faire un ping vers l'adresse .251 de la salle : tapez dans un terminal `ping 10.4.105.251`. Notez dans le tableau suivant les adresses IP et MAC source et destination des paquets *ICMP echo request* et *ICMP reply*. N'oubliez pas d'arrêter la capture.
- Lancer une capture dans Wireshark. Depuis un terminal, faire un ping vers le serveur web : `ping kheops.unice.fr` . Notez les adresses IP et MAC source et destination des paquets *ICMP echo request* et *ICMP reply*. N'oubliez pas d'arrêter la capture.
- Lancer une capture dans Wireshark. Depuis un terminal, faire un ping vers la passerelle du réseau local (rappel : 10.4.105.254). Notez les adresses IP et MAC source et destination des paquets *ICMP echo request* et *ICMP reply*. N'oubliez pas d'arrêter la capture.

	ICMP echo request Adr IP src	ICMP echo request Adr IP dst	ICMP echo request Adr MAC src	ICMP echo request Adr MAC dst	ICMP reply Adr IP src	ICMP reply Adr IP dst	ICMP reply Adr MAC src	ICMP reply Adr MAC dst
Manip 1								
Manip 2								
Manip 3								

Illustration 3: Adresses utilisées dans les 3 pings

1. Quelle est la différence au niveau des adresses MAC entre la manipulation 1 et les manipulations 2 et 3 ?

2. Quel est le lien entre les adresses MAC dans les manipulations 2 et 3 ?

3. Qu'en déduisez-vous sur l'adresse MAC du serveur web *kheops.unice.fr* et sur les adresses MAC utilisées à l'intérieur d'un réseau IP donné (comme celui de la salle 405 en 10.4.105.0/24) ?

4. Rappelez dans le diagramme de flux ci-dessous (figure 4) les étapes permettant à une machine de déterminer l'adresse MAC destination utilisée en fonction de l'adresse IP destination. Remplacez avec précision *test*, *action* et *@IP* :

Indice : la notion de masque doit intervenir dans le test.

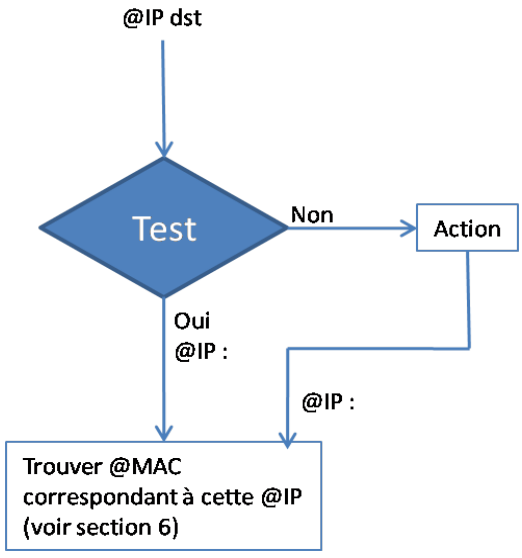


Illustration 4: Diagramme de flux

5. Est-ce que l'adresse MAC de la carte réseau d'une machine peut changer ? Est-ce que l'adresse IP d'une interface réseau d'une machine peut changer ?

5.2 Traceroute

1. Utilisez la commande `man traceroute` dans la console qui affiche le manuel de la commande. A quoi sert traceroute, et comment s'utilise t-il ? Que doit exactement renvoyer traceroute ? Lancez

un traceroute vers kheops.unice.fr

2. Quelle est l'adresse IP de la machine qui a été utilisée ?

3. Quel est le nom et l'adresse IP du serveur ciblé par traceroute ?

4. Quel protocole est utilisé par la machine cliente dans le cadre de traceroute ? Quel est le protocole utilisé pour la réponse à cette machine ?

5. Analyser le champ TTL des paquets envoyés par votre machine vers kheops.unice.fr. Comment varie leur valeur et pourquoi ?

6. Trouvez la série de messages ICMP indiquant un TTL trop grand (TTL exceeded) envoyés par le routeur le plus proche. Quelles sont les valeurs du champ d'identification et du champ TTL ?

7. Faire la liste de tous les routeurs traversés.

8. Décrivez précisément le fonctionnement de traceroute.

Annexe 1 : Dénomination des paquets

« paquet » est le terme générique pour désigner un ensemble de bits issu de n'importe quelle couche OSI, c'est-à-dire des bits en sortie de tout bloc de traitement correspondant à une couche. L'ensemble des bits issu d'une couche regroupe donc les bits rajoutés par cette couche, ainsi que ceux rajoutés aux couches précédentes (« supérieures » dans le modèle OSI). A partir des bits générés par l'application qui veut les envoyer sur le réseau, d'autres bits sont ajoutés par chaque traitement, c'est-à-dire à chaque passage à travers une couche, pour que ce traitement puisse fonctionner. Ce traitement est un protocole qui résout le sous-problème que la couche définit.

Selon la couche, un paquet qui en est issu porte un nom différent. Voir Figure ci-contre.

Couche	Sous-problème	Implémenté dans	Exemple de protocole	Nom du paquet
Application	Communication machine/utilisateur	Logiciel	http, ftp, ssh,...	Message
Transport	Faire communiquer 2 processus entre eux indépendamment de ce qui se passe sur le réseau	OS	TCP, UDP	Segment
Réseau	Trouver le chemin entre les 2 machines (la suite d'équipements intermédiaires à traverser)	OS	IP	Datagramme
Liaison de données	Gérer l'accès au medium (câble, sans-fil, fibre, ...), comme accès multiple, correction d'erreur, etc.	Carte réseau	Ethernet, WiFi,...	Trame
Physique	Assurer la traduction bit/ondes électromagnétiques	Carte réseau	Ethernet, WiFi,...	Trame

Illustration 5: Les couches OSI et les déclinaisons du terme "paquet"

Annexe 2 : Couches et protocoles

Reprenez les transparents 8 et 9 du TP2, et souvenez-vous des explications. Rappelez-vous qu'une couche est un sous-problème, et il peut exister plusieurs façons de le résoudre. Un protocole est un traitement. On dit qu'un protocole appartient à une couche s'il résout le sous-problème de cette couche. Plusieurs protocoles peuvent appartenir à la même couche s'il résolvent le même sous-problème de manières différentes (exemple avec la couche transport : TCP et UDP).

Annexe 3 : L'encapsulation

Si le protocole A est implémenté après le protocole B, c'est-à-dire que le traitement A est effectué après le traitement B, alors on dit que le protocole A « encapsule » le protocole B.

Pour pouvoir fonctionner, un protocole a besoin de rajouter des bits au paquet : on dit que chaque protocole rajoute une entête. Les entêtes sont rajoutées successivement en préfixe du paquet sortant de la couche précedente. Voir figure ci-dessous.

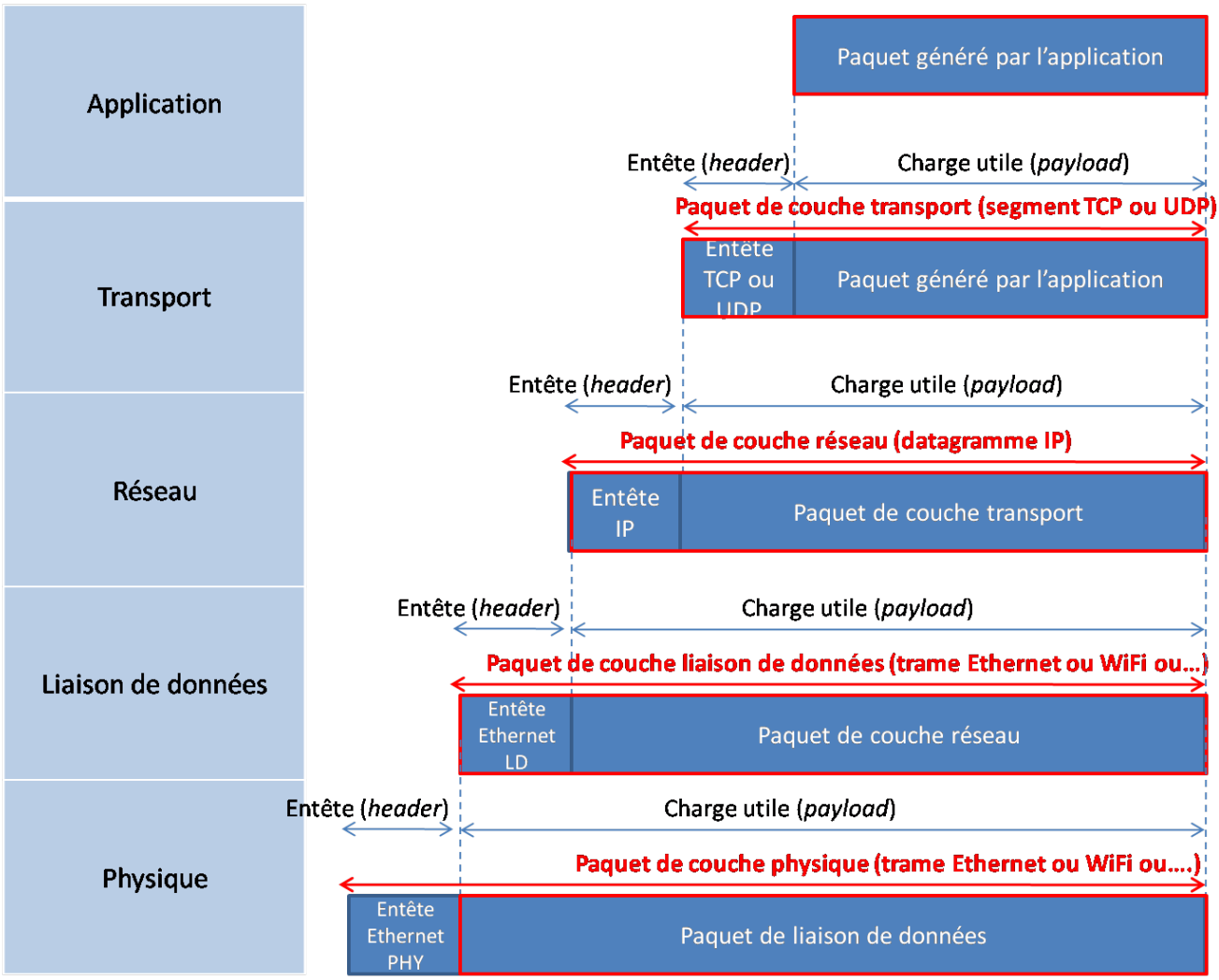
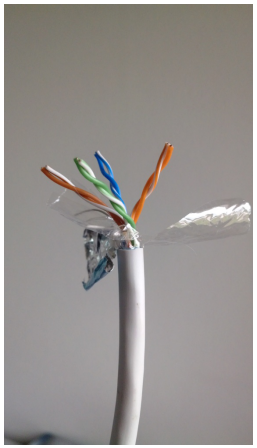


