

RESEAUX

MISE EN ŒUVRE

Objectif :

Ce TD/TP consiste à appliquer les concepts théoriques concernant les routeurs à un cas pratique afin d'assimiler les notions élémentaires de protocole, de routage, et plus largement l'activité des éléments actifs d'un réseau.

Ce TD/TP se décompose en trois parties :

- ◆ **Partie I – Mise en place d'un laboratoire virtuel.**
 - ⇒ Installation/Manipulation d'un simulateur réseau graphique afin de simuler la mise en œuvre de topologie réseau complexe.
 - ⇒ Simulation du déploiement d'un routeur Cisco

- ◆ **Partie II – Analyse des propriétés fonctionnelles et non fonctionnelles d'un routeur.**
 - ⇒ Etude des différents éléments d'un routeur
 - ⇒ Analyse des différents modes de fonctionnement d'un routeur

- ◆ **Partie III – Mise en pratique des concepts fondamentaux des réseaux.**
 - ⇒ Réalisation d'une configuration basic de routeur
 - ⇒ Tester le réseau mis en œuvre
 - ⇒ Initiation à l'analyse (capture et détramage) d'un protocole réseau.
 - ⇒ Découverte des protocoles CDP, ARP, DHCP
 - ⇒ Principe du résolveur DNS

- ◆ **Résumé des commandes apprises**

Ce TD/TP repose sur deux principaux outils *open source* : Dynamips¹ et gns3².

¹ http://www.ipflow.utc.fr/index.php/Cisco_7200_Simulator

² <http://www.gns3.net/>

Partie I

1. Récupérer l'archive contenant le simulateur à l'url suivante :
⇒ <http://dept-info.labri.fr/~bromberg/simul/lab.tgz>
2. Décompresser l'archive dans votre répertoire de travail.
⇒ Vous devriez trouver trois répertoires distincts :
 - GNS3-0.6.x : répertoire contenant l'interface graphique du simulateur Cisco
 - Dynamips : répertoire contenant le simulateur
 - ios : répertoire contenant les images systèmes des routeurs Cisco de la famille 7200 et 3600.
3. Lancer le programme gns3.
4. Indiquez à GNS3 où se trouve le simulateur Cisco (voir Fig.1).
⇒ Ouvrir la boîte de dialogue **Préférences**
⇒ Sélectionner l'onglet **Dynamips**
⇒ Dans le champ *Exécutable Path* indiquer le répertoire *dynamips* **de votre répertoire de travail** et sélectionner le binaire *dynamips-0.2.8-RC2-xxx.bin* qui correspond à votre plateforme.

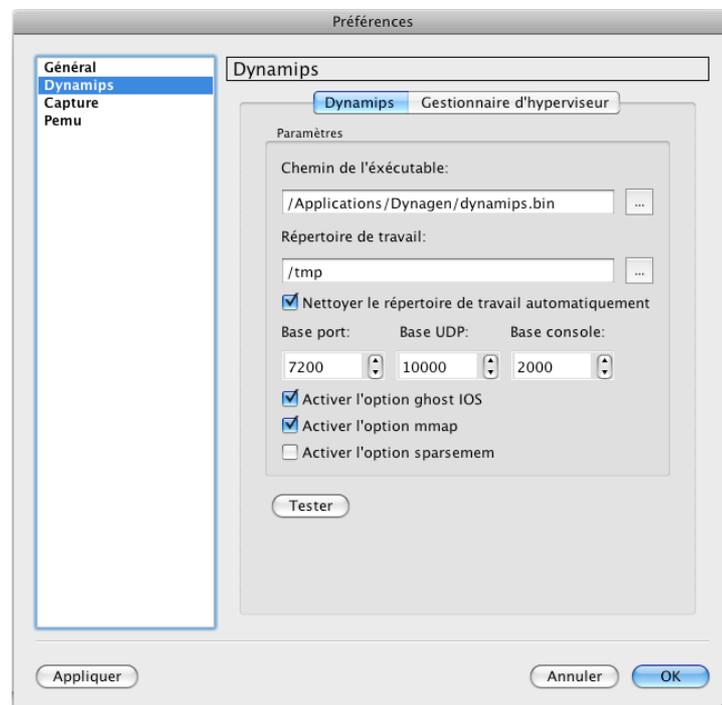


Fig. 1. Localisation du binaire de *dynamips*

- ⇒ Cliquer sur le bouton Tester pour vérifier que le simulateur fonctionne correctement.

- Vous devez maintenant indiquer à GNS3 où se situent les images des routeurs Cisco (voir Fig.2). Pour se faire, ouvrir la boîte de dialogue intitulée IOS images and hypervisors et ajouter les deux images Cisco contenu dans votre répertoire ios. Si vous êtes curieux, vous pouvez consulter la fiche technique des routeurs simuler sur le site de Cisco.

