

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 TPs/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.***

But : Étude des protocoles UDP et TCP

Dans les deux exercices suivants, pour comprendre le rôle de chacun de ces deux protocoles nous nous reposerons pour chacun d'eux d'une application (ou service) particulière.

- Pour UDP, nous nous reposerons sur l'application DNS (Domain Name Services), qui a pour rôle la traduction des « noms de machines » en leur adresse « IP ».
- Pour TCP, nous nous reposerons sur l'application WEB. Est-t-il besoin de vous présenter le WEB ?

 ***Les protocoles UDP et TCP sont deux protocoles de la couche 4 du modèle OSI. Ils ont comme premier rôle de transférer les données émanant des couches 5, 6 et 7 (en général dans le modèle IETF seul la couche 7 est utilisée).***
Rappelons-nous : transactions bancaires Web transportés avec TCP, streaming vidéo transportés avec UDP !

Exercice 1) UDP

Le protocole UDP est le plus simple des protocoles de la couche 4. Il a comme rôle principale l'identification des entités communicantes. Une application (ou service au sens réseau du mot application) qui utilise UDP comme moyen ou support de transport de ses données doit uniquement identifier ses « programmes » qui communiquent.

L'application DNS utilise donc le protocole (de couche 4) UDP pour le transport des données (de bout en bout). Le client et le serveur (les deux programmes qui communiquent) s'échangent des messages UDP dont la forme est donnée dans la figure 1.

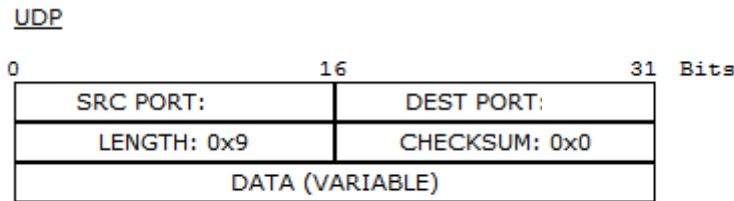


Figure 1 : Message UDP



Bon à savoir : le DNS peut aussi utiliser le transport avec TCP, par exemple, lorsqu'il s'agit de données à fiabiliser comme celles concernant des « zones » entières de noms de domaines entre serveurs DNS

Manipulation A:

- 1) Mettez Packet-Tracer en mode Simulation i.e. en mode pas-à-pas
- 2) Ne gardez que UDP dans le filtre des messages
- 3) Lancez le navigateur Web du PC 192.168.1.1 et mettez dans sa barre de navigation l'adresse Web : **www.droite.fr**
- 4) Faites un schéma des échanges (requêtes/réponses) entre le client et le serveur DNS.

Questions :

1. Quel est le port UDP qui identifie le client ?
2. Quel est le port UDP qui identifie le serveur ?
3. Comment les procédures IP (couche 3) peuvent savoir que le message qu'elle embarque est un message UDP ? (on attend une réponse précise, car c'est un programme qui doit détecter cela)

Manipulation B:

- 1) Relancez la manipulation (en quittant et relançant Paquet-Tracer)
- 2) Attendez que la requête arrive au serveur et coupez la liaison du serveur (sur le switch de droite il suffit de désactiver l'interface le reliant au serveur DNS).
- 3) Que se passe-t-il à ce moment sur le client ?
- 4) Réactivez la liaison avec le serveur : Que se passe-t-il ?

Exercice 2) TCP

Le protocole TCP est le plus complet des protocoles de la couche 4. Il a plusieurs rôles, par exemple :

- i) Comme pour UDP : l'identification des entités communicantes.
- ii) Assurer la « bonne » réception de part et d'autre de données échangées par le client et le serveur de l'application
- iii) « Reprise » en cas d'erreur ou de perte des données
- iv) Contrôler le flux dans le réseau, etc.

Pour cela, le protocole TCP a des états, et il passe d'un état à un autre selon les messages échangés

- 1) État non connecté : c'est celui avant le début du transfert des données et à la fin du transfert des données.
- 2) État connecté : c'est l'état pendant le transfert des données
 - Le passage de l'état 'non connecté' à l'état 'connecté' se fait par l'échange de messages (TCP) spécifique. Ces messages ne doivent pas embarquer des données de niveau application.
 - Le passage de l'état 'connecté' à l'état 'non connecté' se fait par l'échange de trois messages (ou quatre selon la situation). Ces messages ne doivent pas embarquer des

données de niveau application.

- Les programmes client et serveur qui souhaitent échanger des données en utilisant le transport TCP ne peuvent s'échanger ces données que lorsqu'ils sont dans l'état 'connecté'.

L'application WEB (employant le protocole HTTP) utilise le protocole (de couche 4) TCP pour le transport des données (de bout en bout). Le client et le serveur (les deux programmes qui communiquent) s'échangent des messages TCP dont la forme est donnée dans la figure 2. Le protocole TCP impose que ses messages soient numérotés dans le flux (en utilisant le champs SEQUENCE NUM) et que les messages doivent être acquittés (en utilisant le champs ACK NUM).

