

### À lire attentivement : consignes pour toute la série des TPs

1. Le volume accordé à cette ressource est actuellement de 6h de TP (3 séances de 2h). Votre évaluation des TP se basera sur le contenu d'un compte rendu que vous devez rendre en ligne avant la fin de la dernière séance. Ce dernier doit refléter votre travail durant les différentes séances et inclut entre autres les réponses aux questions pratiques et théoriques posées. Dans votre compte rendu notez bien le début et la fin de votre travail pour chaque séance afin de bien distinguer votre évolution au fil des séances. À chaque début de nouvelle séance, vous reprenez votre travail de l'endroit où vous vous êtes arrêté lors de la précédente séance de TP. S'il vous reste du temps lors de la dernière séance, profitez-en pour améliorer et finaliser votre compte rendu.

2. La remise de votre compte rendu (un seul fichier PDF comportant tout votre travail de TP cumulé depuis la première séance) s'effectue avant la fin de la dernière séance de votre TP (mais pas après) exclusivement en ligne sous ENT (espace Moodle nommé : « Espace de remise des comptes rendus TP »). Aucun autre mode de remise ne sera accepté, aucun retard ne sera toléré. La date de l'upload/téléversement de votre fichier fait foi. Assurez-vous de bien uploader/téléverser votre compte rendu dans la section de votre groupe TP (et non pas dans une section qui concerne un autre groupe)

3. Prenez notes lors de vos manipulations afin d'enrichir votre compte rendu en plus des réponses aux questions théoriques et aux captures d'écran qui viendront appuyer votre travail rendu.

4. Les comptes rendus sont le fruit d'un travail personnel, votre compte rendu final (contenu et forme) sera soumis à un traitement anti-plagiat en utilisant les outils automatisés de l'université

Le non respect de ces consignes peut donner lieu à des pénalisations lors de votre évaluation TP.

### Objectifs de ce TP


- Reprendre la maîtrise de l'outil Packet Tracer (simulateur de réseaux) déjà utilisé l'année précédente dans différents modules.
- Comprendre le fonctionnement des équipements d'interconnexion
- Observer et comprendre l'encapsulation des protocoles et le modèle en couches
- Réalisation concrète d'un réseau physique
- Adressage et configuration des équipements

### Outil et documentation :

- Simulateur Packet Tracer 6.0.1 de cisco (déjà installé sur vos machines)
  - N'oubliez pas que les mêmes configurations faites sous Packet Tracer s'appliquent sur un réseau réel (par exemple sur de vrais routeurs Cisco)
  - Attention, si vous utilisez une version Packet Tracer différente de celle installée dans vos machines de TP, c'est à vous de vous documenter pour s'adapter aux manipulations demandées.
- Documentation : section ENT : Contenus des TPs/Documentation (référence :

## Préambule


- Depuis l'ENT (Contenus des TP/TPx/fichier.pkt) récupérer le(s) fichier(s) du TP. Vous l'avez compris, ce sont des fichiers spécifiques au logiciel de simulation de réseaux « Packet Tracer »
- Télécharger et ouvrir le fichier correspondant à chaque TP avant de le commencer.

 ***N'hésitez pas à utiliser la documentation : cours, TD et vos notes prises lors de la correction du TD.***

## Exercice 1) DHCP

Vous avez déjà eu un aperçu rapide du DHCP en le manipulant dans une ressource précédente. Comme vous le savez, le protocole **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) comme son nom l'indique est un protocole qui permet la configuration dynamique d'une machine sans que ce soit fait par vous-même ou par un administrateur. Lorsqu'on fait appel au service DHCP, la configuration fournie consiste à affecter une adresse IP et le masque associé à l'interface de la machine, ainsi que : le routeur par défaut (gateway) que la machine peut utiliser, aussi cela inclut l'adresse IP d'un (ou plusieurs) serveur(s) DNS et éventuellement d'autres informations utiles au bon fonctionnement en réseau d'une machine.

Dans la configuration de cet exercice, il y a deux serveurs DHCP (www.gauche.fr est un serveur DHCP et le routeur de Gauche l'est aussi) dans le réseau local de gauche. Le but de la manipulation est de comprendre les échanges entre client(s) et serveur(s) DHCP.

 ***Il est tout à fait possible et praticable, dans la vraie vie, d'opter pour un serveur DHCP au niveau d'un équipement de type routeur (comme le fait votre boxe d'opérateur) comme c'est possible de mettre en place un serveur DHCP sur une machine de notre réseau***

Le protocole DHCP n'est utilisable que dans un réseau local, i.e. les nœuds de votre LAN peuvent en profiter. Le service DHCP utilise le protocole (de couche 4) UDP pour le transport des données. Le client (machine qui n'a pas au préalable une configuration IP) n'est pas supposé connaître l'adresse IP du serveur DHCP qui existe dans son réseau. De plus, il peut même y avoir plusieurs serveurs DHCP dans le même réseau que le client. La figure 1 vous donne un message DHCP embarqué/transporté dans un message UDP.