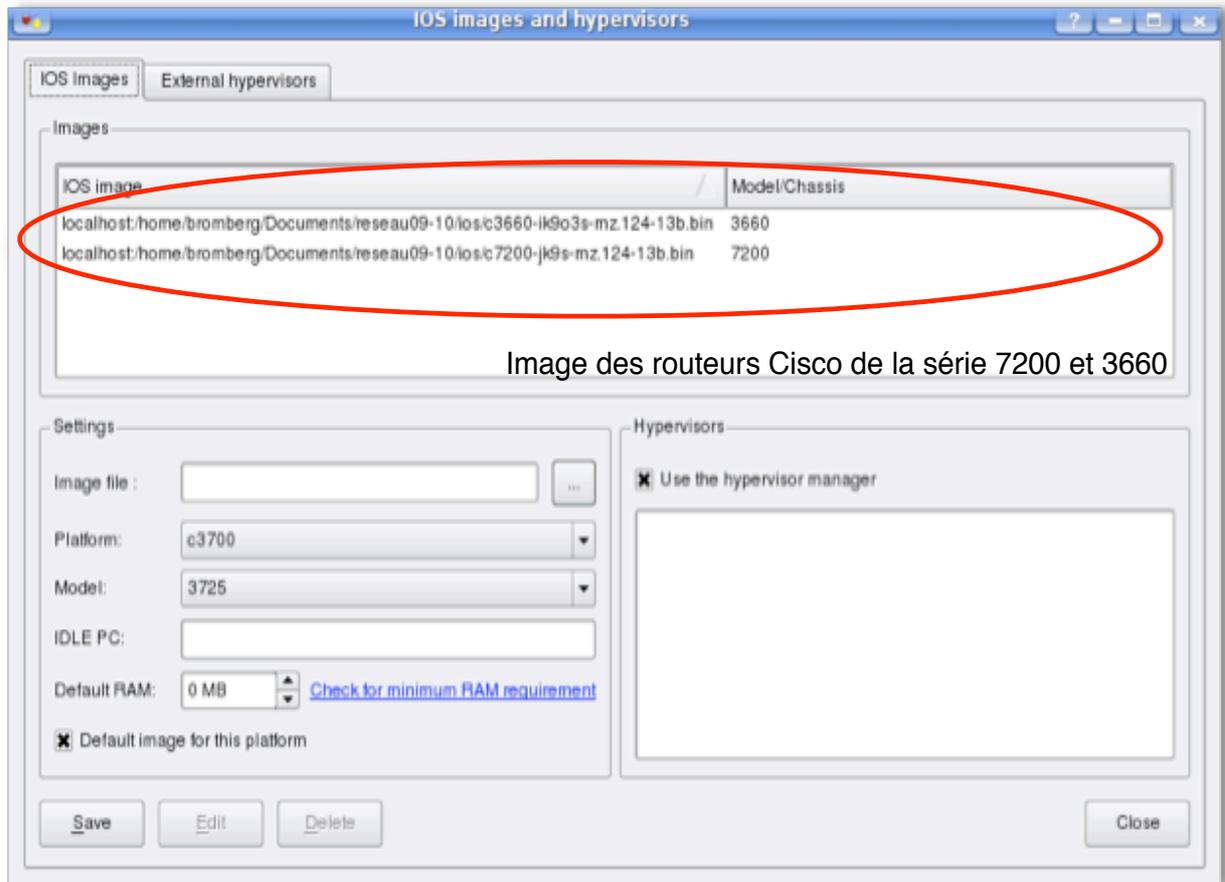


Fig2. Localisation des images des routeurs Cisco

6. GNS3 est maintenant fonctionnel, il vous est dorénavant possible de glisser/déposer un routeur de la série 7200 sur le plan de travail (voir Fig.3).