Illustration 6: L'encapsulation et les entêtes protocolaires

Introduction au câblage

- Un câble Ethernet est constitué de 8 fils, regroupés et torsadés par paire.
- Il y a 4 couleurs : orange, vert, bleu et marron.
- Chaque paire est constituée du fil de couleur C et du fil de couleur blanc et C.

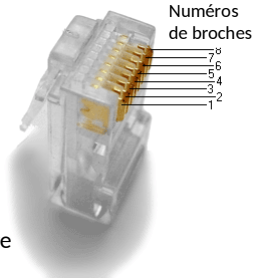


La structure d'un câble

- 2 signaux sont nécessaires à une communication sur un réseau Ethernet : un signal d'émission et un signal de réception.
- La grandeur physique transportant le signal est une tension.
- Or une tension est une différence de potentiels.
- Une tension se mesure donc entre 2 points : entre 2 fils.
- Il faut donc 2 fils pour porter un signal, donc 4 fils en tout sont nécessaires pour communiquer.
- Un signal est donc porté par 2 fils.

La structure d'un câble

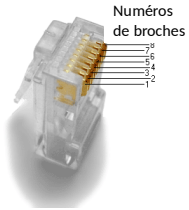
- Sur les 8 fils, seuls 4 sont donc utilisés dans un réseau 10/100 Mbps. (On va voir ce à quoi peuvent servir les autres.)
- Aux extrémités d'un câble doivent être fixés des connecteurs, par exemple des **connecteurs RJ45**.
- Un connecteur RJ45 a 8 broches, pour entrer en contact avec les 8 fils.
- Les broches d'un RJ45 sont numérotées.
- La correspondance entre couleur de fil et numéro de broche est appelée « **code couleur** ».
- La norme classique en Europe, est celle avec laquelle le câblage du bâtiment RT est réalisée, est la norme **EIT-TIA 568B**:



N° de broche	1	2	3	4	5	6	7	8
Couleur de fil	Blanc-Orange	Orange	Blanc-Vert	Bleu	Blanc-Bleu	Vert	Blanc-Marron	Marron

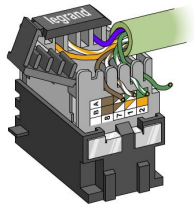
Les connecteurs RJ45

Un connecteur RJ45 mâle :



Un connecteur RJ45 femelle :

Face



Arrière

Les catégories MDI et MDIX

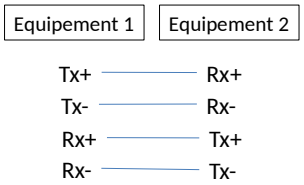
- On distingue 4 grand types d'équipements :

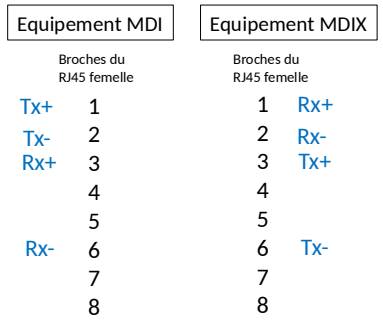
Type	PC	Hub	Switch	Routeur
Catégorie	MDI	MDIX	MDIX	MDI

- On dit qu'un équipement est de catégorie MDI ou MDIX selon la façon dont l'électronique de ses ports Ethernet affecte le signal d'émission et le signal de réception aux numéros de broches :
  - émission affectée sur broches 1 et 2 et réception sur broches 3 et 6 : MDI
  - émission affectée sur broches 3 et 6 et réception sur broches 1 et 2 : MDIX

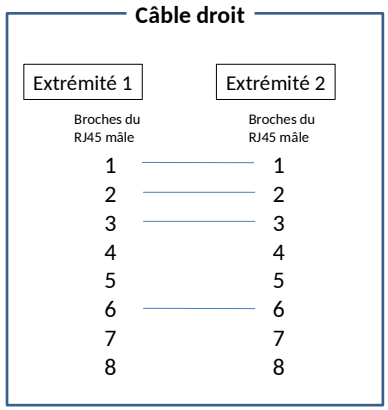
Câble droit ou croisé ?

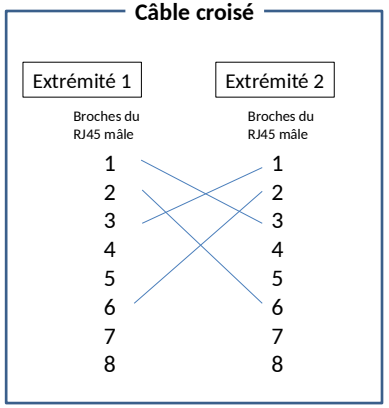
- Pour connecter 2 équipements entre eux à l'aide d'un câble, il faut nécessairement que les broches affectées au signal d'émission d'un côté soit reliées aux broches affectées au signal de réception de l'autre côté :





Câble droit ou croisé ?





Câble droit ou croisé ?

- Donc quand on doit décider quel type de câble utiliser, il faut **d'abord déterminer la catégorie** des 2 équipements qu'on veut relier.

- Ensuite, vous déduisez que :
  - entre 2 éqts de catégorie MDI, on met du câble _____
  - entre 2 éqts de catégorie MDIX, on met du câble _____
  - entre 1 éqt MDI et 1 éqt MDIX, on met du câble _____

- *Attention* : « droit » ou « croisé » s'applique à un câble, pas à un éqt

TP 6 – Module M1101

Câblage et configuration d'interface sous Linux

Ce qu'on veut faire dans ce TP : Configurer les interfaces de différente manières, pour clients et serveurs, et identifier la source des problèmes possibles.

Pourquoi :Pour être capable de configurer le réseau comme requis, et résoudre rapidement les problèmes en identifiant leur cause.

Comment :En comprenant l'impact de chaque commande de configuration, et en provoquant volontairement des problèmes, en connaissant donc la cause, et en voyant le message d'erreur conséquence.

Table des matières

1 Introduction au câblage

1.1 Introduction au tableau

Transparents 1 à 9 précédents

1.2 Le cas des cartes réseau des PC

A retenir: La majorité des carte réseau de machines d'extrêmités sont *Auto MDI/MDIX*, ce qui signifie qu'elles sont capables de changer les broches de transmission et réception pour s'adapter aux fonctions des broches de l'autre carte connectée par un câble. Les équipements intermédiaires switchs et routeurs ont eux en revanche moins fréquemment cette capacité.

2 Configuration d'interfaces sous Linux

Créez une VM comme indiqué en introduction du TP5..

2.1 Les outils et processus système contrôlant les interfaces

1. Tapez `ifconfig` dans le terminal. Quelles sont les informations importantes sur la

configuration des interfaces réseau (c'est-à-dire les cartes) que vous y voyez ?

2. Tapez `route -n` dans le terminal. A quoi correspond la table qui vous est affichée ? Quel peut être son fonctionnement ?

3. Tapez `more /etc/resolv.conf` dans le terminal. Que contient le fichier qui vous est affiché ?

Configurer un connexion réseau sur une machine Linux signifie donc :

- affecter des valeurs valides aux paramètres de l'interface réseau, visible par la commande `ifconfig`
- ajouter des entrées (des lignes) dans la table de routage du noyau pour pouvoir envoyer des paquets vers les réseaux désirés
- ajouter des serveurs de noms de domaine dans le fichier resolv.conf pour obtenir les adresses IP des url désirées

Pour configurer ces 3 éléments, il y a 2 possibilités :

- soit on désire que la configuration se fasse automatiquement, en tant qu'utilisateur, sans rien connaître des paramètres du réseau local auquel on va accéder
- soit on désire contrôler la configuration

Si on désire que la configuration se fasse automatiquement, alors on va indiquer au système d'utiliser un programme qui s'appelle `dhclient`, et qui va demander à un serveur les valeurs de tous les éléments nécessaires pour avoir une connexion au réseau local auquel est physiquement relié la machine. Si ce programme `dhclient` est lancé, alors il va demander à un serveur distant ce qui est contenu dans le fichier suivant :

4. Tapez `more /etc/dhcp/dhclient.conf` dans le terminal. Les lignes précédées d'un # sont commentées (donc non lues). Que contiennent les lignes non commentées (donc effectives) ?