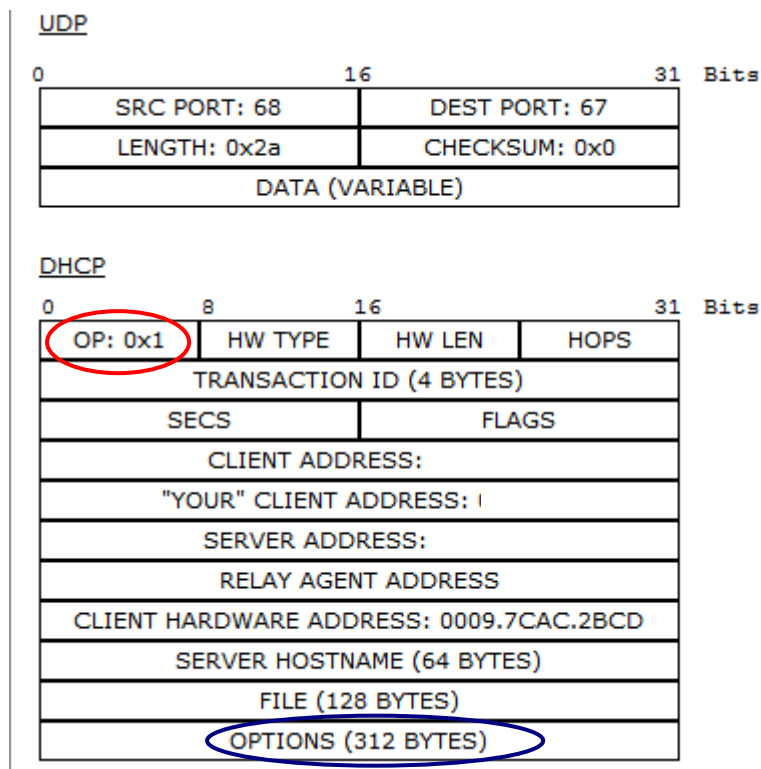


Figure 1 : Message DHCP (dans un message UDP)

Chaque message du protocole DHCP a une signification particulière. Cette signification est donnée par le code opération (**OP**) dont la liste est donnée dans la figure 2. Ce code est associé à l'un des champs 'options' pour identifier le type du message DHCP.

Les champs « Clien Address » jusqu'à « Hardware Address » sont obligatoires dans le message DHCP. Leurs significations est simple à deviner. Le champ « Options », selon le code message, peut être soit une demande spécifique de configuration (i.e. le client demande, par exemple, l'adresse IP d'un serveur DNS) soit une configuration (i.e. le serveur informe le client de l'existence d'un serveur DNS dont l'adresse IP est dans les options).

nom(OP)	Option (valeur)	Code	description
DHCPDISCOVER (1)	'DHCP Message Type' (53)	1	<b>le client (1)</b> envoie ce message pour <i>localiser</i> les serveurs DHCP disponibles et demander une première configuration
DHCPOFFER (2)		2	réponse <b>du serveur (2)</b> à un message DHCPDISCOVER, qui contient les <i>premiers paramètres</i>
DHCPREQUEST (1)		3	requête diverse <b>du client(1)</b> pour par exemple prolonger son « bail »
DHCPDECLINE (1)		4	<b>le client(1)</b> annonce au serveur que l'adresse est <i>déjà utilisée</i>
DHCPACK (2)		5	réponse du <b>serveur(2)</b> qui contient des <i>paramètres et l'adresse IP</i> du client
DHCPNAK (2)		6	réponse du <b>serveur(2)</b> pour signaler au le client que son <i>bail est échu</i> ou si le client annonce une <i>mauvaise configuration</i> réseau
DHCPRELEASE (1)		7	<b>le client(1)</b> libère son adresse IP
DHCPINFORM (1)		8	<b>le client(1)</b> <i>demande des paramètres</i> locaux, il a déjà son adresse IP

Figure 2 : Code Opération d'un message DHCP (le champ 'option' n'est pas visible dans Packet-Tracer)

### Manipulation :

Les deux PC de gauche sont éteints.

- Mettez Packet Tracer en mode « simulation »
- Filtrez les messages DHCP pour capturer exclusivement les messages DHCP

- Allumez les deux PC et configurez les en mode DHCP.
- Répondez aux questions suivantes :

Qa1) Quel est le nom du 'code OP' du premier message DHCP que chaque client transmet ?

Qa2) Dans l'entête IP, quelle est l'adresse IP source que les clients utilisent dans leur premier message ?

Qa3) Est-ce que cette adresse correspond à celle utilisée dans le message DHCP (champ 'CLIENT ADDRESS') ?

Qa4) Dans l'entête IP, quelle est l'adresse IP destination de ce message ?

Qa5) Est-ce que cette adresse correspond à celle utilisée dans le message DHCP (champ 'SERVER ADDRESS') ?