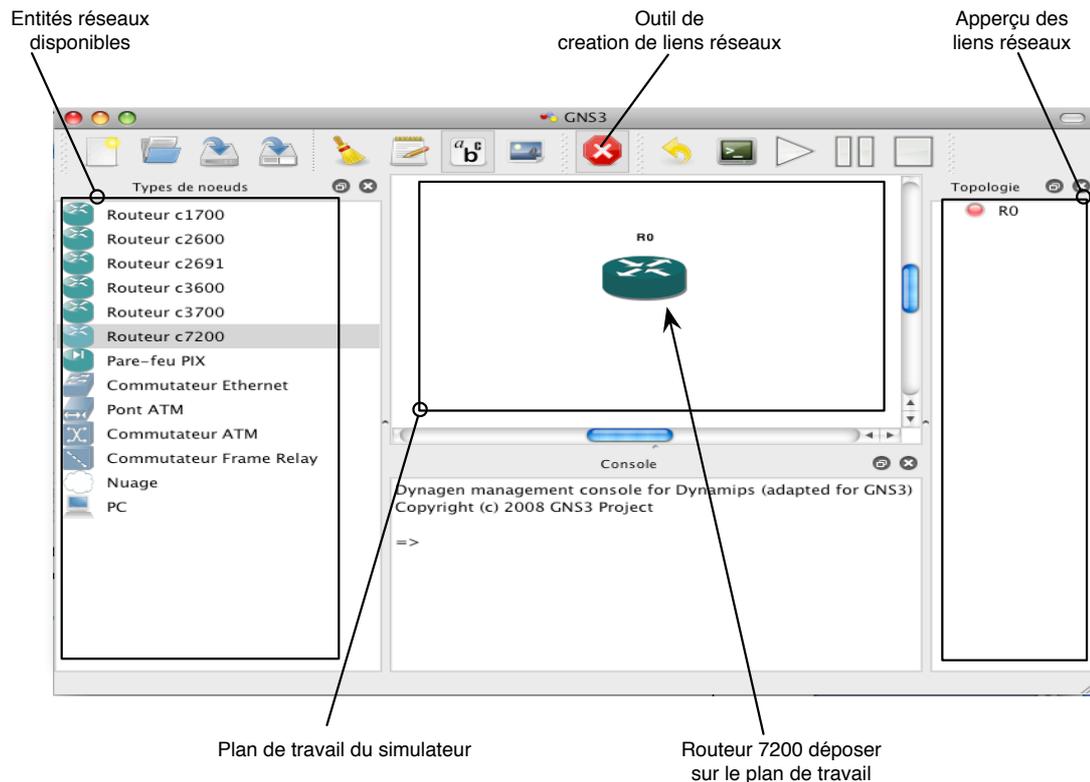


Fig3. Détail de la fenêtre du simulateur

7. Faire un clic droit sur le routeur déposé sur le plan de travail et démarrer le. Par défaut, le simulateur consomme 100% du CPU car il n'a aucune connaissance des moments d'inactivité des machines virtuelles en cours d'exécution. Pour résoudre ce problème, on fixe une valeur *idle-pc* pour forcer la mise en veille des machines virtuelles lorsqu'elles rentrent dans des cycles d'inactivité.
8. Pour fixer la valeur *idle-pc* la plus adéquate, faire un clic droit sur le routeur et sélectionner l'action *idle-pc*, le simulateur calculera automatiquement la valeur la plus judicieuse.
9. Comme décrit sur le site du constructeur³, les routeurs de la série 7200 sont des routeurs modulaires ce qui les rend facilement extensible. Vérifier que votre routeur est équipé du module C7200-IO-2FE (2 ports Fast Ethernet / Ethernet).
- ⇒ Faire un clic droit sur le routeur ; sélectionner configurer ; Dans la boîte de dialogue, sélectionner le routeur concerné ; puis dans l'onglet slots, vérifier que dans le slot0 se trouve bien le module C7200-IO-2FE.

³ <http://www.cisco.com/en/US/products/hw/routers/ps341/>

Partie II

Configuration interne d'un routeur

On rappelle qu'un routeur se distingue des autres entités réseaux comme les Ponts, les Hubs, et les Switch par le fait qu'il embarque un processeur, un système d'exploitation et de la mémoire. La Figure 4, illustre la structure interne généralement observée d'un routeur.