Pour mettre en oeuvre les 2 possibilités mentionnées plus haut, il existe **4 outils différents**, selon nos besoins :

- Network Manager (NM) : NM est un programme rendant conviviale la configuration des interfaces réseau (filaires ou sans-fil) sous Linux. L'utilisateur gère ses connexions par de simple clics exactement comme sous Windows. NM est donc un programme servant d'intermédiaire entre l'utilisateur à qui il présente une gestion unifiée du réseau, et les 3 éléments mentionnés plus haut. **Attention** : NM ne doit pas s'utiliser quand on a des besoins spécifiques, ou sur un serveur.
- L'outil `ifup/ifdown` qui sert également d'intermédiaire entre l'utilisateur et les 3 éléments mentionnés plus haut, sauf que cette fois-ci il s'agit de commande à entrer dans un terminal, et qui vont lire un fichier de configuration ennonçant comment manipuler les 3 éléments.
- L'outil `ifconfig` pour fixer les paramètre de l'interface, utiliser avec l'outil `route` pour modifier les routes.
- L'outil `ip` pour à la fois fixer les paramètre de l'interface et modifier les routes.

Nous allons voir les 2 premiers dans les 2 parties qui suivent, car ce sont ceux que vous allez utiliser systématiquement en M1101 et M1102, et pus généralement quand vous gérez des serveurs.

2.2 Configuration d'interfaces avec Network Manager

Network Manager est automatiquement installé lors de l'install d'un système de type Debian pour Desktop (donc pas pour serveur). Votre VM ne le contient cependant pas pour que vous la gériez comme un serveur. Il faut donc l'installer. En mode root :

```
apt-get install network-manager
apt-get install network-manager-gnome
```

Ouvrez ensuite le fichier interfaces :

```
nano /etc/newtork/interfaces
```

Commentez chaque ligne relative à eth0 et eth1, en rajoutant un # devant. Sauvegardez avec `Ctrl+O [entree]` puis sortie avec `Ctrl+X`.

Cette opération consiste à soustraire le contrôle des interfaces au processus networking et de le donner à Network Manager (NM).

Re-démarrez la VM et effectuer les étapes suivantes une fois que vous êtes re-loggée.

Allez sur l'icône de la prise avec un câble, en haut à droite. *Clic droit → Connection information*. Repérez l'interface connectée : c'est eth1.

1. *Clic gauche → Disconnect* puis *Clic gauche → Wired connection 1*. Que constatez-vous ?
2. *Clic droit → Connection information*. Que voyez-vous, et pour quelle interface ? Fermez la petite fenêtre qui s'est ouverte.
3. *Clic droit → Edit connections*. Sélectionnez *Wired connection 1* et *Edit*, onglet *IPv4 Setting*. Quelle est le mode de configuration de la connexion réseau par l'interface eth1 pour l'instant ?
4. Quelle est le mode de configuration de la connexion réseau par l'interface eth0 pour l'instant ?
5. *Clic gauche → Disconnect* puis *Clic gauche → Wired connection 1* sur eth0. Que constatez-vous ? Pourquoi ?

Nous allons maintenant laisser configurée l'interface eth1 en DHCP, et configurer eth0 manuellement.

6. Editez la connexion eth0, puis onglet IPv4 settings puis Method: Manual, et faites les ajoûts suivants :
   Address : 192.168.0.5 ; Netmask : 255.255.255.0 ; Gateway : 192.168.0.254 ; DNS : 134.59.136.1 et clic sur Apply
7. Fermez la fenêtre NM, puis clic gauche sur l'icône et *Wired connection 1* de eth0. Que se passe t-il ? Comment expliquez-vous cela dans la mesure où vous n'avez branché aucun câble entre eth0 de votre machine physique et SW405 ?
8. Si on branchait un câble droit entre eth0 et SW405, avec la configuration manuelle que vous avez entrée et connaissant l'architecture réseau de la salle, à quelle condition pourriez-vous accéder à une machine située sur le réseau local ?
9. Pourriez-vous accéder à une machine située en dehors du réseau local ?

Nous allons maintenant vouloir une VM sans NM. Vous pourriez faire l'inverse des premières opérations, mais il est plus simple d'éteindre cette VM (vous pouvez la détruire) et en re-créer une autre. Effectuez cette dernière option.

2.3 Configuration d'interfaces avec l'outil `ifup` / `ifdown`

Les commandes `ifup` et `ifdown` peuvent être utilisées pour activer et configurer (ou, respectivement, désactiver) des interfaces réseau en se basant sur les définitions dans le fichier */etc/network/interfaces*.

Nous allons ici écrire un fichier *interfaces* indiquant que ni eth0 ni eth1 ne doivent s'activer automatiquement au démarrage, que eth1 lors de son activation doit obtenir automatiquement sa configuration par DHCP (donc demander à un serveur les valeurs tous les éléments nécessaires pour que la connexion fonctionne, éléments mentionnés page 2), et que eth0 est configurée manuellement avec les valeurs des paramètres entrées dans le fichier *interfaces*.

1. Editez le fichier *interfaces* : dans un terminal, tapez :
   `su`
   `nano /etc/network/interfaces &`
   et recopiez le fichier de la figure 1. “xx” doit être remplacé par le numéro de votre machine dans la salle. Attention aux erreurs de typo !!!
   Sauvegardez avec `Ctrl+O [entree]` puis sortie avec `Ctrl+X`.

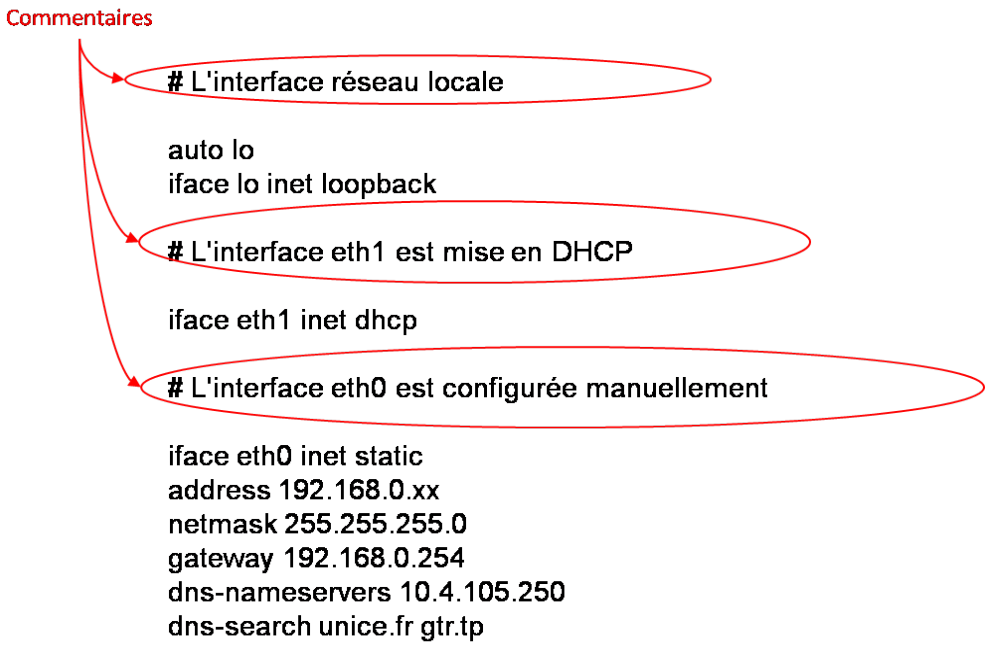


Illustration 1: Fichier /etc/network/interface à faire

2. Activez eth1 par un `ifup eth1` depuis un terminal en mode root.
3. Regardez les 3 éléments importants (page 2) comme indiqué dans les questions 1 à 3 de la section 2.1, et notez-les.
4. Faire un ping vers la machine de votre binôme. Celui-ci fonctionne t-il ? Pourquoi ?
5. Faire un ping vers kheops.unice.fr. Celui-ci fonctionne t-il ? Pourquoi ?
6. Désactivez eth1 par un `ifdown eth1` puis activez eth0.
7. Regardez les 3 éléments importants (page 2) comme indiqué dans les questions 1 à 3 de la section 2.1, et notez-les.
8. Faire un ping vers la machine de votre binôme. Celui-ci fonctionne t-il ? Pourquoi ?
9. Faire un ping vers kheops.unice.fr. Celui-ci fonctionne t-il ? Pourquoi ?

Désactiver les 2 interfaces avec `ifdown`.

3 Erreurs types : relier le message d'erreur émis par le système au problème de configuration

`Attention :` Cette partie est fondamentale pour vous. Il s'agit d'apprendre à identifier la cause du problème si vous avez une connexion réseau qui ne fonctionne pas (par exemple, le ping est un échec).

Désactiver eth0 et activez eth1 avec `ifup`.

