

Préambule

Dans ce TD, nous allons voir, dans la limite du temps disponible, plusieurs notions réseaux relative aux architectures réseaux. Il est recommandé d'utiliser la documentation dont vous disposez y compris le support de votre cours disponible en ligne sur Moodle.

1. Adressage IPv4 (rappel)

1. Pour chacun des numéros de réseau suivants, complétez le tableau.



Pour rappel, la « notation CIDR » (Classless Inter-Domain Routing) donne l'adresse du réseau suivi par une barre oblique (ou slash, « / ») et le nombre de bits à 1 dans la notation binaire du masque du réseau. Par exemple, le masque sous format décimal : 255.255.224.0 est équivalent en binaire à 11111111.11111111.11100000.00000000. La notation CIDR sera donc donnée par /19 (19 bits à la valeur 1, suivis de 13 bits 0).

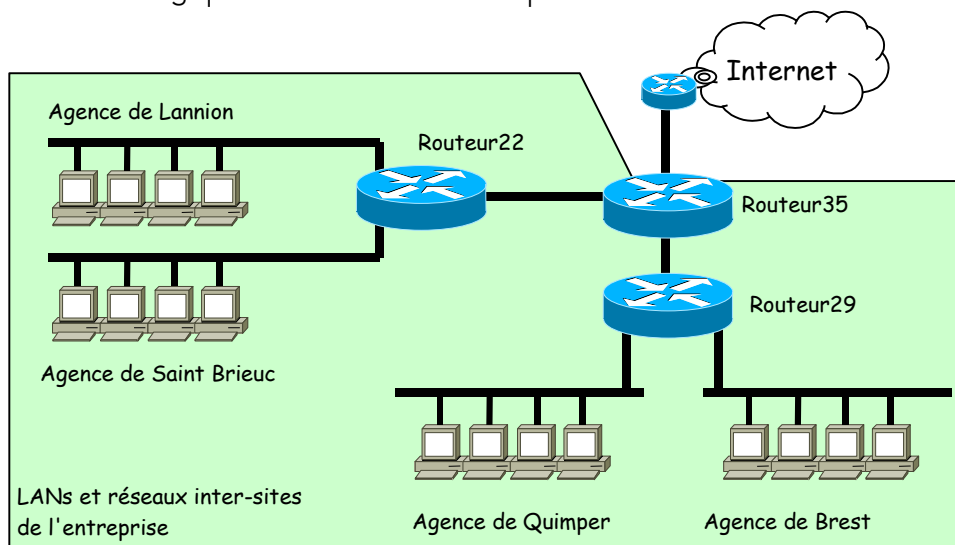
	Numéro du réseau	Masque (décimal ou CIDR)	Nombre d'@Ip	Première @ IP machine	Dernière @ IP machine	@IP de broadcast
1	181.72.27.64/28					
2	81.12.32.0/25					
3	81.12.32.0/20					
4	1.2.0.0 masque 255.255.128.0					
5	12.81.27.48/30					
6	72.27.13.128 masque 255.255.255.240					
7	6.27.16.0 masque 255.255.254.0					
8	7.8.64.0 masque 255.255.252.0					
9	7.8.64.0 masque 255.255.248.0					
10	7.8.64.0 masque 255.255.240.0					

2. Déterminer s'il s'agit d'un numéro de réseau, d'une adresse de machine ou d'une adresse de broadcast dans le tableau suivant.

	Numéros IPv4	Numéro réseau	Adresse machine	Adresse Broadcast
1	10.254.65.10 255.255.240.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	172.0.15.255/19	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	172.0.15.255/20	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	25.15.8.15 255.255.255.240	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	25.15.8.15 255.255.255.224	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	25.15.48.0 255.255.240.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	25.15.49.0 255.255.224.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	54.55.56.132/30	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	54.55.56.133/30	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	54.55.56.134/30	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Architecture réseau et affectation d'adresses

Voici l'architecture logique du réseau d'une entreprise :



L'entreprise a acheté le numéro de réseau 149.20.30.0/24. Après analyse de ses besoins, l'administrateur réseau de l'entreprise :

- Constate que le plus grand réseau IP n'accueillera jamais plus de 12 ordinateurs.
- Décide de découper linéairement le numéro de réseau qu'elle a acheté (donc d'avoir des réseaux IP de même taille).
- Décide d'effectuer un découpage qui permette de maximiser le nombre de sous-réseaux IP disponibles.