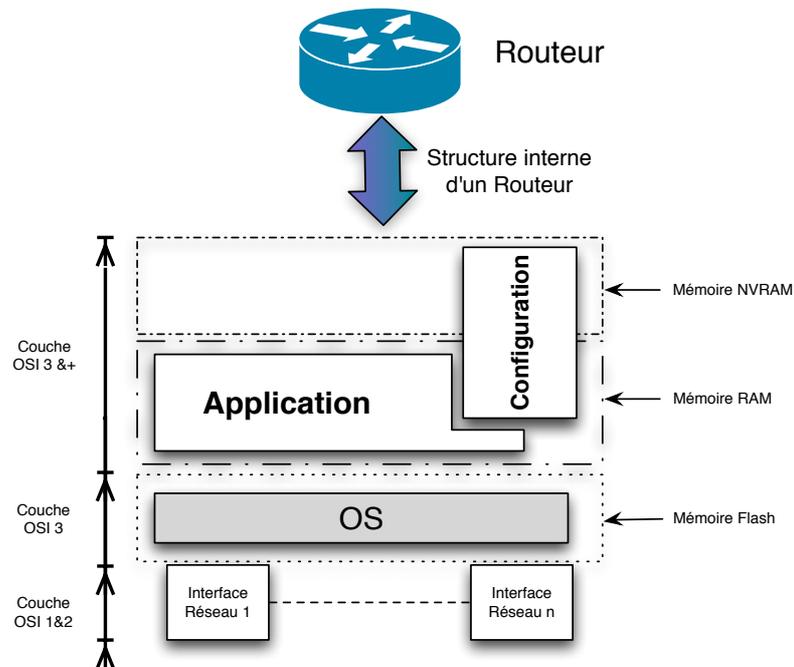


Fig. 4. Structure interne d'un routeur

Dans la suite de cette partie, nous allons nous intéresser aux différents principes de fonctionnement/configuration de l'OS des routeurs de type Cisco (IOS).

Les modes de l'IOS Cisco

L'OS des routeurs Cisco dispose de deux principaux modes de fonctionnement : (i) le *mode utilisateur* et (ii) le *mode privilège*. Par défaut, lorsque l'on se connecte au routeur, l'utilisateur se trouve dans le *mode utilisateur* ; Le *mode utilisateur* est caractérisé par l'invite de commande '>' (voir Fig.5 ❶) tandis que le *mode privilège* est caractérisé par l'invite de commande '#' (voir Fig.5 ❷) . Un mode peut être décomposé en sous modes. Par exemple, la configuration d'une interface réseau se fait par le sous mode *config-if* du *mode configuration* (voir Fig.5 ❹) .

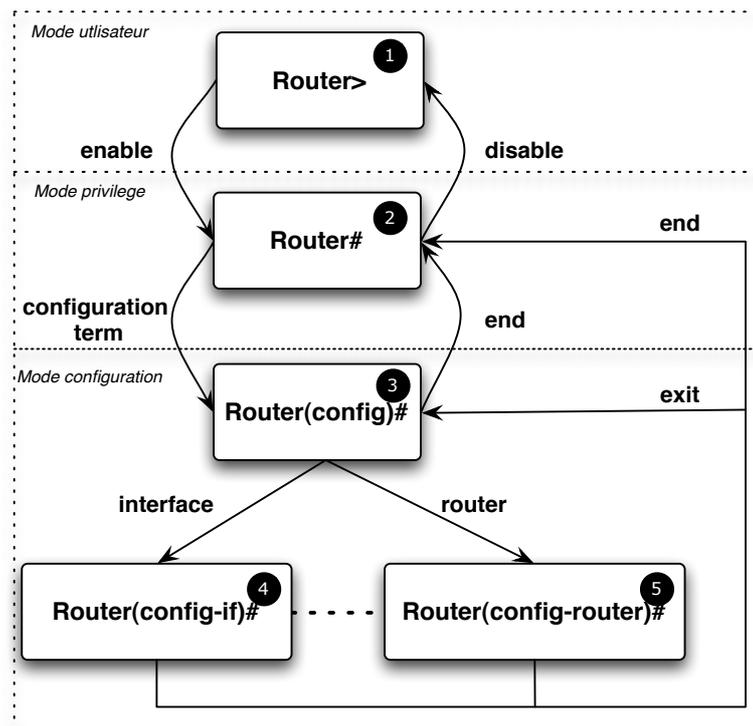


Fig. 5. Mode de fonctionnement d'un routeur Cisco

1. Connectez vous au routeur précédemment déposé sur le plan de travail. Faire un clic droit sur le routeur et sélectionner **console** pour ouvrir la console du routeur. A la question **Would you like to enter the initial configuration dialog ?**, répondre **no**.
2. Chaque mode de fonctionnement dispose d'une liste limitée de commandes. Pour afficher les commandes disponibles dans un mode, utilisez la commande **?**. Saisir la commande **exit** ou tapez **Ctrl-Z** pour sortir d'un mode. Comparez les commandes disponibles dans le *mode utilisateur* (Fig.5 ❶) , *privilège* (voir Fig.5 ❷) et *configuration* (voir Fig.5 ❸) .
3. Suivant les modes de fonctionnement, les commandes n'offrent pas les mêmes options. Comparer le résultat des commandes **show ?** dans le *mode utilisateur* et *privilège*. Exécutez la commande **show running-config** dans le *mode utilisateur*. Que se passe t'il ? Réitérez dans le *mode privilégié*. Quelles sont les caractéristiques des interfaces réseaux du routeur ? Identifiez le nom du routeur. Changer le nom du routeur.