1. Faites un ping entre les 2 VM de la paillasse. Vérifiez que le ping est un succès.
2. Débranchez le destinataire du ping. Quel message d'erreur apparaît ? Comment le traduisez-vous en français ?
3. Rebranchez le destinataire, et vérifiez que le ping fonctionne. Désactivez eth1 dans la VM. Que se passe t-il lors du ping ? Pourquoi ?
4. Ré-activer eth1 comme précédemment, notez l'adresse IP et vérifiez qu'un ping vers kheops.unice.fr fonctionne.
5. Recopiez le fichier *interfaces* donné en figure 2 dans /etc/network/interfaces (vous remplacerez le dernier nombre xx par celui noté dans l'adresse IP de la question précédente).

```
# L'interface locale
auto lo
iface lo inet loopback

# L'interface eth1
iface eth0 inet dhcp

# L'interface eth0

iface eth1 inet static
address 10.4.105.xx
netmask 255.255.255.0
dns-nameservers 10.4.110.250
dns-search unice.fr gtr.tp
```

Illustration 2: Fichier /etc/network/interface à faire

7. Faîtes ensuite `ifdown eth1` puis `ifup eth1`. Re-démarrez votre VM si vous obtenez une erreur sur la première étape.Vérifiez la configuration obtenue avec `ifconfig`.
8. Faîtes un ping vers kheops.unice.fr. Quel est le message d'erreur ? A quoi est dû le problème ?
9. Remédiez au problème dans en changeant le fichier interfaces de façon appropriée. Vérifiez que le ping fonctionne.
10. Vérifiez que le ping fonctionne également depuis la machine physique, puis débranchez l'émetteur. Que se passe t-il lors du ping depuis la VM ? Que se passe t-il lors du ping depuis la machine physique ? Pourquoi ?

TP 7– Module M1101

Gestion des adresses MAC dans un PC et dans un switch

Ce qu'on veut faire dans ce TP : Comprendre comment sont utilisées les adresses MAC dans 2 types d'équipements : les machines d'extrémité (ou routeurs), et les switchs.

Pourquoi : Pour comprendre les problèmes possibles dus à la couche 2 sur un réseau local, et plus tard des configurations plus évoluées, comme les VLAN (réseaux locaux virtuels).

Comment : D'abord en identifiant comment est faîte la correspondance entre adresses IP de prochain saut et adresses MAC, puis en étant administrateur d'un switch pour identifier comment il transfère les trames Ethernet le traversant.

Table des matières

Créez une VM comme indiqué en intro du TP5, en la nommant VM1.

1 La couche liaison de donnée et la résolution d'adresses MAC : le protocole ARP

Lancez une capture. Faîtes un ping entre votre machine et la passerelle.

1. Tapez `arp -a` dans le terminal. Une table apparaît. Elle s'appelle la « table ARP ». Quelle correspondance stocke t-elle ?

2. Faîtes un ping entre votre machine et l'adresse .251 de la salle. Regardez de nouveau la table ARP de votre machine. Que remarquez-vous. Quelle en est la raison ?

3. Lancez une capture Wireshark. Faîtes un ping entre votre machine et celle de votre binôme (dont vous récupérez l'@IP avec `ifconfig` , cf. TP6). Arrêtez la capture et observez-la pour répondre aux questions suivantes.

4. Quel est le protocole déclenché par la commande `ping` pour créer un paquet ?

5. Dans quel protocole ce protocole est-il directement encapsulé ?

6. Indiquez les adresses dans l'entête rajoutée par IP, et comment votre OS en a t-il la connaissance ?

7. De quoi devrait être constituée l'entête Ethernet ajoutée par la carte réseau au moment de l'encapsulation du paquet IP ? Votre machine dispose t-elle de ces éléments au moment où vous tapez la commande `ping` ?

8. S'il lui manque un élément, quel est le mécanisme mis en place pour qu'elle le trouve ? Détaillez ce mécanisme en observant la capture.

A quoi sert donc le protocole ARP ? A quel moment le premier paquet généré par la commande `ping` part-il effectivement de votre carte réseau ?

2 Un premier équipement d'interconnexion : le commutateur. Accès et fonctionnement.

2.1 Préambule

Mettez le switch Cisco Catalyst (2950 ou 3560) de votre paillasse sous tension.

1. Branchez les eth0 de vos machines sur le switch, et choisissant des ports du milieu et adjacents. Ce qui suit fait appel aux connaissances acquises dans le TP6. Sur vos 2 VM, désactivez eth1 et dans le fichier d'interfaces, configurez eth0 avec l'adresse 192.168.0.1 pour la VM de gauche, et 192.168.0.2 pour la VM de droite. Activez ensuite eth0 et vérifier la bonne configuration de cette interface. Indiquez les commandes entrées dans chaque VM.
2. Faites un ping dans chaque sens entre vos 2 machines pour vérifier que les 2 machines peuvent communiquer à travers le switch.

2.2 Accéder au switch

Se connecter à un équipement d'interconnexion permet de surveiller son fonctionnement, et d'activer ou désactiver certaines fonctionnalités, c'est-à-dire le configurer. Pour s'y connecter, on distingue 2 types de moyens : en passant par le réseau, ou en passant par une liaison série, c'est-à-dire par des ports série sur l'ordinateur et l'équipement, et non pas par des cartes réseau.

Attention : Tout ce qui suit est à faire depuis seulement un des 2 PC physiques (gauche ou droit).

2.2.1 Connexion par le port série

Une connexion série, ou "console", s'effectue par un câble série entre le port série du PC et le port

console de l'équipement (câbles souvent bleus et plats).

1. Connectez l'interface console du switch (reportée sur le bandeau de pré-câblage) au port série de la machine (reportée également sur le bandeau de pré-câblage).
2. Ouvrez un terminal sur la **machine hôte**, et lancer la commande :

   ```
   kermit
   ```

   Nous avons besoin de 2 lignes de commande au prompt de kermit :

   ```
   C-Kermit> set line /dev/ttyS0 #(pour choisir le port série)
   C-Kermit> set carrier-watch off  #(évite la détection de modem)
   C-Kermit> connect
   ```

   Appuyez plusieurs fois sur entrée pour voir la ligne d'invite du switch.
3. Visualisez la configuration courante du switch par :

   ```
   Switch> enable
   ```

   Les éventuels login/mot de passe demandés sont : `rt/rt (ou rt/cisco)`

   ```
   Switch# show running-config
   ```

2.2.2 Connexion par le réseau

Accéder à un équipement par le réseau veut dire établir une communication Ethernet, à travers un câble Ethernet et par 2 ports Ethernet, l'un de la carte réseau de votre PC, l'autre sur l'équipement. Cependant, comme vous le savez maintenant, établir une communication sur le réseau (donc permettre que 2 programmes de part et d'autre, constituant la couche application, rentrent en communication) nécessite d'avoir au préalable configuré une interface réseau de chaque côté, donc avoir une configuration IP valide pour le switch. C'est ce que nous allons faire :

1. Rentrez en mode "configuration du terminal" en tapant :

   ```
   Switch#config terminal
   ```

   Puis dans l'interface que nous allons configurer :

   ```
   Switch(config)#interface vlan 1
   ```
2. Attribuez une adresse IP et un masque de sous-réseau à cet interface. Remplacez [150+P] par 150+num de paillasse. Puis activez l'interface :

   ```
   Switch(config-if)# ip address 10.4.105.[150+P] 255.255.255.0
   Switch(config-if)#no shutdown
   Switch(config-if)#exit
   Switch(config)#enable password cisco
   ```

2.2.2.1 Connexion par Telnet

Le premier protocole de couche application qui va être utilisé pour se connecter au switch à travers le

réseau est Telnet.

3. On configure ensuite une connexion telnet (l'application sur le switch)

   ```
   Switch(config)# line vty 0 2
   Switch(config-if)# password cisco
   Switch(config)# login
   ```

   ou, si le switch affiche une erreur :

   ```
   Switch(config)# login authentication default
   ```

   puis

   ```
   Switch(config)# exit
   ```

4. Branchez un câble entre le switch de la paillasse et SW405, et le câble de eth1 des 2 PC dans le switch de la paillasse. Désactivez les eth0 et activez les eth1 de vos VM.

Attention : Ce qui suit est à faire depuis les 2 PC physiques (gauche et droit).

5. Vérifiez que vous pouvez vous connecter en telnet depuis votre VM :

   ```
   telnet 10.4.105.[150+P]
   ```

Vous devez constater après la question précédente que le terminal auquel vous avez accès par ce moyen est exactement le même que celui par connexion série.

2.2.2.2 Connexion par HTTP

Le deuxième protocole de couche application qui peut être utilisé pour accéder au switch à travers le réseau est HTTP.

Ouvrez un navigateur web, enlever le proxy du navigateur et dans la barre d'adresse tapez `http://10.4.105.[150+P]`

2.3 Explorer la configuration et comprendre le fonctionnement du switch

Nous allons maintenant examiner plus en détail le switch.

1. Dans la connexion telnet, tapez :

   ```
   Switch> enable
   Mot de passe : cisco
   ```

2. Visualisez ensuite la “table MAC” ou “table d'adressage”. Cette table gère le fonctionnement fondamental du switch : commuter les paquets vers leurs destinations respectives.

   ```
   Switch# show mac address-table
   ```

   Quelle correspondance la table MAC stocke t-elle ?

Dans les deux parties qui suivent, nous allons faire une série de manipulations pour exposer le fonctionnement interne d’un switch.