1. L'entreprise a besoin de combien de sous-réseaux IP pour ses LANs et les réseaux inter-sites ?

2. Donnez le masque de sous-réseau (notations / et décimale pointée) pour chaque sous-réseau de l'entreprise.
3. Avec ce découpage, de combien de sous-réseaux l'entreprise dispose-t-elle en tout (pour ses besoins actuels et futurs) ?
4. Donnez la liste des numéros de sous-réseaux disponibles pour ses réseaux IP.
5. Avec ce découpage, l'entreprise dispose de combien de numéros de sous-réseaux de libre ?
6. Quel est l'inconvénient de ce découpage en terme de :
 - ↳ Gaspillage d'adresses IP (nombre d'adresses disponibles dans chaque sous-réseau par rapport au nombre de machines réellement présentes).

3. TCP

Le protocole de transport TCP (Transport Control Protocol) assure le bon acheminement de bout en bout des données :

- En détectant les erreurs de transport grâce au contrôle du flux de données.
- En adaptant la vitesse d'émission des données grâce au contrôle de congestion qui exécute un algorithme particulier dont le but est d'adapter le débit d'émission des segments TCP à la charge du réseau

Les données échangées sont considérées comme un flot de bits divisé en octets (groupes de 8 bits). Ces octets doivent être reçus dans l'ordre où ils sont envoyés.

Contrôle de flux

Il permet d'assurer qu'il n'y aura pas de perte de segments.

- Les données émises sont acquittées grâce au mécanisme reposant sur les deux compteurs présents dans l'entête TCP de chaque segment :
 - N° séquence (numéro du 1er octet transporté)
 - N° d'acquittement (numéro du prochain octet attendu)
- L'absence d'un acquittement indique :
 - Soit la perte d'un segment.
 - Ou la perte de son acquittement.
 - Ou encore une congestion du réseau (temps de transit anormalement long).

C'est pourquoi, TCP gère une temporisation qui déclenche la retransmission du segment sur la non réception de l'acquittement de celui-ci au bout d'un temps donné (time-out). La valeur de cette temporisation est déterminée par une estimation du temps aller-retour d'un segment (RTT, Round Trip Time).

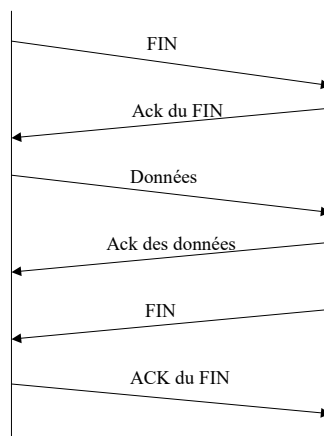
Afin d'optimiser le débit efficace, la transmission des segments par un émetteur est anticipée grâce à une fenêtre d'anticipation (les acquittements sont alors cumulatifs et sur épuisement de la temporisation, il y a retransmission à partir du 1er octet non acquitté). La taille de la fenêtre d'anticipation est la plus petite valeur entre :

- La valeur du champ Window de l'entête TCP du segment reçu. Rappel : Window indique le nombre d'octets que le récepteur est prêt à accepter (taille du tampon de réception) ; pour obtenir sa valeur en nombre de segments, il suffit de diviser Windows par le MSS (Maximum Segment Size qui limite la taille des paquets).
- La fenêtre de congestion dont la taille est déterminée localement par les mécanismes appelés « démarrage lent ou slow-start » et de « évitement de congestion ou collision avoidance »



À noter que la fenêtre TCP a eu une utilisation surtout historique au niveau du fonctionnement des réseaux (même si elle est toujours utilisée aujourd'hui pour d'autres utilisations). Elle permettait notamment aux machines les moins puissantes de ralentir une connexion TCP si l'émetteur envoyait ses informations trop rapidement.