4. Changer le message du jour. Dans le mode configuration, tapez **banner motd #** puis saisir une phrase sur 2 lignes. Sortir du mode faisant un **exit** ou **Ctrl-Z**
5. Protéger l'accès au *mode privilège* en spécifiant un mot de passe. Dans le mode configuration, utiliser la commande **enable password**.
6. On cherche à modifier la description de l'interface FastEthernet du slot 0/0. Quel mode devez vous utiliser ? Une fois dans ce mode, chercher la commande adéquate, ajouter une description puis sortir du mode faisant un **exit** ou **Ctrl-Z**.
7. Toutes les commandes précédentes modifient la configuration active du routeur. Selon vous dans quelle zone mémoire se situe la configuration active du routeur ? Que se passe t'il si vous redémarrez le routeur ?
8. Quelle est la principale caractéristique de la mémoire NVRAM ? Dans le mode privilège, vérifier le contenu de la mémoire NVRAM du routeur (**dir nvram:**). Tapez **copy running-config startup-config**. Quel est l'effet de cette commande ? vérifier.
9. En cas de mauvaises manipulations, vous pouvez toujours effacer le fichier *startup-config* par la commande **erase startup-config**.
10. Tapez les commandes ci-dessous et précisez à quel niveau OSI les commandes suivantes collectent les informations :
 - a. show interface
 - b. show ip interface
 - c. show ip route
 - d. ping

Ces commandes vous seront utiles ultérieurement pour vérifier la configuration du routeur.

Partie III

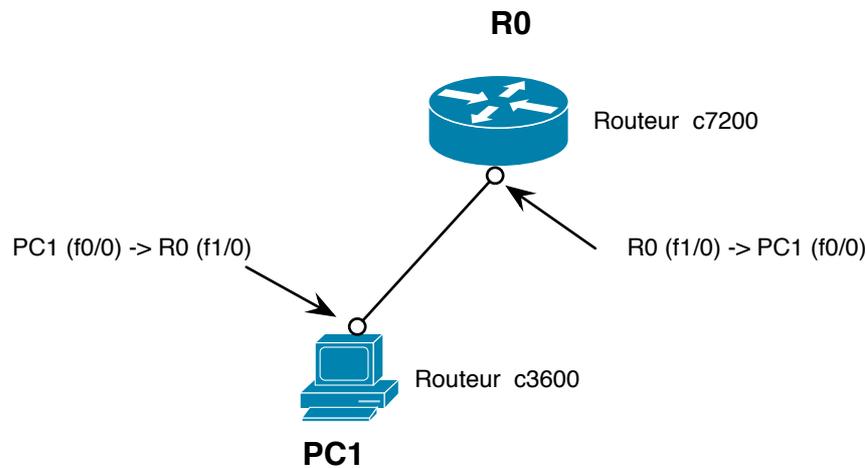


Figure 1 - Prise en main d'un routeur.

Configuration basique du routeur

1. Lancer le simulateur GNS3. Glisser/déposer deux routeurs sur le plan de travail. Un routeur du type c7200 fera office de routeur et un autre de type c3600 fera office de PC. Reliez les deux entités par un câble *FastEthernet*.
2. Changer le nom du routeur c7200 afin qu'il se nomme R0 et changer le nom du routeur c3600 afin qu'il se nomme PC1.
3. Quelles sont les caractéristiques IP par défaut du routeur ?
4. Assigner l'adresse IP 192.168.1.1 au routeur R0. Rappeler à quoi sert le *netmask*, et indiquer/justifier quel *netmask* avez vous choisi.
5. Vérifier la configuration IP de l'interface et activer là.

Initiation à l'analyse de protocole : exemple de CDP et ECTP

6. Activer la capture de l'interface *FastEthernet* du routeur connecté à PC1 (*R0 (f1/0) -> PC1 (f0/0)*). Patienter quelques minutes et lancer *Wireshark* sur la capture réalisée. Identifier les protocoles utilisés sur lien réseau.
7. Identifier les trames encapsulant le protocole CDP (*Cisco Discovery Protocol*). En analysant la trame vous devriez comprendre le rôle de ce protocole et pouvoir répondre aux questions suivantes. A chaque réponse indiquer à quelle couche du modèle OSI vous vous situez.
 - a. A qui est destiné le message envoyé ? Quelle est l'adresse IP du destinataire ? Pourquoi ?
 - b. Quelle est la fréquence de ces messages ?
 - c. Quelles informations fondamentales ce protocole véhicule ?