3. Dans la suite vous allez utiliser le mode “promiscuité” de votre carte réseau, dans Wireshark. Faîtes une recherche web rapide (« promiscuité réseau » et la première page wikipédia en français suffit) pour comprendre ce que signifie exactement ce mode. Faites au moins 2 phrases pour répondre, l'une décrivant ce que la carte réseau en mode non-*promiscuous* fait quand elle reçoit une trame du réseau, l'autre ce qu'elle fait de différent en mode *promiscuous*.
4. Établissez la configuration suivante, telle qu'indiquée Fig. 1. Pour cela :

- Réalisez la topologie indiquée, en reliant un 5ème port du switch de la paillasse à SW405.

- Créez une VM supplémentaire sur chaque PC, en la nommant VM2.

- Une fois démarrée, changez le fichier d’interface de VM2 pour que eth0 soit configurée avec une IP fixe à `10.4.105.[120+PC]` ou PC est le numéro de votre PC dans la salle. Indiquez l’adresse et le mask uniquement (ni passerelle ni DNS).

- Désactivez eth1 et activez eth0 sur les VM2.

- Vérifiez que vous pouvez pinger votre 4 VM de la paillasse, et les machines physiques, c’est-à-dire toutes les interfaces connectées au switch de votre paillasse.

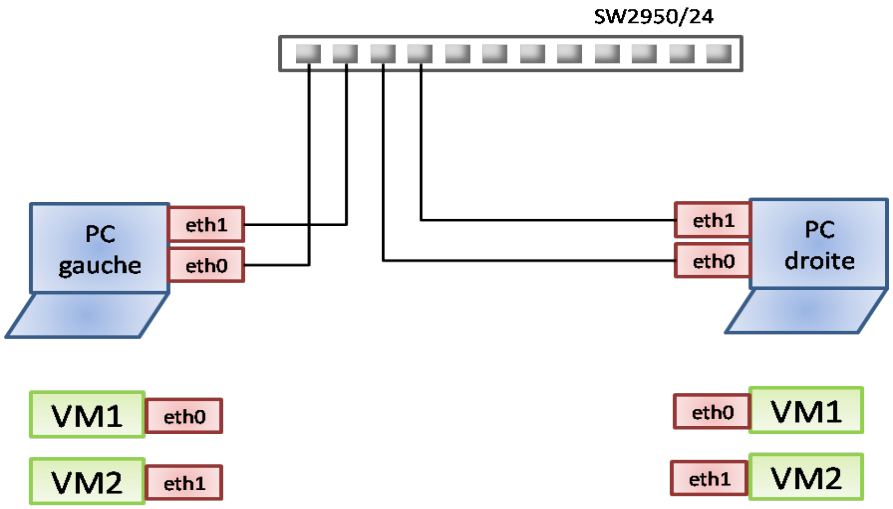


Illustration 1: Configuration pour l'étude du switch

5. Pour les 4 VM, autorisez le mode “promiscuous” dans la configuration Virtualbox des cartes réseaux virtuelles eth0 et eth1 (éteindre la VM si nécessaire).
6. Indiquez les adresses MAC et IP de chacune de vos interfaces virtuelles dans la Fig. 1.
7. Faites 2 pings, entre VM1 gauche et VM1 droite, et VM2 gauche et VM2 droite. Regardez la table MAC du switch et décrivez le rapport avec vos VM.
8. Refaîtes le ping depuis VM1 gauche vers VM1 droite, et lancez une capture Wireshark avec mode “promiscuous” activé sur les 4 VM. Les paquets que vous voyez sur chaque capture sont-ils émis par les 4 VM, ou seulement par certaines et alors lesquelles ?
9. Qu'en déduisez-vous sur ce que fait le switch ? Donnez la réponse complète avec les termes

précis :

"Le but d'un switch quand il reçoit une trame est de..... . Quand un switch reçoit une …...., il lit l'entête …..... dans laquelle est écrite …..... . Ensuite le switch accède à sa …..... pour lire dans la …..... et trouver l'entrée..... et savoir sur quel …..... transférer la …..... . "

2.3.2 Etablissement de la table MAC

10. Pendant ce qui suit regardez la table MAC du switch depuis PC gauche (rafraîchir l'affichage toutes les 2 secondes). Refaîtes le ping depuis VM1 gauche vers VM1 droite. Arrêtez-le et débranchez les 2 eth0 du switch. Que remarquez-vous alors sur les adresses MAC des VM1 dans la table MAC ?
11. Vérifiez que la table ARP de VM1 droite stocke bien l'adresse MAC de VM1 gauche. Rebranchez les 2 eth0 sur le switch. Lancez une capture Wireshark en mode "promiscuous" activé sur les VM2 gauche et droite, et simultanément regardez l'évolution de la table MAC. Faîtes un ping de VM1 gauche vers VM1 droite, puis arrêtez le ping et la capture.
12. Notez les paquets importants (avec leurs adresses MAC et IP src et dst) dans la Fig. 2. Que constatez-vous comme comportement en début de capture, non-observé jusque là ?
13. Que déduisez-vous comme mécanisme d'établissement de la table d'adressage d'un switch ? Vous pouvez prendre des notes sur vos observations sur la figure 4 pour vous aider. Donnez la réponse complète avec les termes précis :

    "Quand un switch reçoit une …..... dont l'adresse..... de …..... n'est pas présente dans …....., alors il …..... . Quand une …..... entre par un port du switch et que son adresse …..... est inconnue du switch (c'est-à-dire absente de la ….....) alors une ligne est ajoutée à la …..... pour enregistrer la correspondance entre..... et …..... . »

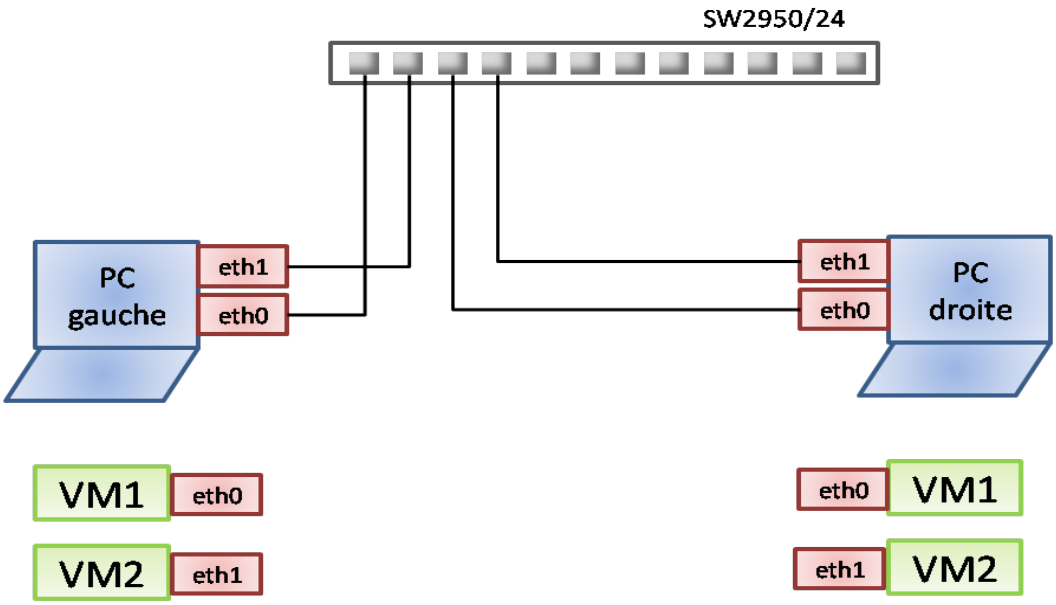


Illustration 2: Configuration pour l'étude du switch

TP 8– Module M1101

Etude et configuration d'un routeur

Ce qu'on veut faire dans ce TP : Mettre en place un réseau local additionnel de la paillasse, en plus du réseau local de la salle, et les interconnecter par un routeur à configurer.

Comment : En utilisant une adresse réseau et un switch différents de ceux de la salle, un routeur virtuel et le protocole de routage OSPF.

Pourquoi : Pour comprendre et savoir effectuer une configuration de base d'un routeur agissant comme passerelle d'un réseau local.

Table des matières

1 Mise en place d'un routeur virtuel dans GNS3

La pile d'équipements d'interconnexion au dessus de vous contient un ou deux routeurs, sauf en 102. Pour uniformiser les fonctionnements et parce-que le matériel n'est malheureusement pas fiable en salle 405, nous allons utiliser un routeur virtuel en M1101.

GNS3 est l'équivalent de VirtualBox pour les équipements réseau : on peut y créer des VM dont l'OS est un Cisco IOS (OS de routeur), qui voit un matériel virtuel exposé par GNS3 (châssis de routeur). GNS3 peut être relié à un réseau physique, ce que nous allons utiliser dans ces TP.