Les messages TCP sont typés (voir le champ TYPE). Le typage permet de savoir interpréter la signification soit du message lui-même soit de certain champs du message. (voir types de message TCP)

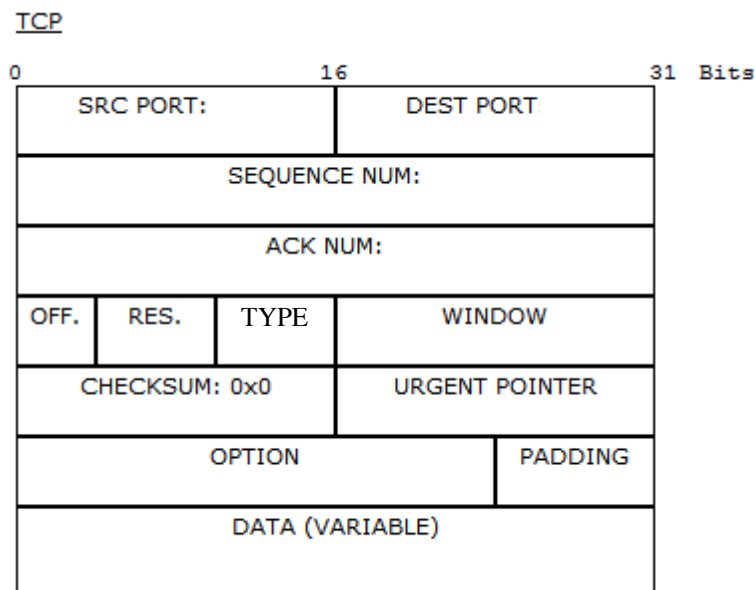


Figure 2 : Message TCP

Type du message (6 bits) TCP : chaque bit, s'il vaut 1, à la signification suivante :

- **URG** : les octets compris entre le début de la trame et le champ pointé par 'Pointeur Message Urgent' (URGENT POINTER) doit être servi en priorité
- **ACK** : les données du champ « Acquittance » (ACK NUM) sont valides
- **PSH** : le paquet doit être transmis à la couche supérieure (au programme qui attend).
- **RST** : réinitialisation de la connexion (de la synchronisation)
- **SYN** : demande de l'ouverture d'une connexion (synchronisation).
- **FIN** : fin de connexion (de la synchronisation)

Manipulation A: TCP en fonctionnement normal

- 1) Mettez Packet-Tracer en mode Simulation en mode pas-à-pas
- 2) Ne gardez que TCP dans le filtre des messages
- 3) Lancez le navigateur Web du PC 192.168.1.1
- 4) Dans la barre de navigation : tapez l'adresse Web **www.droite.fr**
- 5) Faites un schéma des échanges TCP (en incluant HTTP) entre le client et le serveur

But : Comprendre le rôle des différents champs (SEQUENCE, ACK, 'TYPE'...) d'un message TCP

• **Questions :**

1. Faites un schéma (sous forme de diagramme) d'échange entre le client et le serveur.
2. Identifier le type (il peut être de plusieurs types en même temps) de chaque message et sa signification (en particulier les messages qui ne sont que de type ACK)
3. Quels sont les ports TCP qui identifient le client et le serveur ?
4. Identifiez les messages TCP qui permettent l'ouverture de la connexion
5. Identifiez les messages TCP qui permettent l'échange de données entre le client et le serveur (au niveau application).
6. Pouvez-vous donner la longueur du champ de données (DATA) de chacun des messages ci-dessus en ne regardant que le champ SEQUENCE ?
7. Identifiez les messages de fermeture de la connexion

Manipulation B: TCP en cas d'anomalie dans le réseau

Le but de cette manipulation est de voir comment réagi le protocole TCP en cas de perte d'un message.

1. Relancez la manipulation (en quittant et relançant Paquet-Tracer éventuellement)
2. Attendre que le 1^o message TCP arrive au serveur et coupez la liaison du serveur (sur le switch de gauche, il suffit de désactiver l'interface le reliant au serveur « www »).
3. Que se passe-t-il par la suite sur le client ?
4. Réactivez la liaison avec le serveur : que se passe-t-il (au niveau TCP) ?
5. Refaire la même chose (coupez la liaison entre switch et serveur), après que le serveur ait transmis le premier message de données (de la page web en fait).
6. Que se passe-t-il au niveau TCP ?
7. Que se passe-t-il lors de la reprise de la liaison entre le switch et le serveur ?
8. Faites un schéma des échanges que vous avez observé en précisant les numéros des séquences des messages et les numéros d'acquittance (ACK NUM).
9. Pouvez-vous en déduire la véritable signification du champ « SEQUENCE NUM » ?