8. Réinitialiser la capture du trafic réseau de *Wireshark* (arrêter, puis démarrer une nouvelle capture). Assigner dorénavant une adresse IP à la station PC1 de façon à ce qu'elle soit sur le même réseau IP que le routeur R0. La station PC1 utilise t'elle le protocole CDP ? Pourquoi ?
9. Tester alternativement les commandes relatives au protocole CDP sur le routeur R0 et la station PC1 *via* les commandes ***show cdp traffic***, ***show cdp neighbors***, ***show cdp neighbors détail***, ***show cdp***. Ces commandes génèrent-elles de nouveaux messages CDP sur le réseau ? Quel est le mode de fonctionnement de ce protocole ?
10. Le protocole CDP ne nous sera plus utile momentanément. Désactiver CDP de l'interface, sur laquelle le protocole a été perçu, à l'aide de la commande ***no cdp run*** sur chaque routeur. Cette commande génère t'elle du trafic réseau ? Pourquoi ? L'usage du protocole CDP peut-il être gênant sur un réseau de production ? Pourquoi ?
11. A terme, vous ne devriez capturer plus que des messages réseaux issus du protocole ECTP (Ethernet Configuration Testing Protocol). A votre avis, suivant la capture *Wireshark* obtenue, dans quel but le protocole ECTP est-il utilisé par les routeurs CISCO ?
12. Désactiver le protocole ECTP sur chacune des interfaces utilisées *via* la commande ***no keepalive***. Normalement vous ne devriez ne plus avoir de trafic capturé.

Analyse d'ARP

13. Réinitialiser la capture réseau. Faire un ***ping*** du routeur R0 vers PC1 et *vice versa*. Vous devriez obtenir la capture réseau suivante :

No..	Time	Source	Destination	Protocol	Info
1	0.000000	ca:0a:01:45:00:1c	Broadcast	ARP	Who has 192.168.1.2? Tell 192.168.1.1
2	0.015122	cc:06:01:45:00:00	ca:0a:01:45:00:1c	ARP	192.168.1.2 is at cc:06:01:45:00:00
3	1.991250	192.168.1.1	192.168.1.2	ICMP	Echo (ping) request
4	2.001908	192.168.1.2	192.168.1.1	ICMP	Echo (ping) reply

Figure 2 – Analyse du trafic réseau.

Suivant votre capture, déduisez le rôle du protocole ARP ? Pourquoi le protocole ICMP est-il utilisé ? Faire un diagramme de séquence des messages véhiculés sur le réseau et provoqués par la commande ***ping***.

14. Quelle est la valeur de l'@ Ethernet source et destination d'une requête ARP ? Pourquoi ?
15. A votre avis, que se passe t'il si de très nombreux paquets ARP sont générés sur le réseau ? Pourquoi ?
16. Répéter plusieurs ***ping*** de R0 vers PC1 et *vice versa*. De nouveaux messages **ARP** sont-ils de nouveau émis ? Si oui justifiez, sinon précisez les différents cas susceptibles d'être responsable d'une nouvelle génération de messages ARP.
17. Que se passe t'il si vous changez l'adresse IP de la station PC1 ? Justifiez, testez et décrire la trace réseau correspondante Percevez-vous de nouveaux messages ARP ? pourquoi ?

18. Peut-on utiliser ARP sur Internet ? Pourquoi ?

Résolution de nom statique

19. Faire un **ping R0** et/ou **ping PC1** à partir de PC1. Quel est le retour de la commande ? Pourquoi ? Analyser/expliquer en conséquence la trace réseau résultante.

20. Saisir les commandes suivantes sur PC1 : **config t ; ip host PC1 @IP_PC1 ; ip host R0 @IP_R0 ; end** et refaire un **ping R0** et/out un **ping PC1** à partir de R0 et de PC1. Quels sont les retours de ces commandes ? Pourquoi ? Analyser/expliquer en conséquence les traces réseau résultantes. Quels sont les avantages et/ou inconvénients des commandes tapées ?

21. Faire un **ping www.google.fr**. Quelles observations peut on faire ? Rappeler le fonctionnement de la résolution de nom et schématiser le fonctionnement du **resolver**.

22. Saisir les commandes suivantes : **config t ; no ip domain lookup**. Quel est l'effet de ces commandes ? Pourquoi ? Quels sont les répercussions sur la stratégie du resolver ?

Notion de routage

L'administrateur décide de modifier la topologie du réseau, et obtient la topologie suivante.