1.1 Présentation de GNS3

Pour prendre en main rapidement GNS3 pour ce dont on a besoin dans les TP :

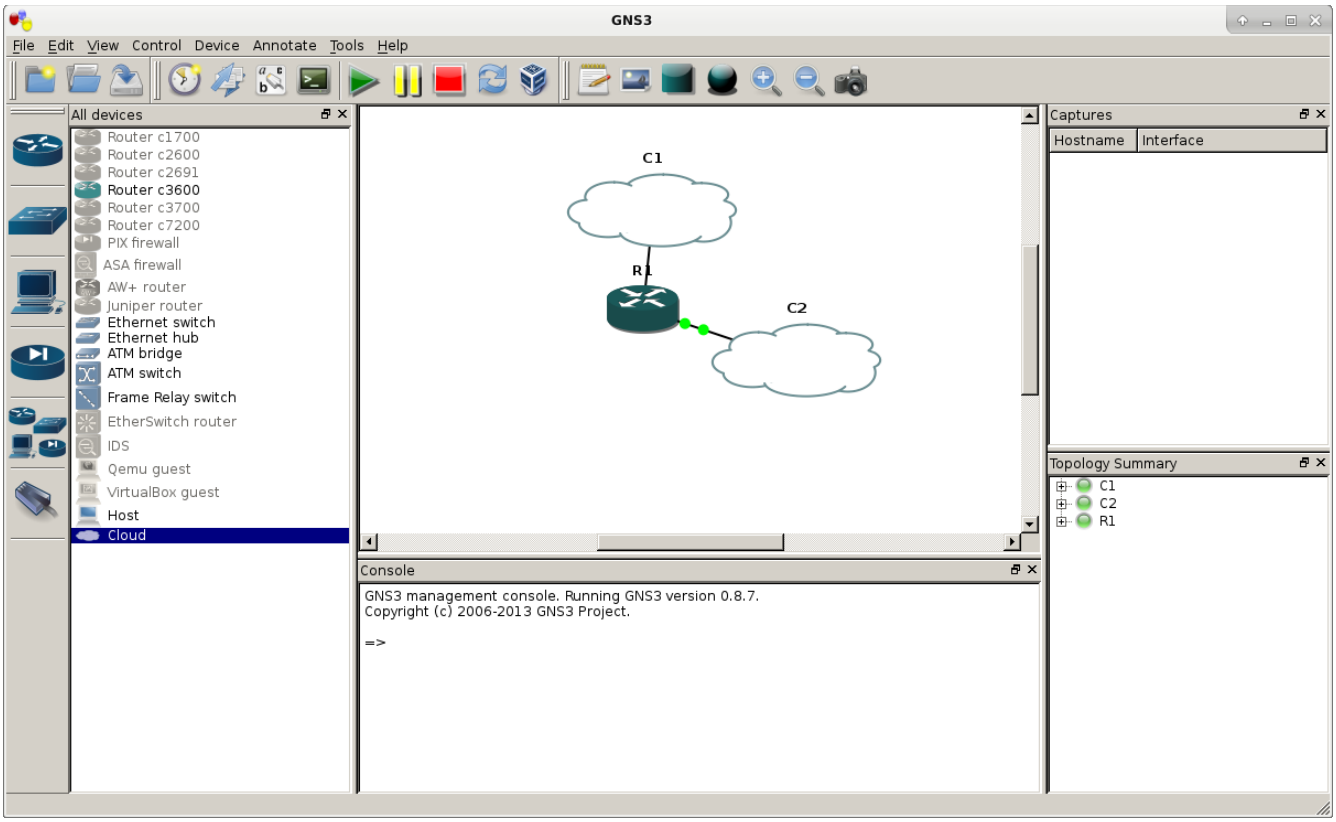


Illustration 1: Topologie incluant le routeur virtuel, et ses liens aux interfaces physiques (les nuages).

1. Ouvrez GNS3 : Application → Education → GNS3
2. Dans Edit → Preferences → Dynamips, cliquez sur « Test settings ». Puis « ok »/ »yes ».
3. Dans Edit → IOS images and hypervisors, cliquez sur la première icône avec « ... » pour rajouter une image IOS, en face de *Image file*. Allez chercher l'image de la série de routeur c3600 depuis le chemin /home/Vbox/IOS/.
   Ces images sont la propriété de Cisco, et elles nous sont fournies par un accord entre Cisco et l'IUT dans le cadre de la formation académique. Ces images stockent les systèmes d'exploitation des routeurs.
4. Lancez ensuite le calcul de *Idle PC* en cliquant sur « Auto calculation ». Cela a pour but le calcul de paramètres de virtualisation permettant qu'un routeur virtuel n'occupe pas 100 % du CPU de la machine physique.
5. Une fois le calcul achevé, fermez la fenêtre, « Save » puis « Close ».

1.2 Topologie désirée et équivalence physique-virtuelle

Le but du TP est de constituer un réseau local spécifique par paillasse, relié au réseau de la salle par un routeur situé sur la paillasse. Ce réseau aura un adressage différent du réseau de la salle : 192.168.N.0/24, avec N= [10+num de paillasse] en 405, N=[20+num de paillasse] en 102.

La topologie obtenue en utilisant le routeur physique serait celle de la Fig. 3 : Fa0/0 du routeur relié au

réseau de la salle, Fa1/0 du routeur relié au réseau de la paillasse. Notez ces 2 interfaces du routeur sur la Fig. 2. Cependant comme expliqué en introduction, nous allons utiliser un routeur virtuel à la place du routeur physique. Ce routeur est hébergé dans le PC gauche. Il est relié aux interfaces physiques eth0 et eth1, qui se comportent comme des switchs internes, faisant ainsi de la topologie virtuelle de la Fig. 3 l 'équivalent exacte de la Fig.2.

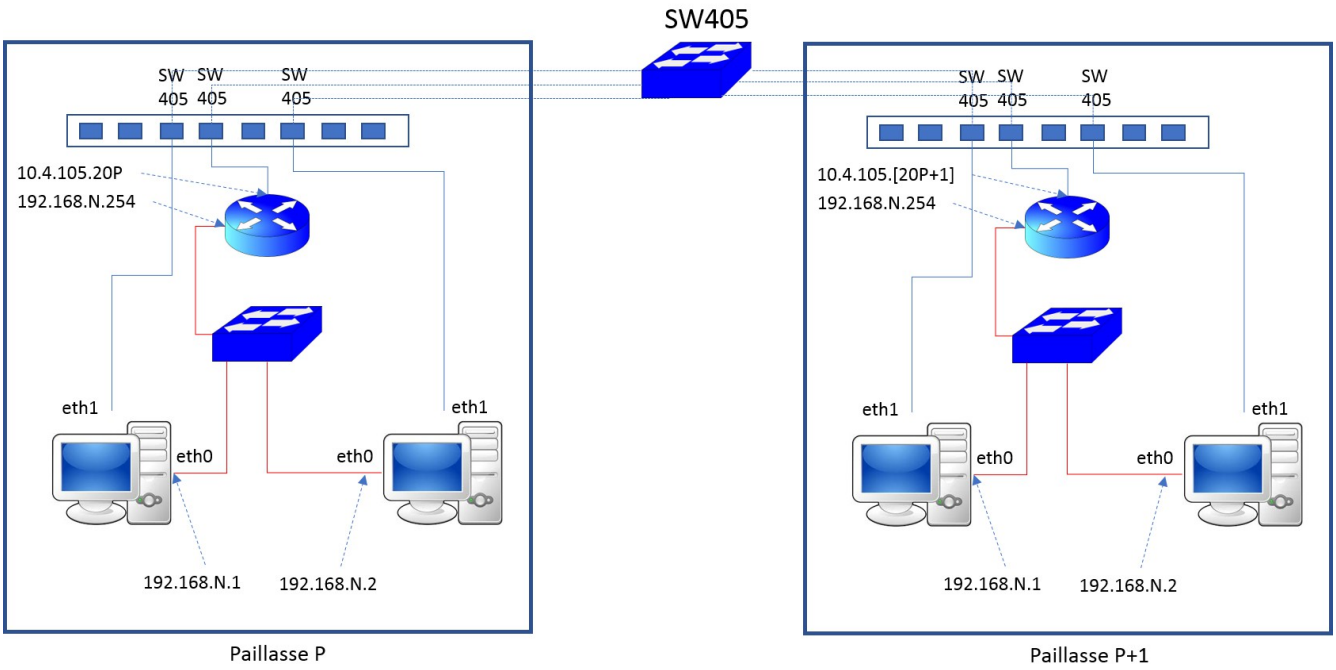


Illustration 2: Topologie physique de référence : les liens rouge sont ceux reliant les interfaces appartenant au réseau local de la paillasse ; les liens bleus à celui de la salle.