1. De point de vue applicatif, d'après vous, pourquoi on a inventé TCP et UDP et ne pas se contenter d'échanger des paquets IP bruts ?
2. Sur combien d'octets sont encodés les ports sources et destination d'un paquet TCP ?
3. Quelles sont les valeurs théoriques possibles des ports TCP ? Même question pour les ports UDP ?
4. Quelle entité (entité passive ou active) qui utilise des ports bien connus et celle qui utilise des ports éphémères et pourquoi ?
5. Quel mode de transport (TCP ou UDP) vous pensez plus pertinent pour les services multimédias et le service DNS (entre un client et un serveur) ?
6. Comment sont différenciés les différents rôles des messages TCP (ex. SYN, FIN, etc.) ?
Donnez la valeur hexadécimale et décimale des messages TCP très utilisés : SYN, ACK, SYN+ACK, FIN, ACK+FIN
7. Ci-dessous un diagramme d'échange en TCP entre deux machines :



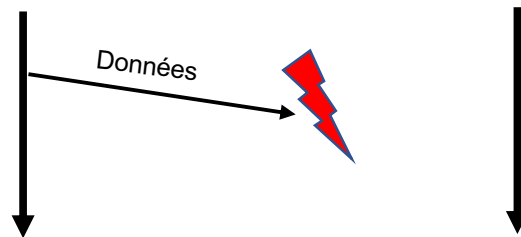
- a. Rappelez la signification des différents messages présents dans le diagramme
- b. Peut-on déduire le nom de l'entité de droite ainsi de celle de gauche (entité active/passive) ?
- c. Ce diagramme est-il correct ? Si non proposez -sous forme de phrases- une correction
- d. Redessinez le diagramme ci-dessous avec l'échange correct en maintenant les deux premiers messages intacts

8. Deux types de problèmes possibles peuvent se produire lors d'un envoi de segments en TCP :

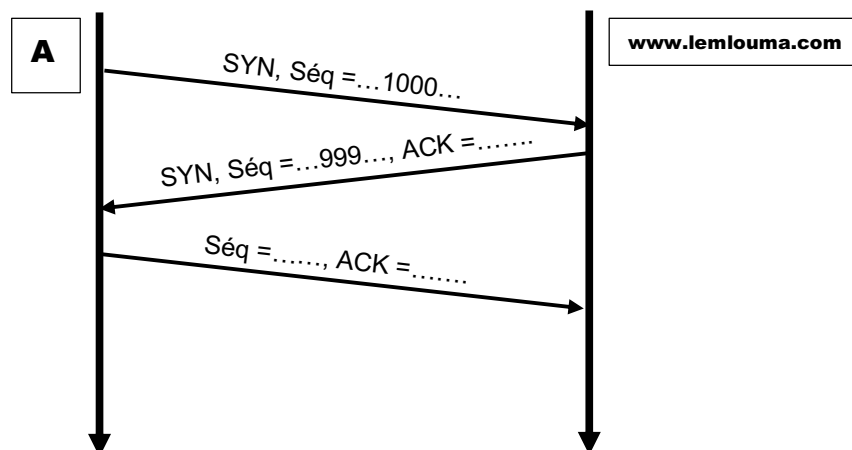
- Les données reçues du segment sont endommagées au niveau du destinataire
- Le segment n'arrive jamais au destinataire

Pour détecter ce type de problème, chaque fois qu'il envoie un segment l'expéditeur effectue une utilisation : « un buffer » et « une temporisation ».

- Expliquer sous forme de texte l'algorithme utilisé basé sur le buffer et la temporisation.
- Représenter cet algorithme dans le diagramme suivant :



9. Sur une machine A, on a ouvert un navigateur Web et tapé l'URL : <http://www.lemlouma.com>. Le diagramme suivant représente les trois premiers segments de « transport réseau » capturés sur l'interface Ethernet de sortie de la machine A :



- Quel est le protocole de transport utilisé ?
- À quoi correspond cette séquence de segments TCP ? Que peut-on dire sur les ports impliqués ?
- Quelle est la différence entre le premier et le deuxième segment TCP ?
- Complétez l'échange en précisant les valeurs manquantes
- Précisez dans le diagramme d'échange précédent, l'instant exact où la connexion est réputée « confirmée » pour la machine A et aussi pour la machine serveur.
- Imaginez que l'ouverture de session TCP ne s'effectue pas à 3 phases (envoi de 3 segments) **mais à 1 ou 2 phases**, dessiner deux cas d'échange entre A et le serveur qui montrent que des données peuvent être perdues suite à un déséquilibrage des paquets introduit par le routage du réseau (c-à-d : en routage on a aucune garantie que les paquets sont reçus dans le même ordre de leur émission)

10. Complétez les numéros de séquence et d'acquittements des messages de l'échange TCP suivant entre les machines A et B :