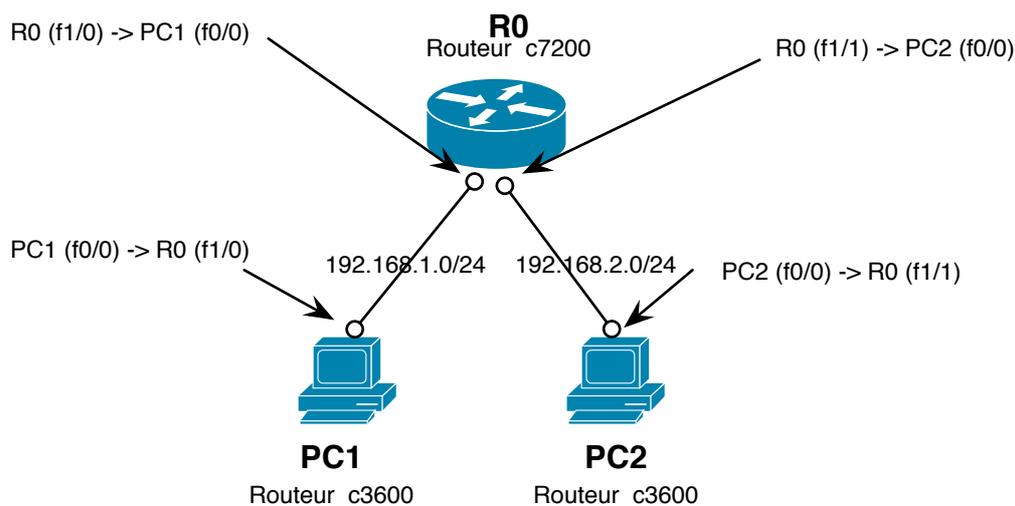


Figure 3 – Modification de la topologie

23. Répercuter les modifications de topologie sur votre topologie et configurer en conséquence la station PC2 (Ne pas oublier de désactiver le protocole CDP et ETCP de son interface active). Indiquer les commandes effectuer sur chaque entité concernée.

24. Démarrer la capture du trafic réseau sur les interfaces PC1(f0/0) et PC2(f0/0). On souhaite à partir de la station PC1 faire un **ping** de la station PC2. **Théoriquement** : sur le schéma de la Figure 3: (i) indiquer quels sont les messages ARP générés et leurs cheminements au travers le réseau, (ii) indiquer également le cheminement des messages ICMP. **Par la pratique**, vérifier la validité de vos réponses précédentes et analyser les traces sur les deux segments réseaux. Les requêtes ICMP de type ECHO atteignent-elles les interfaces f1/0 et f1/1 du routeur R0 et l'interface de la station PC2 ? Pourquoi ?

25. Saisissez les commandes suivantes sur la station PC1 : **ip route 0.0.0.0 0.0.0.0 192.168.1.1**. Quel est l'effet de cette commande ? (Aidez vous des traces réseaux issues de la capture, et relever quels sont les @MACs et @IPs source et destination). Les requêtes ICMP de type ECHO atteignent-elles les interfaces f1/0 et f1/1 du routeur R0 et l'interface de la station PC2 ? Mettre à jour votre schéma précédent à partir de votre expérimentation.
26. A partir des traces réseau, indiquer si les requêtes ICMP de type ECHO sont elles suivies de réponses ICMP de type ECHO. Justifiez, et sinon identifier le problème et rectifier le.

Attribution dynamique d'adresse IP

L'administrateur ajoute de nouvelles stations et décide d'utiliser DHCP pour attribuer automatiquement une @IP aux stations du réseau. Il obtient la topologie suivante :

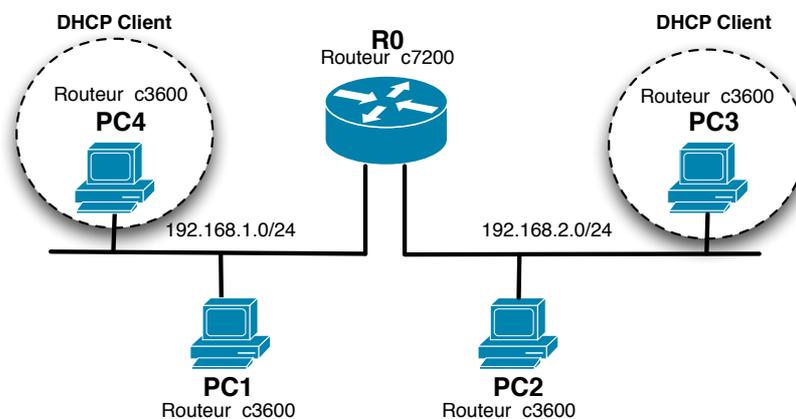
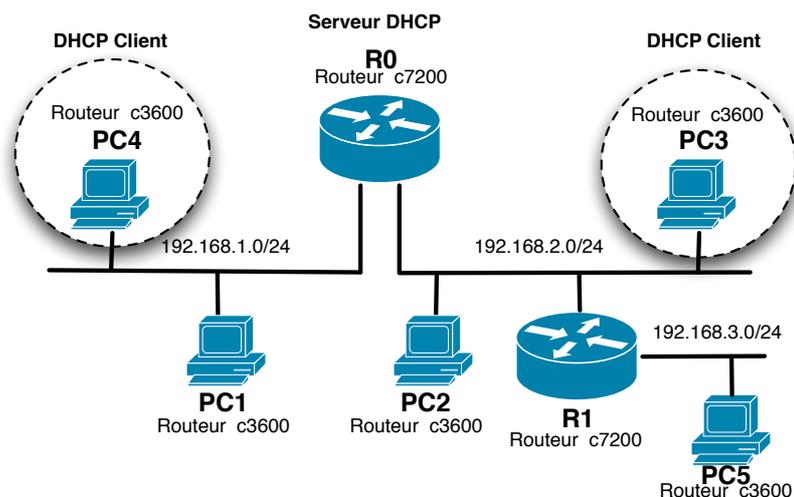