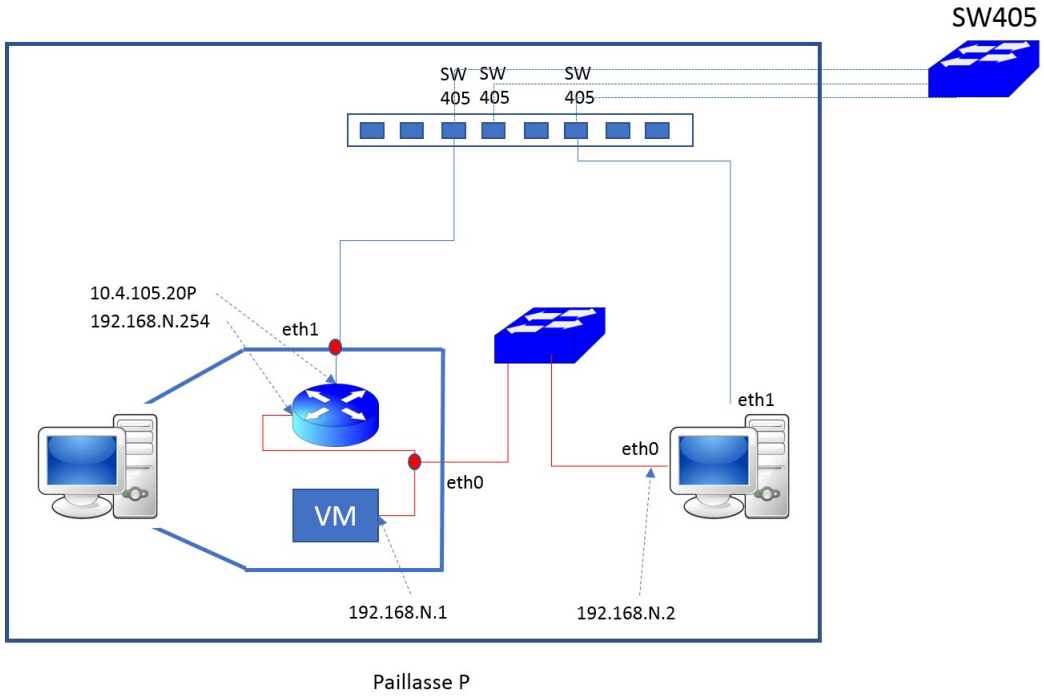


Illustration 3: Topologie équivalente de paillasse avec routeur virtuel : le PC gauche héberge une machine virtuelle et le routeur virtuel. Les points rouges sont des switchs implémentés par les interfaces physiques.

1.3 Création d'un routeur virtuel

6. Dans la barre de gauche des équipements disponibles, sélectionnez un routeur c3600 et tirez-le sur la partie centrale de la fenêtre.
7. Rajouter 2 interfaces au routeur : bouton droit sur le routeur, puis Configure → Slots. Sélectionnez le premier choix de FE (fastethernet) pour les 2 interfaces.
8. Rajoutez ensuite 2 nuages (*Clouds*), représentant les interfaces de la machine physique. Affecter un nuage à eth0 et l'autre à eth1, par clic droit sur chacun.
9. Connecter les interfaces du routeur au bon nuage par l'outil « câble » accessible depuis l'icône représentant un connecteur dans la barre d'outils supérieure.
10. Démarrez le routeur avec : bouton droit → start. Ouvrez ensuite une console en double-cliquant sur le routeur.

La console (« écran noir ») ainsi obtenue est exactement la même que celle que vous obtenez par liaison série ou telnet sur le routeur physique de la paillasse.

2 Configuration du routeur en passerelle

Dans cette partie, vous allez configurer le routeur qui sera la passerelle du réseau local de la paillasse. Ce réseau aura un adressage différent du réseau de la salle : 192.168.N.0/24, avec N= [10+num de

paillasse] en 405, N=[20+num de paillasse] en 102.

La première étape est de configurer les interfaces fa0/0 et fa1/0 chacune sur le bon réseau, comme indiqué Fig. 2.

1. Si la question initiale « Do you want to run initial configuration » apparaît, répondez « no ».
2. Accédez d'abord à la configuration de fa0/0 :

```
Routeur> enable
Routeur# config t
Router(config)# interface fast 0/0
```

3. On va maintenant la configurer (attention si vous êtes en 102, adaptez), P=[200+num de paillasse] :

```
Router(config-if)# ip address 10.4.105.P 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

4. Vérifiez par un ping (toujours depuis le routeur) que vous pouvez joindre l'adresse .251 ou .254 de la salle. Si ce n'est pas le cas, vérifiez la configuration des interfaces en tapant `sh ip int brief`, et re-faîtes les étapes précédentes si nécessaire.
5. On fait de même pour fa1/0. Accédez à sa configuration :

```
Routeur# config t
Router(config)# interface fast 1/0
```

6. On va maintenant la configurer (attention si vous êtes en 102, adaptez) :

```
(config-if)Router# ip address 192.168.N.254 255.255.255.0
(config-if)Router# no shutdown
(config-if)Router# exit
```

7. Vérifiez la bonne configuration des 2 interfaces en tapant `sh ip int brief`

Le **deuxième étape** est de configurer un processus de routage sur le routeur. Ca consiste à activer un protocole de routage, ici nous prenons OSPF. Quand un routeur recevra un paquet qui ne lui est pas destiné, il saura vers quel autre routeur le transférer. Exemple : vous enverrez à la fin un message de ping vers une VM d'une autre paillasse. Il faudra donc que votre routeur sache transférer ce paquet au routeur de la paillasse destinataire. Le protocole de routage gère donc la découverte par un routeur des réseaux accessibles par ses routeurs voisins.

8. On va donc démarrer le processus OSPF (ligne 1) et lui faire annoncer sur l'interface fa0/0 (la non-passive, ligne 3), le réseau de votre paillasse (ligne 5). Remplacez [SALLE] par ce qu'il faut.

```
Router(config)#router ospf 1
Router(config-router)#log-adjacency-changes
Router(config-router)#passive-interface fastEthernet 1/0
```