Qa6) A votre avis, quelle est la raison qui oblige cette redondance entre le niveau IP et le niveau DHCP ?

Qa7) Quel est le port source et destination de ce message ? Remarquez-vous que le port 'client' ne suis pas la règle comme les autres protocoles qui ont comme obligation d'avoir un port > 1024 pour les clients.

Qb1) Quel est le nom du 'code OP' de la réponse du serveur ?

Qb2) Reprenez les questions Qa2 à Qa7 pour ce message.

D'une manipulation à l'autre on peut avoir soit l'un, soit l'autre des deux serveurs qui répond à une requête de l'un ou de l'autre des deux clients.


 ***Vous pouvez voir (dans la configuration des deux clients) lequel des deux serveurs a répondu à la sollicitation du client (le serveur [www.gauche.fr](http://www.gauche.fr) donne des adresses IP entre 100 et 150 alors que le routeur donne les autres adresses (sauf la 1 et la 254).***

**Dessinez un diagramme d'échange entre les clients et les serveurs que vous avez constaté.**

## Exercice 2) NAT (Network Address Translation)

Le NAT n'est pas un protocole mais une technique utilisée par les routeurs. Cette technique sert à « traduire » (translate) une adresse IP d'un réseau local (non reconnu à l'extérieur du réseau local) en une adresse IP reconnue (au niveau mondial) par l'internet.

La configuration consiste (pour les routeurs CISCO) à différencier les interfaces internes (*inside* en anglais) de celles qui sont externes. Il suffit, par la suite, de commander la translation des adresses (des paquets) sortantes et (des paquets) entrants : sortant de vos nœuds locaux de votre LAN et entrants vers vos nœuds locaux.

 *À la maison, supposons que votre smartphone est connecté en WiFi à votre boxe d'opérateur. Votre smartphone a une adresse locale non reconnue sur Internet (ex. 192.168.1.20). Votre boxe a une adresse IP publique (fournie par votre opérateur) et qui est reconnue sur Internet. De même, si vous mettez un serveur Web chez vous qui est connecté à votre boxe, comment il pourrait être accessible depuis Internet ? Merci le NAT !*

### Manipulation:

- 1) Mettez Packet Tracer en mode « simulation »
- 2) Filtrez les messages HTTP et TCP
- 3) Mettez-vous sur le navigateur du Client G1. (celui de gauche)
- 4) Tapez dans le bandeau de navigation l'adresse Web « **www.bas.fr** »
  - Q1) Quelle sont les adresses IP source et destination du message TCP qui sort de ce PC ?
  - Q2) Que deviennent ces deux adresses dans le message après son passage par le routeur\_G ?
- 5) Reprendre la manipulation avec le Client G2 (celui de gauche)
  - Q1) Quelle sont les adresses IP source et destination du message TCP qui sort de ce PC ?
  - Q2) Que deviennent ces deux adresses dans le message après son passage par le routeur\_G ?

Le routeur de Gauche est configuré pour « cachez » (mise en mémoire cache) les adresses IP du réseau local (de gauche).

- 6) Identifiez les adresses IP de **www.gauche.fr** et de **www.droite.fr**
  - Q1) Que constatez-vous ?

Remarque : en principe c'est le mode de fonctionnement normal pour un réseau domestique (on utilise les mêmes adresses de réseau de la majorité de ces réseaux).

- 7) Mettez-vous sur le navigateur du ClientB (celui du bas) .  
Tapez dans le bandeau de navigation l'adresse Web « **www.droite.fr** »
  - Q1) Quelle sont les adresses IP source et destination du message TCP qui sort de ce PC ?
  - Q2) Que deviennent ces deux adresses dans le message après son passage par le routeur\_D (celui de droite) et à leur arrivée au serveur dont le nom est **www.droite.fr** ?

Remarque : c'est cette technique qui est utilisée pour pouvoir mettre un serveur (Web, Mail, etc.) interne dans un réseau domestique. Le routeur est configuré pour relayer les messages (de niveau application) à un serveur interne, lorsque le message a comme adresse de destination son adresse IP externe (confirmez en regardant l'adresse externe du routeur de droite en la comparant à l'adresse de destination du message d'origine transmis par ClientB).

- 8) Mettez-vous sur le navigateur du Client G1 (celui de gauche)
- 9) Tapez dans le bandeau de navigation l'adresse Web « **www.droite.fr** »
  - Q1) Quelle sont les adresses IP source et destination du message TCP qui sort de ce PC ?
  - Q2) Que deviennent ces deux adresses dans le message après son passage par le routeur\_G ?
  - Q3) Que deviennent ces deux adresses dans le message après son passage par le routeur\_D ?

Remarque : c'est le cas lorsque depuis un réseau local (domestique) on sollicite un serveur qui est dans un autre réseau local (domestique). Remarquez que si vous tapez l'adresse IP de [www.droite.fr](http://www.droite.fr) (locale au réseau de droite), depuis le ClientG1, vous obtiendrez une réponse de [www.gauche.fr](http://www.gauche.fr).