Figure 4 – Activation du service DHCP

27. Répercuter les modifications de topologie sur votre topologie. Quel(s) élément(s) actif(s) allez vous rajouter à votre réseau ? Ne pas configurer manuellement les @IP des stations PC3 et PC4. (Ne pas oublier de désactiver le protocole CDP et ETCP de son interface active)
28. Les stations PC1 et PC2 restent configurées manuellement, par contre les stations PC4 et PC3 deviennent des clients DHCP. Activer la capture de trafic sur le réseau 192.168.1.0/24 et 192.168.2.0/24. Activer le client DHCP sur ces stations, utiliser la commande **ip address dhcp** sur les interfaces réseaux concernées.
29. Vérifier que le DHCP a bien été activé. Quelles sont les conséquences de l'activation du client DHCP sur les stations PC4 et PC3 sur le réseau ? Analyser les traces réseaux. Indiquer :
- Quels sont les messages générés,
 - Quels sont les protocoles sous-jacents,
 - Comment sont encapsuler les messages,
 - Pour chaque message, précisez quels sont les @Ethernet/IP source et destination, les ports utilisés, les options utilisés.
 - Quelles sont les informations que cherche à obtenir le client DHCP ?

30. L'attribution dynamique d'@IP fonctionne selon un mode client/serveur. Activer le serveur DHCP sur le routeur R0 *via* les commandes **service dhcp** ; **ip dhcp pool nom_du_pool**; Dans le sous *mode dhcp*, lister l'ensemble des commandes disponibles. Indiquer le réseau IP sur lequel vous souhaitez activer le serveur DHCP et Configurer l'option qui permet d'ajouter un routeur par défaut.
31. Combien de réseaux IP devez-vous configurer ? Pourquoi ?
32. Sur le réseau 192.168.1.0/24, Quelles sont les conséquences de l'activation du serveur DHCP sur le routeur ? Analyser les traces réseaux. Indiquer :
- Quels sont les messages générés,
 - Indiquer les raisons pour lesquelles ces messages sont de type *Broadcast* ou *Unicast*,
 - Pourquoi des messages ARP sont-ils générés ? justifiez.
 - Pour chaque message, précisez quels sont les @Ethernet/IP source et destination, les ports utilisés, les options utilisées.
33. Une erreur, indiquant qu'il y a un conflit d'@IP, est susceptible de s'afficher sur la console du routeur R0. Indiquer pourquoi et résoudre le problème. Pour vérifier la configuration DHCP du routeur utiliser la commande **show ip dhcp arg**.
34. A partir des précédentes questions, donner un diagramme de séquence des messages qui transitent dans le réseau afin d'affecter une @IP à une station.
35. Annoter le schéma de la Figure 4 en indiquant le cheminement des différents messages sur le réseau.
36. L'administrateur du réseau décide de rajouter un nouveau réseau. Mettez à jour votre topologie suivant le schéma ci-dessous.



37. Activer la station PC5 comme client DHCP. Suivant les traces réseaux, la station parvient-elle à obtenir une @IP à partir du serveur DHCP ? Pourquoi ? Proposer une solution, discuter des avantages/inconvénients.

38. Activer la capture du trafic sur le réseau 192.168.2.0/24 et sur le réseau 192.168.3.0/24. Sur le routeur R1, paramétrer l'interface du routeur connectée au réseau 192.168.3.0 en tapant la commande **ip helper-address 192.168.2.1**. Sur la station PC5, réitérer le renouvellement d'un bail DHCP *via* la commande **renew dhcp**. En vous aidant des traces réseaux, indiquer quelle est la conséquence de la commande taper sur le router R1 ?
39. La station PC5 obtient-elle son @IP dynamique ? Si non, déterminer le problème et le résoudre.
40. Donner le diagramme de séquence des messages échangés qui ont permis à la station PC5 d'obtenir une @IP dynamiquement.