```
Router(config-router)#network 10.4.105.0 0.0.0.255 area [SALLE]
Router(config-router)#network 192.168.N.0 0.0.0.255 area [SALLE]
Router(config-router)#exit
Router(config)#exit
```

9. Une fois cela effectué, vérifiez que vos changements apparaissent exactement comme vous les avez entrés dans ce qu'affiche la commande `show running-config`

3 Configuration des VM sur le réseau local de la paillasse

Dans cette partie, vous allez configurer les VM qui seront les machines présentes sur le réseau local de la paillasse. Ce réseau a un adressage différent du réseau de la salle (voir ci-dessus).

1. Reliez eth0 des 2 PC (et ainsi fast 1/0 du routeur virtuel) au switch de votre paillasse, et allumez-le.
2. Créez une VM sur chacun de vos PC.
3. Désactivez eth1.
4. Configurez les interfaces eth0 avec le fichier d'interfaces en adresse IP fixe, avec la passerelle que vous venez de créer, et sans serveur DNS. Utilisez les adresses IP 192.168.N.0 et masque 255.255.255.0 avec :
   - N qui vaut [10+num de paillasse] en 405, [20+num de paillasse] en 102.
   - la VM sur PC gauche a l'adresse IP en .1, celle sur PC droite en .2.
5. Activez les eth0. Testez que chaque VM peut pinger les 2 interfaces du routeur et se pinger entre elles.

6. Effectuez ensuite un ping vers une VM ou la passerelle d'une autre paillasse (d'un groupe ayant terminé la configuration de leur routeur), et vérifiez que c'est un succès.

4 Analyse du fonctionnement des routeurs

1. Sur chaque routeur, faire
   `Router#show ip route`

   Indiquez ce que signifie chaque colonne, et commentez les 3 lignes apparaissant.

2. Lancer ensuite une capture Wireshark sur chacune des VM émettrice et réceptrice du ping, et analyser les adresses MAC et IP du paquet *ICMP echo request* à chaque saut. Que pouvez-vous dire ?

5 Complémenter le réseau local avec un serveur DHCP

Un réseau local dispose en général de plusieurs services (=programmes rendant des services à des machines extérieures) hébergées sur un serveur. Un de ces services de base est le service DHCP

(Protocole de Configuration Dynamique d'Hôte), qui permet à une interface s'activant de demander toutes les valeurs de paramètres réseau, si elle est configurée en « dhcp ».

1. Désactivez eth0 et activer eth1.
2. Faire `apt-get update`.
3. On veut transformer VM gauche en serveur DHCP.
   Pour cela, en extrayant la documentation nécessaire de https://wiki.debian.org/fr/DHCP_Server , configurez un serveur DHCP sur VM gauche qui serve les machine entre 192.168.N.2 et 192.168.N.50, sans DNS ni nom de domaine mais passerelle en 192.168.N.254.
   Commentez également les 2 lignes commençant par `option domain-name`.
   Il faut également mentionner « eth0 » dans le champ `INTERFACESv4=` du fichier `/etc/default/isc-dhcp-server`

   Attention, à l'installation du paquet (package), apt-get va tenter de démarrer le serveur, mais comme il n'est pas encore configuré, cela conduit à une erreur. Une fois configuré, vous pourrez le démarrer sans problème.

4. Configurez, sans encore l'activer, eth0 de VM droite en DHCP en recopiant ce que vous voyez pour eth1 dans le fichier d'interfaces.
5. Sur VM droite, désactivez eth1.
6. Activez eth0. Vérifiez par `ifconfig` que la configuration IP de eth0 est celle attendue.
7. Lancez une capture Wireshark sur VM gauche. Désactivez et ré-activez eth0, et analysez la capture : quels sont les paquets DHCP que vous voyez, et quel est leur sens ?

TP 9 et 10 – Module M1101

TP projet : un petit réseau d'entreprise

Table des matières

1 Introduction

Important :

Ce TP est un TP de type projet. Cela signifie que vous devez agir en complète autonomie. Vous pouvez vous aider des énoncés des TP précédents de M1101 pour résoudre les problèmes rencontrés. Vous devez utiliser l'accès Web pour toute commande que vous devez utiliser et dont vous ne connaissez pas la syntaxe (ou les manpages, vous devez vous débrouiller seuls).

Le rôle de l'enseignant se limite à valider votre avancement aux différentes étapes, correspondant à chaque fin de section ou sous-section.

Vous disposez de 6 heures pour faire la totalité de ce TP.

Appeler l'enseignant en fin de chaque sous-partie validation une fois que vous avez vérifié que ce qui est demandé fonctionne.

Objectifs du TP :

Le principe de ce TP est que chaque paillasse reproduise in fine, un réseau privé interconnecté au réseau public, comme peut l'être une PME connectée à Internet par une box DSL (LiveBox, FreeBox, etc.). De plus, vous allez installer un serveur Web sur chaque paillasse et faire en sorte d'y accéder depuis les autres paillasses.

Pour la suite de ce TP, le chiffe N utilisé pour les adresses correspondra au numéro de votre paillasse plus 10 (N=Numéro_paillasse+10).

NB : Vous pouvez accéder aux pages en https depuis les machines physiques sur le réseau

10.4.105.0/24 avec un proxy web : `wall.unice.fr` et port `3128`.

La configuration des interfaces des VMs doit se faire par le fichier d'interfaces, tel qu'en M1102.

2 Configuration simple d'un réseau local par paillasse, avec passerelle

Dans cette partie, vous allez configurer un réseau local sur lequel seront connectées les VM de votre paillasse. Ce réseau aura un adressage différent du réseau de la salle 405 :192.168.N.0/24, avec N= [10+num de paillasse] en 405, N=[20+num de paillasse] en 102. La configuration à reproduire est celle des Figures 2 et 3 du TP8.
NB : un routeur par paillasse

2.1 Sans routeur et en IP fixe

1. Créez un VM sur chaque PC.
2. Configurez eth0 de vos VM comme désiré (en IP fixe).
3. Désactivez eth1, activez eth0, et effectuez le câblage adéquat avec le switch.
4. Vérifiez la connexion à votre réseau local par un ping dans chaque sens entre les 2 VM.

2.2 Rajout de la passerelle

1. Toujours en reproduisant la configuration de Fig. 3 du TP8, créer un routeur virtuel et configurez-le pour que sa fastEthernet 0/0 soit en 10.4.105.[200+P]/24, et fastEthernet 1/0 soit en 192.168.N.254/24, et qu'il annonce ces réseaux avec OSPF.
2. Vérifiez que vos VM peuvent pinger les 2 interfaces du routeur ainsi que tout autre routeur ou VM des paillasses déjà configurées.

3 Installation d'un serveur Web

Transformez votre VM Debian en serveur Web avec le programme Apache, en installant le paquet apache2 (`apt-get install apache2`).

NB : un serveur Web par VM (2 par paillasse)

3.1.1 Serveur Web basique

1. Vérifiez que le serveur est actif en demandant depuis un navigateur dont vous aurez au préalable enlevé le proxy (depuis Preferences de Firefox) : `http://localhost/index.html`
2. Personnalisez votre page d'accueil en modifiant le fichier `/var/www/html/index.html` à la ligne « It works » en « Ici Paillasse [N] »et vérifiez l'accessibilité de votre serveur Web depuis l'autre VM.
3. Tester la connexion vers les autres serveurs Web :

http://192.168.N.1/index.html ou http://192.168.N.2/index.html pour différents N.

3.1.2 Pages Web des utilisateurs

Nous allons ici créer un nouvel utilisateur puis faire en sorte qu'il puisse créer ses propres pages Web.

1. Créez un utilisateur (utilisez votre prénom comme identifiant) avec la commande `adduser`.
2. Placez-vous dans le répertoire racine de cet utilisateur et créez un répertoire `public_html` (commande `mkdir`). Copiez dans ce répertoire le fichier `/var/www/index.html` et personnalisez le (commande `cp`) en remplaçant « Ici Paillasse [N] » en « Ici [PRENOM] ».
3. Il faut maintenant qu'Apache autorise les utilisateurs à publier leurs pages personnelles. Pour cela :

- Placez vous dans `/etc/apache2/mods-enabled`
- Tapez la commande `a2enmod userdir`
- Redémarrez le serveur Apache

4. Vérifiez l'accessibilité de la page d'accueil de votre utilisateur depuis l'autre VM : `http://192.168.N.1/~prenom`

3.2 Fichier hosts

Utilisez les adresses IP n'est pas très pratique et nous préférons en général utiliser des noms. C'est le service DNS qui offre la traduction entre nom et adresse IP. L'ancêtre (toujours vivant) du DNS est le fichier `hosts` qui est dans le répertoire `/etc/`.

1. Ajouter les lignes suivantes (il faut être root) pour votre machine et celle d'une paillasse voisine dans ce fichier :
   192.168.N.1 www.pailN.fr où pailN est à personnaliser.
2. Vérifiez que vous pouvez utilisez ces noms pour joindre votre serveur Web et celui d'une paillasse autre que la vôtre.

4 Configuration d'un réseau privé non visible de l'extérieur : le NAT

4.1 Introduction à la traduction d'adresses réseau (Network Address Translation - NAT)

Depuis le début de ce TP projet, toutes les machines ont des adresses IP distinctes. Dans la pratique des réseaux d'entreprise (où même domestiques), on utilise un réseau IP dit « privé » : 2 machines dans des réseaux privés différents peuvent avoir la même adresse IP (ceci permet de limiter le nombre d'adresses IP dont on a besoin pour les machines clientes). Lorsqu'une telle machine a besoin d'accéder à un réseau extérieur (à l'Internet), pour être identifier de façon unique elle utilise l'adresse IP de la

passerelle (FreeBox, Livebox, le routeur local). Pour que cela puisse se faire, la passerelle doit implémenter la fonction de NAT : modifier à la volée l'adresse IP source des paquets IP reçus d'une machine du réseau privé local et qui partent vers l'extérieur, et l'adresse IP destination des paquets qui arrivent à la passerelle depuis l'extérieur et à destination d'une machine du réseau privé.

Avec ce système, on a besoin que d'une seule adresse IP pour toutes les machines du réseau (tant que celui-ci n'a pas plus que quelque dizaines de machines). De plus, 2 machines dans 2 réseaux privés distincts peuvent avoir les mêmes adresses sans que cela soit un problème puisque leurs identifiants, si elles communiquent entre elles, seront distincts (les adresses IP publiques de leur passerelle). Notez que vous avez vu jusque là qu'un routeur ne modifie pas les adresses IP : c'est effectivement le cas si cette option NAT n'est pas activée.

4.2 Configuration du routeur en mode NAT basique

Votre réseau de paillasse va maintenant être en 192.168.0.0/24 (le même pour toutes les paillasses donc).

1. Re-configurez la bonne interface du routeur correctement.
2. Reconfigurez donc vos VM, pour que leurs IP fixes soit 192.168.0.1/24 et 192.168.0.2/24, respectivement et leur passerelle par défaut de votre interface en 192.168.0.254.
3. Vérifiez que vous ne pouvez pas joindre tout routeur d'une autre paillasse.
4. Configurez un mode NAT sur le routeur, graĉe aux sections « Configuration commune à tout type de NAT » et « Configuration du NAT dynamique avec surcharge (sans pool) »: http://www.ciscomadesimple.be/2013/04/06/configuration-du-nat-sur-un-routeur-cisco/
5. Vérifiez que vous pouvez joindre tout routeur d'une autre paillasse depuis vos VM.
6. Vérifiez que vous ne pouvez plus joindre le serveur Web sur une VM d'une paillasse autre que la vôtre.

4.3 NAT et re-direction de port : accès depuis l'extérieur à une machine du réseau privé

On désire maintenant pouvoir joindre de l'extérieur un serveur Web hébergé sur le réseau privé. On doit donc configurer le routeur pour qu'il transfère tous les paquets entrant par l'adresse publique 10.4.105.20N sur le port TCP 80 vers l'adresse privée de votre serveur Web gauche (en 192.168.0.1).

1. Utilisez le lien ci-dessous pour cette configuration de traduction statique de port (*static PAT*) : http://www.cisco.com/en/US/tech/tk175/tk15/technologies_configuration_example09186a0080093e51.shtml
2. Vérifiez que vous pouvez de nouveau joindre le serveur Web sur une VM d'une paillasse autre que la vôtre. Quelle est l'adresse IP à utiliser ?
3. Effectuez la même opération pour que le serveur Web droit soit joignable sur le port 81.
4. Vérifiez depuis l'extérieur que le serveur droit peut aussi être joint, et indiquer le port à utiliser.

5 Avec un serveur DHCP

On veut transformer VM gauche en serveur DHCP.

1. Pour cela, en extrayant la documentation nécessaire de https://wiki.debian.org/fr/DHCP_Server , configurez un serveur DHCP sur VM gauche qui

serve les machine entre 192.168.0.2 et 192.168.0.50, sans DNS ni nom de domaine mais passerelle en 192.168.0.254. Attention lors de l'installation du serveur, vous devez être connecté à Internet par le biais de eth1 restée en DHCP, (désactiver eth0 à ce moment-là).
(Attention, à l'installation du paquet (package), apt-get va tenter de démarrer le serveur, mais comme il n'est pas encore configuré, cela conduit à une erreur. Une fois configuré, vous pourrez le démarrer sans problème.)

2. Configurez eth0 de VM droite en DHCP.
3. Désactivez et ré-activez eth0, et vérifiez l'adresse IP obtenue.
4. Re-faîtes le processus en lançant une capture Wireshark sur VM gauche, ensuite à analyser : quels sont les paquets successifs relatifs à DHCP ?